DATI PERSONALI

PROTEZIONE, LIBERA CIRCOLAZIONE E *GOVERNANCE*

1. Principi

a cura di
Fabio Bravo

Pacini Giuridica

DATI PERSONALI

PROTEZIONE, LIBERA CIRCOLAZIONE E *GOVERNANCE*

1. Principi

a cura di
Fabio Bravo

Pacini Giuridica

© Copyright sull'Opera 2023 Prof. Avv. Fabio Bravo

Tutti i diritti riservati al Curatore Fabio Bravo, salvo quanto di seguito specificato. All'Editore è stato concesso il diritto esclusivo e senza limiti territoriali (con divieto di cessione a terzi) di pubblicazione a stampa e distribuzione dell'Opera. Gli ulteriori diritti restano in capo al Curatore in via esclusiva. L'Editore e il Curatore, ciascuno per quanto di propria spettanza, rilasciano la presente opera anche in formato digitale (PDF editoriale) ad accesso aperto in licenza Creative Commons CC BY ND 4.0, disponibile per il download gratuito sul sito cris.unibo.it, con il seguente identificativo persistente 11585/948658 | https://hdl.handle.net/11585/948658.

ISBN 978-88-3379-672-7

Realizzazione editoriale

Pacini Editore

Via A. Gherardesca
56121 Pisa

Responsabile di redazione
Gloria Giacomelli

Fotolito e Stampa
IGP Industrie Grafiche Pacini

INDICE

Introduzione ..... » XV
Fabio Bravo

Prefazione ..... » XIX
Guido Alpa

Capitolo I
I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, nel solco delle *rules of construction* ..... » 1
Fabio Bravo

1. Stefano Rodotà, i principi in materia di protezione dei dati personali e la «riscrittura delle tavole dei valori» nel contesto tecnologico ..... » 2
   1.1. La funzione adeguatrice dei principi ..... » 2
   1.2. La funzione ordinante dei principi e la composizione degli interessi in gioco ..... » 3
   1.3. Principi e tecnica legislativa ..... » 4
   1.4. Dai principi in materia di protezione dei dati personali all'*Internet Bill of Rights* e l'enfasi sulla necessità di una «riscrittura delle tavole dei valori» ..... » 4
2. L'affermazione dei principi nel GDPR ..... » 9
3. Prospettive ed obiettivi della ricerca sull'applicazione dei Principi del GDPR ..... » 11
4. Dalla protezione dei dati personali al diritto a trattare dati personali. La collocazione dei principi del GDPR nel panorama più esteso dei nuovi *Digital Rights and Principles* ..... » 12
5. La "riscrittura" della tavola dei valori ad opera dell'UE: la nuova «*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*» ..... » 15
   5.1. Il solco tracciato da Stefano Rodotà e la "riscrittura" della tavola dei valori ad opera della Commissione europea. La Comunicazione «relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali» [COM(2022)27 *final*] ..... » 15
   5.2. L'asserita (ma illusoria) natura meramente politica della Dichiarazione europea sui diritti e sui principi digitali ..... » 18
   5.3. La «*European Declaration on Digital Rights and Principles for the Digital Decade*» (2023/C 23/1) ..... » 21
   5.4. Mettere le persone al centro della trasformazione digitale ..... » 23
   5.5. Solidarietà e inclusione (connettività, condizioni di lavoro, istruzione, formazione e competenze digitali, condizioni di lavoro giuste ed eque, servizi pubblici digitali *online*) ..... » 24
   5.6. Libertà di scelta (interazioni con algoritmi e sistemi di intelligenza artificiale, un ambiente *online* equo) ..... » 28
   5.7. Partecipazione allo spazio pubblico digitale ..... » 30

5.8. Sicurezza, protezione ed *empowerment* (un ambiente digitale sicuro, protetto e tutelato, vita privata e controllo individuale sui dati, protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale) ... » 31
5.9. Sostenibilità ... » 34
6. Una lettura circolare: dai *Digital Principles* ai principi in materia di protezione dei dati personali ... » 35
6.1. La circolarità del discorso ... » 35
6.2. Verso una "costituzionalizzazione" dei nuovi diritti e principi digitali ... » 35
6.3. L'embrionale fase di "riscrittura" dei nuovi diritti e principi digitali e prospettive di successivo ampliamento ... » 38
6.4. Nuovi diritti e principi digitali e trattamento di dati personali ... » 38
6.5. Valenza "interna" ed "esterna" dei principi in materia di protezione dei dati personali ... » 39
6.6. Funzioni e caratteristiche dei principi in materia di protezione dei dati personali. "Principi-valore" e "principi-funzionali" ... » 40
6.6.1. La scelta sistematica del legislatore europeo: i principi nel GDPR ... » 40
6.6.2. La funzione dei principi in materia di protezione dei dati personali e l'aderenza diretta e indiretta al piano assiologico: "principi-valore" e "principi-funzionali" ... » 41
6.6.3. (segue) L'individuazione dei "principi-valore" e "principi-funzionali" nel GDPR ... » 45
6.6.4. Importanza ed opportunità della "rilettura" dei principi alla luce del diritto vivente, nonché dell'individuazione e della ricostruzione sistematica delle *rules of construction* ad essi riferibili ... » 50

Capitolo II
Il principio di liceità ... » 55
Giacomo Bianchedi - Cristina Modica
1. Inquadramento normativo ... » 56
1.1. I riferimenti normativi alla liceità del trattamento nel GDPR e nella Carta dei diritti fondamentali dell'UE ... » 56
1.2. La rilevanza dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo del 1950 ... » 58
1.3. La liceità del trattamento nella Convenzione n. 108 del 1981 e nella Convenzione n. 108+, aggiornata con Protocollo emendativo del 2018 ... » 59
1.4. La liceità del trattamento nella Direttiva 95/46/CE ... » 59
1.5. La liceità del trattamento nella l. n. 675/96 ... » 61
1.6. La liceità del trattamento nel d.lgs. n. 196/03 (Codice in materia di protezione dei dati personali), antecedentemente alla novellazione del 2018 ... » 63
1.7. Novellazione del Codice in materia di protezione dei dati personali ad opera del d.lgs. n. 101 del 2018 e principio di liceità del trattamento ... » 64
2. Portata applicativa del principio ... » 65
2.1. Inquadramento teorico ed interpretazione dottrinale ed istituzionale del principio di liceità ... » 65

2.2. Condizioni di liceità rimesse alla valutazione dell'interessato: il consenso ..... » 69
2.2.1. In particolare, il consenso dei minori ..... » 74
2.3. Condizioni di liceità rimesse alla valutazione congiunta tra interessato e titolare: esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato ..... » 75
2.3.1. In particolare, la commercializzazione dei dati personali tra consenso e contratti di scambio ..... » 76
2.4. Condizioni di liceità rimesse alla valutazione del legislatore: adempimento di un obbligo legale, salvaguardia di interessi vitali dell'interessato o di un'altra persona, esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ..... » 77
2.4.1. In particolare, il trattamento effettuato dalla pubblica amministrazione ..... » 80
2.4.2. In particolare, i trattamenti nel contesto dell'epidemia ..... » 80
2.5. Condizioni di liceità rimesse alla valutazione del titolare: il legittimo interesse del titolare o di un terzo ..... » 82
2.5.1. In particolare, il *marketing* diretto e i *cookies* ..... » 84
3. Applicazione del principio nella casistica ..... » 84
3.1. Il principio di liceità nella casistica nazionale ..... » 84
3.1.1. La liceità del consenso nella commercializzazione di dati personali e nelle pratiche di *marketing*. Il caso «Ad Spray» innanzi al Garante per la protezione dei dati personali e alla Corte di Cassazione ..... » 84
3.1.2. L'illiceità del trattamento avente ad oggetto operazioni di recupero del consenso alle campagne di *marketing*. Il caso «Wind Tre» innanzi al Garante per la protezione dei dati personali e alla Corte di Cassazione ..... » 88
3.1.3. Ancora sulla liceità del consenso al trattamento dei dati personali quale controprestazione della fornitura di servizi erogati senza richiesta di compenso. Il caso «Facebook» innanzi all'AGCM e al giudice amministrativo (TAR e Consiglio di Stato) ..... » 90
3.1.4. Liceità del trattamento e consenso dei minori nella società digitale. Il caso «Tik Tok» nei diversi provvedimenti del Garante ..... » 93
3.2. La casistica internazionale sulla «*lawfulness of processing*» ..... » 96
3.2.1. Liceità del trattamento, approvazione dei *cookies* e validità del consenso. Il caso della SA spagnola sul vettore «Vueling Airlines» ..... » 96
3.2.2. (*segue*): e la pronuncia della CGUE sul caso «Planet49» ..... » 97
3.3. Le *app* di *contact tracing* nella pandemia da Covid-19 in Europa e in Italia ... » 99
3.4. (*segue*): Le Linee Guida dell'*European Data Protection Board* (EDPB) ..... » 100
3.5. (*segue*): Le *app* di *contact tracing* nei provvedimenti del Garante ..... » 104

Capitolo III
Il principio di correttezza ..... » 107
Giovanni Di Ciollo
1. Inquadramento normativo ..... » 107
1.1. Le disposizioni rilevanti in ambito nazionale e sovranazionale ..... » 107
1.2. La correttezza tra clausola generale e principio ..... » 109

2. Portata del principio ..... » 111
2.1. La determinazione contenutistica del principio di correttezza. L'inevitabile confronto con il canone civilistico di correttezza e buona fede ..... » 111
2.2. Il principio di correttezza come criterio di bilanciamento di interessi ..... » 118
2.3. Rilevanza dell'abuso del diritto in ambito *privacy*. Il problema della revoca del consenso ..... » 121
2.4. Correttezza e modalità operative ..... » 129
2.5. Regole deontologiche e codici di condotta ..... » 131
2.6. Finalità del trattamento, ragionevoli aspettative ..... » 133
3. Applicazione del principio nella casistica ..... » 135
3.1. Estensione e limiti del principio di correttezza ..... » 135
3.2. Uno sguardo concreto alla correttezza "procedurale" ..... » 138
4. Riflessioni conclusive ..... » 139

Capitolo IV
Il principio di trasparenza ..... » 141
Federica Cilia - Silvia Dalle Nogare - Raffaella Pozzi
1. Inquadramento normativo ..... » 141
1.1. L'enunciazione del principio di trasparenza nel GDPR ..... » 141
1.2. Il principio di trasparenza nell'evoluzione normativa in materia di protezione dei dati personali ..... » 142
1.3. Ancora sulla trasparenza nel GDPR come principio del diritto europeo in materia di protezione dei dati ..... » 149
2. Portata del principio ..... » 153
2.1. Contenuti del principio di trasparenza ..... » 153
2.2. Principio di trasparenza, diritti dell'interessato e obblighi di informazione in relazione alle attività di trattamento. Connessioni tra principio di trasparenza e principio di liceità ..... » 156
2.3. Ancora su principio di trasparenza e diritti dell'interessato ..... » 160
2.4. Il principio di trasparenza nei trattamenti effettuati dalla Pubblica Amministrazione ..... » 165
3. Applicazione del principio nella casistica ..... » 170
3.1. Il principio di trasparenza nell'adempimento dell'obbligo di informativa ..... » 170
3.2. Il principio di trasparenza rispetto all'uso di nuove tecnologie e ai diritti dell'interessato ..... » 177
3.3. Pubblica Amministrazione e trattamenti dei dati personali tramite processi decisionali automatizzati. Bilanciamento tra principio di trasparenza e diritto d'autore ..... » 180

Capitolo V
Il principio di limitazione delle finalità ..... » 185
Alice Incerti
1. Inquadramento normativo ..... » 186
1.1. L'enunciazione del principio di limitazione delle finalità nell'art. 5 del GDPR ..... » 186

1.2. L'embrionale formulazione del principio di limitazione delle finalità nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali ... » 187
1.3. Il principio di limitazione della finalità nel Patto internazionale sui diritti civili e politici ... » 188
1.4. Il principio di limitazione della finalità nella Convenzione 108 e nella Convenzione 108+ ... » 192
1.5. Il principio di limitazione della finalità nella Direttiva 95/46/CE ... » 194
1.6. Il principio di limitazione delle finalità nella Carta dei diritti fondamentali dell'Unione europea ... » 195
1.7. Il principio di limitazione delle finalità nella l. 31 dicembre 1996, n. 675 ... » 198
1.8. Il principio di limitazione delle finalità nel Codice della *privacy* e nel GDPR ... » 200
2. Portata del principio ... » 203
2.1. La *ratio* del principio di limitazione della finalità nel GDPR ... » 203
2.2. Il principio di limitazione della finalità quale fondamento di ulteriori principi in materia di *data protection* ... » 205
2.3. Il ruolo del titolare ed il trattamento dei dati nel rispetto del principio di limitazione della finalità ... » 209
2.4. Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi ... » 212
2.5. Il principio di limitazione della finalità quale presupposto per il rilascio del consenso al trattamento ... » 214
2.6. Le cc.dd. finalità incompatibili e il *compatibility test* ... » 217
3. Applicazione del principio nella casistica ... » 221
3.1. Granularità del consenso, *marketing* diretto, *social spam* e *marketing* virale ... » 221
3.2. Il principio di limitazione della finalità nella giurisprudenza della Corte europea dei diritti dell'uomo ... » 224
3.3. Principio di limitazione della finalità e *big data* ... » 226
3.4. Covid-19 *pandemic*. Limitazione della finalità ed *app* per il tracciamento dei contatti ... » 228

Capitolo VI
Il principio di minimizzazione dei dati ... » 231
Silvia Giulia Battistini - Lucrezia Matarazzo - Lara Zanetti
1. Inquadramento normativo ... » 231
1.1. L'enunciazione del principio di minimizzazione dei dati nel GDPR ... » 231
1.2. Minimizzazione e "qualità dei dati" nella Convenzione n.108 del 1981 ... » 232
1.3. Minimizzazione e "qualità dei dati" nella Direttiva 95/46/CE ... » 233
1.4. La normativa italiana di recepimento ... » 235
1.5. Il principio di «minimizzazione dei dati» nel GDPR ... » 237
1.6. Il principio di minimizzazione dei dati nella Convenzione di Strasburgo n. 108, aggiornata a seguito del Protocollo di modifica del 2018 (c.d. Convenzione n. 108+) ... » 238
2. Portata del principio ... » 240

2.1. Il principio di minimizzazione dei dati e i tre criteri in cui si declina ..... » 240
2.2. Il rapporto con altri principi complementari (con particolare riferimento al principio di necessità e di proporzionalità) ..... » 244
2.3. Principio di minimizzazione dei dati ed approccio "olistico" di tipo "quali-quantitativo" ..... » 245
2.4. (*segue*): connessioni con la *privacy by design* e *by default* ..... » 246
3. Applicazione del principio nella casistica ..... » 249
3.1. Il principio di minimizzazione dei dati nella casistica del Garante per la protezione dei dati personali ..... » 249
3.2. Il principio di minimizzazione dei dati nella casistica delle Autorità di controllo degli altri Paesi membri dell'UE ..... » 254
3.3. Il principio di minimizzazione dei dati nella giurisprudenza della Corte di giustizia dell'UE ..... » 257
3.4. Il principio di minimizzazione dei dati nella giurisprudenza nazionale italiana e straniera ..... » 259
3.4.1. Il principio di minimizzazione dei dati nella giurisprudenza della Corte di Cassazione ..... » 259
3.4.2. Il principio di minimizzazione dei dati nella giurisprudenza della Corte Regionale di Bonn ..... » 260
3.5. Riflessioni conclusive ..... » 261

Capitolo VII
Il principio di esattezza ..... » 263
Francesco Avveduto - Carlo Basunti
1. Inquadramento normativo ..... » 263
2. Portata del principio ..... » 269
2.1. Il principio di esattezza: un'ipotesi ricostruttiva ..... » 269
2.2. Il principio di esattezza come baluardo a difesa dei diritti e degli interessi dell'interessato ..... » 271
2.3. Il principio di esattezza tra obblighi e interesse del titolare ..... » 276
2.4. L'esattezza dei dati nell'ambito dei diritti dell'interessato previsti dal GDPR . » 279
3. Applicazione del principio nella casistica ..... » 284
3.1. Il diritto di rettificare dati inesatti al vaglio della Corte di giustizia. Il caso dei documenti dei concorsi professionali e delle valutazioni dell'esaminatore ..... » 284
3.2. Il principio di esattezza nelle pronunce del Garante ..... » 287

Capitolo VIII
Il principio di limitazione della conservazione ..... » 293
Alessandro Chiappini
1. Inquadramento normativo ..... » 293
2. Portata del principio ..... » 296
3. Applicazione del principio nella casistica ..... » 304
3.1. Il principio di limitazione della conservazione nei provvedimenti del Garante per la protezione dei dati personali ..... » 304

3.1.1. Il mutato approccio in materia di limitazione della conservazione: dai provvedimenti generali del Garante (o resi a seguito di verifica preliminare) all'applicazione del principio di *accountability* ... » 304
3.1.2. I provvedimenti in materia di lavoro ... » 306
3.1.3. I provvedimenti in materia di biometria ... » 310
3.1.4. I provvedimenti in materia di videosorveglianza ... » 313
3.1.5. I provvedimenti in materia di *marketing* e profilazione ... » 316
3.1.6. I provvedimenti in ambito giudiziario ... » 318
3.1.7. I provvedimenti in materia di trattamenti a fini statistici o di ricerca scientifica ... » 320
3.2. Il principio di limitazione della conservazione nella giurisprudenza della Corte europea dei diritti dell'uomo ... » 321
3.3. Il principio di limitazione della conservazione in materia di *data retention* tra la giurisprudenza della Corte di giustizia dell'UE e la normativa italiana ... » 322
3.4. Principio di limitazione della conservazione, diritto alla cancellazione e diritto all'oblio ... » 329

Capitolo IX
Il principio di integrità e riservatezza (*rectius*, di sicurezza) ... » 333
Gian Mauro Bilotta - Daniele Sborlini - Ilaria Scarpelli
1. Inquadramento normativo ... » 333
2. Portata del principio ... » 342
2.1. Le funzioni della sicurezza in materia di trattamento dei dati personali e il *risk management approach* ... » 342
2.2. La sicurezza del trattamento e le sue declinazioni (riservatezza, integrità, disponibilità) ... » 346
2.3. Le misure di sicurezza tecniche e organizzative ai sensi dell'art. 32 GDPR e le istruzioni ai sensi dell'art. 29 GDPR ... » 350
2.4. La sicurezza del trattamento sin dalla progettazione e per impostazione predefinita ... » 351
2.5. La sicurezza del trattamento in caso di violazione dei dati (*data breach*) ... » 352
2.6. La sicurezza nei trattamenti che presentano rischi elevati (DPIA) ... » 353
3. Applicazione del principio nella casistica ... » 355

Capitolo X
Il principio di necessità ... » 369
Cristina Chilin - Daniele Sborlini
1. Inquadramento normativo ... » 369
1.1. Premessa su diritto alla protezione dei dati personali e principio di necessità ... » 369
1.2. Il principio di necessità e il suo inquadramento normativo: dal Codice della *privacy* al GDPR ... » 372
1.3. Il principio di necessità nella Convenzione 108/81 e nella Convenzione 108+ ... » 374
2. Portata del principio ... » 376
2.1. Il principio di necessità nel Codice della *privacy* ... » 376

2.2. (*segue*): Rapporto tra principio di necessità e principio di pertinenza e non eccedenza nel Codice della *privacy*: endiadi o duplicazione? ... » 382
2.3. Il principio di necessità alla luce del GDPR ... » 383
2.4. (*segue*): Il principio di necessità nel bilanciamento tra diritto alla protezione dei dati e libera circolazione degli stessi (art. 1, part. 3, GDPR) ... » 384
2.5. (*segue*): Principio di necessità e condizioni di liceità del trattamento diverse dal consenso ... » 388
2.6. (*segue*): Principio di necessità e principio di minimizzazione dei dati nel GDPR ... » 392
2.7. (*segue*): Principio di necessità e valutazione d'impatto *ex* art. 35 GDPR ... » 394
2.8. Il principio di necessità e *privacy by design* e *by default* nel GDPR. Il consolidamento nell'ordinamento europeo dell'originaria accezione del «principio di necessità» già emergente *ex* art. 3 del Codice della *privacy* ... » 395
3. Applicazione del principio nella casistica ... » 397

Capitolo XI
Il principio di proporzionalità ... » 411
Carlo Basunti
1. Inquadramento normativo ... » 411
1.1. La proporzionalità nell'alveo dei principi inerenti al trattamento dei dati personali: nota introduttiva per un inquadramento sistematico ... » 411
1.2. La limitazione secondo proporzionalità dei diritti fondamentali: tra la funzione sociale insita nel *considerando* n. 4 del GDPR e l'apertura dell'art. 1, par. 3, del GDPR ... » 415
2. Portata del principio ... » 420
2.1. Il principio di proporzionalità: radici antiche e nuove prospettive di applicazione ... » 420
2.2. Il test di proporzionalità: il (più) corretto bilanciamento tra interessi concorrenti ... » 423
2.3. Il trattamento dei dati personali alla luce del principio di proporzionalità ... » 426
3. Applicazione del principio nella casistica ... » 430
3.1. Il principio di proporzionalità nei provvedimenti del Garante e orientamenti applicativi ... » 430
3.1.1. Applicazione del principio di proporzionalità con riferimento al tempo di conservazione dei dati ... » 430
3.1.2. Applicazione del principio di proporzionalità con riferimento alle modalità di trattamento ... » 433
3.1.3. Applicazione del principio di proporzionalità con riferimento alla condizione di liceità del «legittimo interesse» e, segnatamente, con riferimento alla valutazione del bilanciamento proporzionale degli interessi ... » 435
3.1.4. Applicazione del principio di proporzionalità per la valutazione delle deroghe all'esercizio dei diritti dell'interessato e, in particolare, dei casi di esonero dall'obbligo, per il titolare del trattamento, di rendere l'informativa all'interessato ... » 438

3.2. Il principio di proporzionalità in materia di trattamento di dati personali in ambiti specifici ... » 440
3.2.1. Il principio di proporzionalità quale limite al (e garanzia per il) controllo dei lavoratori ... » 440
3.2.2. L'applicazione del principio di proporzionalità nel settore pubblico in seguito alla sentenza n. 20/2019 della Corte costituzionale: dal bilanciamento tra riservatezza e trasparenza, al diritto all'oblio quale "questione di proporzionalità" ... » 446

Capitolo XII
Il principio di *privacy by design* e *privacy by default* ... » 457
Stefano Faillace
1. Inquadramento normativo ... » 457
2. Portata del principio ... » 465
2.1. La ricostruzione della portata del principio nella dottrina e nei documenti istituzionali: l'impostazione predefinita di misure di protezione dei dati (*privacy by design*) da parte del titolare. Dalla valutazione del contesto alla scelta della tecnologia più adeguata ... » 465
2.2. Le impostazioni di controllo dei dati oggetto del trattamento (*privacy by default*) e il consenso consapevole dell'interessato ... » 471
2.3. L'integrazione contenutistica dei principi di cui all'art. 25 GDPR ad opera delle Linee Guida n. 4/2019 dell'*European Data Protection Board* (EDPB) ... » 473
2.4. La fonte delle obbligazioni *ex* art. 25 GDPR e la natura della responsabilità per il loro inadempimento ... » 481
3. Applicazione del principio nella casistica ... » 488
3.1. I provvedimenti del Garante nei confronti di privati: *a)* la *privacy by design* nei rapporti di lavoro ... » 488
3.2. (*segue*): *b)* attività promozionali dell'impresa e obblighi da rispettare in conformità alle prescrizioni del GDPR ... » 492
3.3. La violazione delle norme di cui all'art. 25 del GDPR da parte della pubblica amministrazione ... » 495

Capitolo XIII
Il principio di responsabilizzazione (*accountability*) ... » 501
Fiorella Albanese - Isabella Cardinali
1. Inquadramento normativo ... » 501
2. Portata del principio ... » 507
2.1. Il concetto di *accountability* ... » 507
2.2. Codici etici e certificazioni ... » 508
2.3. Ricadute applicative nel diritto positivo ... » 510
2.4. Gli strumenti documentali e probatori espressione del principio di *accountability* ... » 517
2.5. Le misure di "secondo livello": modelli organizzativi e nomina volontaria del DPO ... » 520
2.6. Dalla responsabilità *ex ante* a quella *ex post*: i riflessi del principio di *accountability* sulla responsabilità civile (legittimazione passiva e prova liberatoria) ... » 522

2.7. Brevi cenni al rapporto fra *accountability* e responsabilità amministrativa ..... » 525
3. Applicazione del principio nella casistica ..... » 526
3.1. Breve premessa ..... » 526
3.2. *Accountability* e trattamento dati per finalità di *marketing*: i casi Tim S.p.a e Wind Tre S.p.a. nei provvedimenti del Garante ..... » 527
3.3. (*segue*): i casi Fastweb S.p.a. ed Edison Energia S.p.a. ..... » 534
3.4. L'*accountability* al suo esordio: le prime sanzioni delle autorità di controllo degli altri Paesi dell'EU ..... » 536
4. Riflessioni conclusive ..... » 537

Capitolo XIV
Il principio di solidarietà ..... » 541
Fabio Bravo
1. Inquadramento normativo ..... » 541
1.1. La solidarietà come principio normativo e la sua declinazione nel settore della datificazione della società, dell'economia e delle istituzioni ..... » 541
1.2. Il principio di solidarietà nel GDPR e nel *Data Governance Act* (Reg. UE 868/2002) e il *data altruism* ..... » 548
2. Portata del principio ..... » 555
2.1. Le direzioni del principio di solidarietà al cospetto (del trattamento) dei dati personali: (i) la solidarietà come "limite" per il titolare del trattamento ..... » 555
2.2. (*segue*): (ii) …e per l'interessato. La «funzione sociale» al cospetto (del trattamento) dei dati personali ..... » 558
2.3. (*segue*): (iii) la solidarietà come "orizzonte", secondo le logiche dell'inclusione ..... » 563
2.4. (*segue*): (iii) …e secondo le logiche della condivisione e dell'altruismo (*data altruism*) ..... » 564
3. Applicazione del principio nella casistica ..... » 570
3.1. Il principio di solidarietà nei provvedimenti del Garante ..... » 570
3.2. Il principio di solidarietà nelle pronunce della Cassazione in tema di «funzione sociale» e in tema di risarcimento del danno da illecito trattamento di dati personali (ed altre significative sentenze della giurisprudenza di merito) ..... » 575
3.3. Riflessioni critiche sulla deriva giurisprudenziale in tema di "solidarietà-tolleranza" e sui filtri selettivi della "gravità della lesione" e della "serietà del danno". Le peculiarità in tema di protezione dei dati personali ..... » 586
3.4. La sentenza della Corte di giustizia dell'UE del 4 maggio 2023 (C-300/21) sull'inammissibilità di soglie minime di risarcibilità del danno non patrimoniale relative alla gravità del danno (ed alla serietà della lesione) in materia di protezione dei dati personali e il parziale *revirement* della Corte di Cassazione ..... » 598

INTRODUZIONE

L'orizzonte dell'opera è quello di un'analisi sistematica della disciplina in tema di protezione e libera circolazione dei dati personali e della loro *governance*, in una prospettiva che mira a coniugare i diversi formanti del diritto, da quello normativo a quello dell'elaborazione dottrinale e istituzionale a quello dell'applicazione casistica per mano delle autorità competenti a *jus dicere*, giurisprudenziali e "para-giurisprudenziali".

La protezione dei dati personali s'è da tempo affermata come diritto fondamentale delle persone fisiche, con un percorso inarrestabile che, dall'ottocentesca affermazione del *right to privacy* come *right to be let alone* (dovuta all'elaborazione teorica di Samuel Warren e Luis Brandeis, consacrata nel celeberrimo saggio affidato alla *Harvard Law Review* nel 1890) è giunta fino all'espressa cristallizzazione del "diritto alla protezione dei dati personali" nell'art. 8 della Carta dei Diritti Fondamentali dell'Unione europea. L'ottica è stata quella di tutelare le persone fisiche dai rischi che incombono sui loro diritti e libertà fondamentali a seguito dei trattamenti di dati a loro riferibili, assicurando al contempo la libera circolazione di tali dati, per fini di mercato, per fini istituzionali e per realizzare altre libertà, incluso quelle legate allo svolgimento dell'attività economica e, comunque, di natura privatistica (e qui rimando, più diffusamente, a F. Bravo, *Il "diritto" di trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018).

La contrapposizione tra tutela della persona di fronte al trattamento dei dati e tutela della loro libera circolazione per il raggiungimento di finalità legittime e determinate ha portato a delineare una normativa volta a fissare il difficile punto di equilibrio tra esigenze contrapposte, ora soggetta a profondo ripensamento da parte delle istituzioni eurounitarie, per via della necessità di cogliere nuove opportunità mediante la nuova dimensione della *governance* dei dati.

L'approccio è stato ridelineato nella Comunicazione della Commissione europea sulla *European Strategy for Data*, resa nel febbraio 2020, poco dopo la definitiva applicazione del GDPR (Reg. EU 2016/679), seguita dall'emanazione del Regolamento sulla *governance* dei dati (*Data Governance Act*), entrato in vigore nel 2022 (Reg. UE 868/2022), nonché dalla *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*, del febbraio del 2022 [COM/2022/68 final] e dalla *Proposal for a Regulation on the European Health Data Space* (EHDS), del maggio 2022 [COM(2022) 197 final], destinate a riscrivere ulteriormente le regole in tale tormentata materia, già segnata da numerosi provvedimenti delle Autorità di controllo e da documenti interpretativi dell'EDPB

(*European Data Protection Board*) e dell'EDPS (*European Data Protection Supervisor*).

Si vede bene la linea di sviluppo della materia, volta a creare un *framework* giuridico per consentire una più facile utilizzabilità o ri-utilizzabilità dei dati, per esigenze diverse, incluse quelle di mercato e quelle istituzionali di matrice giuspubblicistica, che, nella visione antropocentrica voluta dall'UE, non possono tralasciare il punto di iniziale approdo del ragionamento giuridico: la salvaguardia delle ineliminabili esigenze di tutela dei diritti e della libertà fondamentali della persona fisica di fronte al trattamento dei dati personali che la riguardano.

In questa prospettiva, protezione dei dati, libera circolazione dei dati e *governance* dei dati rappresentano le direzioni di un crocevia che costituisce il punto di intersezione su cui l'ordinamento giuridico europeo e quelli nazionali dei singoli Paesi membri concentreranno i loro sforzi nei prossimi decenni, nella nuova e rivoluzionaria prospettiva offertaci dal progresso tecnologico, che in questi anni ha raggiunto traguardi enormi. Si tratta di traguardi costituiscono non certo il punto di arrivo, ma un trampolino per gli ulteriori sviluppi di tecnologie che pervasive, inclusa l'intelligenza artificiale, in una società ed in un'economia sempre più "datificate", in tutti i settori, sia pubblici che privati.

Si impone, nell'anno del rilancio eurounitario delle iniziative legislative per il ripensamento della disciplina giuridica sui dati personali vocato al mercato digitale e all'uso (o riuso) anche istituzionale dei dati per favorire nuove prospettive di sviluppo, un riesame critico della disciplina che ruota attorno a tale crocevia, che va rimeditata profondamente, dalle base e dai principi, in una visione prospettica, per essere poi analizzata nel dettaglio anche negli aspetti più innovativi.

Ecco allora che si comprende il contesto in cui si colloca il lavoro condotto con il Gruppo di Ricerca «*Data Protection Law*», da me coordinato, collegato con il Corso di Alta Formazione in *Privacy* e *Data Protection Officer* dell'Università di Bologna (https://site.unibo.it/dpo), di cui ho l'onore di essere Direttore. L'attività di ricerca si inserisce anche nell'ambito dell'analisi svolta presso l'Università di Bologna all'interno del Progetto PNRR NextGenerationEU, GRINS (Growing Resilient, INclusive and Sustainable), EP09, Spoke0, con particolare riferimento ai temi della *data governance* e della *data protection* relativi alla realizzazione di una *data platform* di amplissime dimensioni, destinata alla raccolta ed alla condivisione dei risultati delle attività di ricerca.

Il presente volume, che si colloca nell'ambito di un progetto di riflessione sistematica di più ampio respiro dai confini sopra richiamati, mira a tracciare una riflessione sui principi in materia di protezione dei dati personali, con attenzione anche ai nuovi *European Digital Rights and Principles*, destinati a riscrivere i valori della *Digital Society and Economy* del nuovo millennio, e alla disciplina della libera circolazione dei dati e della *data governance*.

Il capitolo iniziale, a mia firma, offre una lettura critica di inquadramento, con portata di carattere generale e sistematica, sui "principi" in materia, analizzati

anche in funzione prospettica nelle loro connessioni sia con i nuovi principi e diritti digitali, sia con la necessaria aderenza alla casistica concreta («*I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, alla luce delle* rules of construction»).

Gli ulteriori dodici capitoli del volume sono dedicati, invece, all'analisi dei singoli principi rilevanti in materia di protezione dei dati personali, rinvenibili dalla lettura del GDPR, siano essi "inscritti" o meno nel suo art. 5, par. 1 e 2. Così l'analisi è dedicata, rispettivamente, a «*Il principio di liceità*», «*Il principio di correttezza*», «*Il principio di trasparenza*», «*Il principio di limitazione delle finalità*», «*Il principio di minimizzazione dei dati*», «*Il principio di esattezza*», «*Il principio di limitazione della conservazione*», «*Il principio di integrità e riservatezza (*rectius*, di sicurezza)*», «*Il principio di necessità*», «*Il principio di proporzionalità*», «*Il principio di* privacy by design e by default» e «*Il principio di responsabilizzazione (*accountability*)*». Il capitolo finale – il quattordicesimo – è invece dedicato a «*Il principio di solidarietà*», visto nella sua più ampia collocazione tra *data protection*, libera circolazione dei dati e *data governance*. Per ciascuno di tali tredici capitoli s'è scelto di seguire una linea di riflessione strutturata in maniera tripartita, prestando di volta in volta attenzione, in corrispondenza di ciascun capitolo, sia all'iniziale inquadramento normativo, sia alla portata applicativa del principio ricavabile dalla lettura critica del dibattito dottrinale e delle fonti istituzionali, sia, infine, alla disamina dell'applicazione del principio nella casistica concreta, mediante l'esame dei provvedimenti delle autorità intervenute a decidere le questioni dipanatesi nella fattispecie concreta. L'idea è quella di offrire una prospettiva di analisi attenta anche al diritto vivente, in un'opera che non ha precedenti nella letteratura di settore, dato che nessun volume, finora, è stato mai interamente dedicato ai principi in materia di protezione dei dati personali.

Ripercorrendo in maniera sistematica e approfondita tali principi, singolarmente analizzati, s'è dunque voluto costruire una solida base di riflessione per interpretare meglio lo *ius condito* e lo *ius condendo* in tale specifica materia, segnata, oggi più che mai, da evoluzioni vorticose che tracciano una direzione non ancora ben delineata nei contorni specifici. Sarà compito dell'interprete plasmare il diritto in evoluzione, ma è un compito che deve essere assolto camminando giorno per giorno lungo una strada che si sta facendo impervia. E l'interprete deve procedere – come gli illustri Maestri ci hanno insegnato – con sguardo sempre attento a quei "principi" che costituiscono, al contempo, faro illuminante e sostegno sicuro di ogni viaggio che si vuole intraprendere nei meandri del diritto.

FABIO BRAVO

PREFAZIONE

Riguardata sotto il profilo delle fonti, la disciplina dei dati personali presenta una situazione complessa. Essa è ben diversa da quella iniziale che si limitava a scindere le fasi del trattamento e a rendere applicabile l'art. 2050 c.c. all'attività di raccolta, conservazione e trattamento dei dati contenuta nell'art. 15 del d.lgs. 30 giugno 2003, n. 196. Con il tempo si è passati ad una articolata normazione, che prevede un regolamento (GDPR, Reg. UE n. 679/2016) che articola le diverse fasi del processo di utilizzazione dei dati, le condizioni per la loro commercializzazione, e per il loro trasferimento al di fuori dei confini dell'Unione, accompagnato da un decreto legislativo del 10 agosto *2018*, n. 101 che ha coordinato il Regolamento con le norme del diritto interno. Non solo. Ogni fase richiede una attenta valutazione dei termini impiegati, e l'affinamento dei concetti che la dottrina aveva faticosamente elaborato nel corso di mezzo secolo, dall'opera profetica e pionieristica di Stefano Rodotà sugli elaboratori elettronici.

Coordinare le fonti ed assegnare loro un significato univoco non è operazione semplice. Di qui il merito dell'opera che si presenta, che deve all'attenta e paziente ricerca di Fabio Bravo un così apprezzabile risultato.

Al fine di orientare l'interprete nell'insidioso sentiero delle fonti Fabio Bravo e gli altri Autori del libro hanno organizzato l'intera materia sulla base dei principi che essa sottende: si tratta dei principi di liceità, di correttezza, di trasparenza, di limitazione delle finalità, di minimizzazione dei dati, di esattezza, di limitazione della conservazione, di sicurezza, di necessità, di proporzionalità, di *privacy by design* e *by default*, di responsabilizzazione, di solidarietà.

L'organizzazione per principi consente all'interprete di individuare subito i valori che la disciplina esprime e le sue finalità: un principio, inteso in questo senso, è appunto una norma di secondo grado ricavata con processo induttivo da disposizioni dettagliate e particolari, per giungere alla formulazione di una disposizione più generale che tutte le ricomprende e per tutte costituisce il punto di avvio del processo ermeneutico.

Dalla griglia dei principi si può intendere l'intreccio dei problemi, la cui soluzione è affidata all'analisi del testo, alla critica della dottrina, all'esame della sua applicazione da parte della giurisprudenza.

La redazione di un testo analitico quale quello emergente dal GDPR con le sue regole minuziose e con la lista dei significati tecnici dei termini impiegati – un glossario che, inserito nel testo, raccoglie definizioni aventi natura normativa – dovrebbe assicurare una armonizzazione di livello elevato. Di qui il prezioso sussidio degli Autori che è riuscito a semplificare il lavoro complesso dell'interprete. E di ciò siamo davvero grati al coordinatore e ad ognuno di loro.

GUIDO ALPA

Capitolo I

I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, nel solco delle *rules of construction*

Fabio Bravo

SOMMARIO: 1. Stefano Rodotà, i principi in materia di protezione dei dati personali e la «riscrittura delle tavole dei valori» nel contesto tecnologico. – 1.1. La funzione adeguatrice dei principi. – 1.2. La funzione ordinante dei principi e la composizione degli interessi in gioco. – 1.3. Principi e tecnica legislativa. – 1.4. Dai principi in materia di protezione dei dati personali all'*Internet Bill of Rights* e l'enfasi sulla necessità di una «riscrittura delle tavole dei valori». – 2. L'affermazione dei principi nel GDPR. – 3. Prospettive ed obiettivi della ricerca sull'applicazione dei Principi del GDPR. – 4. Dalla protezione dei dati personali al diritto a trattare dati personali. La collocazione dei principi del GDPR nel panorama più esteso dei nuovi *Digital Rights and Principles.* – 5. La "riscrittura" della tavola dei valori ad opera dell'UE: la nuova «*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*». – 5.1. Il solco tracciato da Stefano Rodotà e la "riscrittura" della tavola dei valori ad opera della Commissione europea. La Comunicazione «relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali» [COM(2022)27 *final*]. – 5.2. L'asserita (ma illusoria) natura meramente politica della Dichiarazione europea sui diritti e sui principi digitali. – 5.3. La «*European Declaration on Digital Rights and Principles for the Digital Decade*» (2023/C 23/1). – 5.4. Mettere le persone al centro della trasformazione digitale. – 5.5. Solidarietà e inclusione (connettività, condizioni di lavoro, istruzione, formazione e competenze digitali, condizioni di lavoro giuste ed eque, servizi pubblici digitali *online*). – 5.6. Libertà di scelta (interazioni con algoritmi e sistemi di intelligenza artificiale, un ambiente *online* equo). – 5.7. Partecipazione allo spazio pubblico digitale. – 5.8. Sicurezza, protezione ed *empowerment* (un ambiente digitale sicuro, protetto e tutelato, vita privata e controllo individuale sui dati, protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale). – 5.9. Sostenibilità. – 6. Una lettura circolare: dai *Digital Principles* ai principi in materia di protezione dei dati personali. – 6.1. La circolarità del discorso. – 6.2. Verso una "costituzionalizzazione" dei nuovi diritti e principi digitali. – 6.3. L'embrionale fase di "riscrittura" dei nuovi diritti e principi digitali e prospettive di successivo ampliamento. – 6.4. Nuovi diritti e principi digitali e trattamento di dati personali. – 6.5. Valenza "interna" ed "esterna" dei principi in materia di protezione dei dati personali. – 6.6. Funzioni e caratteristiche dei principi in materia di protezione dei dati personali. "Principi-valore" e "principi-funzionali". – 6.6.1. La scelta sistematica del legislatore europeo: i principi nel GDPR. – 6.6.2. La funzione dei principi in materia di protezione dei dati personali e l'aderenza diretta e indiretta al piano assiologico: "principi-valore" e "principi-funzionali". – 6.6.3. (segue) L'individuazione dei "principi-valore" e "principi-funzionali" nel GDPR. – 6.6.4. Importanza ed opportunità della "rilettura" dei principi alla luce del diritto vivente, nonché dell'individuazione e della ricostruzione sistematica delle *rules of construction* ad essi riferibili.

1. STEFANO RODOTÀ, I PRINCIPI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E LA «RISCRITTURA DELLE TAVOLE DEI VALORI» NEL CONTESTO TECNOLOGICO

1.1. La funzione adeguatrice dei principi

Un anno prima che, con la l. 675/96, entrassero per la prima volta in vigore nel nostro ordinamento le norme di matrice comunitaria in materia di protezione dei dati personali, sulle pagine di *Tecnologie e diritti*, per i tipi de Il Mulino, Stefano Rodotà rimarcava l'importanza dei *principi*, quale meraviglioso antidoto contro l'obsolescenza delle soluzioni giuridiche riferite alla tecnologia, che inarrestabile muove passi troppo veloci rispetto al più lento incedere del diritto[1].

Rodotà avvertiva che «la nuova angoscia nasce dalla consapevolezza dello scarto assai forte tra la rapidità del progresso tecnico-scientifico e la lentezza con cui matura la capacità di controllo dei processi sociali che a quel progresso si accompagnano. Ed è proprio su questo terreno che bisogna lavorare, per colmare lo scarto, analizzando in tutta la loro complessità i processi in corso, progettando politiche consapevoli, mettendo a punto rimedi istituzionali»[2], ma ammoniva anche che «Questo lavoro (…) si risolve spesso in un affannoso e vano inseguimento delle novità tecnologiche. Talvolta, anzi, si ha la sensazione che cresca la distanza tra il mondo velocissimo dell'innovazione tecnologica e quello lentissimo della progettazione

[1] S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, pp. 41 ss. L'importanza di una "legislazione per principi" era stata dall'A. messa in evidenza, molti anni prima, in ID., *Ideologie e tecniche della riforma del diritto civile*, prolusione tenuta all'Università di Macerata nel dicembre 1966, pubblicata in *Riv. dir. comm.*, 1967, pp. 83 ss.
Ai principi la dottrina ha dedicato molta attenzione. Si ricordano, tra tutti, gli studi di E. BETTI, *L'interpretazione della legge e degli atti giuridici*, Milano, 1949; V. CRISAFULLI, *La Costituzione e le sue disposizioni di principio*, Milano, 1952; G. DEL VECCHIO, *Sui principi generali del diritto*, Milano, 1958; N. BOBBIO, *Principi generali di diritto*, in *Noviss. dig.it.*, XIII, Torino, 1966; R. DWORKIN, *I diritti presi sul serio*, Bologna, 1976; S. BARTOLE, *Princìpi generali del diritto (dir. cost.)*, in *Enc dir.*, XXXV, 1986, pp. 494 ss.; L. MENGONI, *Spunti per una teoria delle clausole generali*, in *Riv. crit. dir. priv*., 1986, pp. 5 ss.; S. RODOTÀ, *Il tempo delle clausole generali*, in *Riv. crit. dir. priv.*, 1987, pp. 709-733; A. BELVEDERE, *Le clausole generali tra interpretazione e produzione di norme*, in *Politica del diritto*, 1988, pp. 631-653; G. TARELLO, *Cultura giuridica e politica del diritto*, Bologna, 1990; F. MODUGNO, *Principi generali dell'ordinamento*, in *Enc. giur.*, XXIV, Treccani, Roma, 1991; G. ALPA, *I principi generali*, in *Trattato di diritto privato*, a cura di G. IUDICA e P. ZATTI, 2ª ed., Milano, 2006 (1ª ed., 1993); P. RESCIGNO, *Appunti sulle "clausole generali"*, in *Riv. dir. comm.*, 1998, pp. 1-8; R. GUASTINI, *Principi del diritto e discrezionalità giudiziale*, in *Diritto Pubblico*, 1998, 3, p. 651 ss.; V. VELLUZZI, *Osservazioni sulla semantica delle clausole generali*, in *Etica e politica*, 2006, 1, pp. 1 ss. (e, successivamente, V. VELLUZZI, *Le clausole generali. Semantica e politica del diritto*, Milano, 2010); F.D. BUSNELLI, *La «danza dei principi»: diritto naturale, diritto positivo, bioetica* in G. ALPA-V. ROPPO (a cura di), *Il diritto privato nella società moderna. Seminario in onore di Stefano Rodotà*, Napoli, 2005, pp. 223 ss.; L. NIVARRA, *Clausole generali e principi generali del diritto nel pensiero di Luigi Mengoni*, in *Eur. e dir. priv.*, 2007, 2, pp. 411-446; VETTORI, *Regole e principi. Un decalogo*, in *Nuova giur. civ. comm.*, 2016, 1, pp. 124 ss.; C. CAMARDI, *Brevi riflessioni sull'argomentazione per principi nel diritto privato*, in *Riv. dir. civ.*, 2017, 5, pp. 1130 ss.

[2] S. RODOTÀ, *Tecnologie e diritti*, cit., p. 42.

socio-istituzionale. Quasi in ogni momento si coglie la rapida obsolescenza delle soluzioni giuridiche riferite ad un solo dato tecnico o ad un solo problema. Si avverte così la necessità di individuare i principi, di riferirli a tendenze di lungo periodo. Questo, certamente, è l'insegnamento che viene da una riflessione sul primo periodo di progettazione e di applicazione delle leggi relative al trattamento elettronico delle informazioni»[3].

In questa prospettiva, i principi hanno una *funzione*, per così dire, "*adeguatrice*", nel senso che consentono all'interprete, chiamato ad applicare le norme in ambito tecnologico – incluse quelle in materia di protezione dei dati personali –, di adeguare la portata della norma alla mutevolezza imposta dal progresso della tecnica e, dunque, di fornire una risposta cangiante nel tempo, soprattutto in una prospettiva di lungo (ma anche di medio) periodo, per fornire calzanti risposte alle istanze sociali ed economiche, che mutano con l'evolversi della tecnologia a cui siamo costantemente esposti[4].

1.2. La funzione ordinante dei principi e la composizione degli interessi in gioco

La straordinaria duttilità dei principi rendono il ricorso a questi ultimi assai prezioso, perché sono in grado di avere una portata ordinante di fronte ad una complessità che è difficile da prevedere e gestire *ex ante*, in via di emanazione delle regole giuridiche che dovrebbero governare la fattispecie, sicché appare preferibile rimettere all'interprete, chiamato ad applicare il diritto, l'individuazione e l'applicazione della norma nel caso concreto, poggiandosi sulle solide e ampie basi offerte proprio dai principi. Anche su tale aspetto non è mancata la riflessione di Rodotà, là dove ha evidenziato che «Le difficoltà nella ricerca di questi principi non derivano solo dal fatto che si tratta di regolare una realtà in continuo mutamento. Nascono pure dalla necessità di fare i conti con una molteplicità di esigenze, interessi, valori, spesso tra loro confliggenti. E pure questo è un effetto delle nuove tecnologie, del loro essere pervasive delle più diverse attività, dal fatto che investono trasversalmente i più diversi settori»[5].

In questa seconda prospettiva i principi hanno una *funzione ordinante*, di fronte alla complessità, *e di propulsione per il bilanciamento* tra contrapposti interessi in gioco, che, proprio con il ricorso ai principi, possono essere più efficacemente composti da chi è chiamato all'applicazione delle norme, pur trovandosi di fronte all'intersezione di valori fondamentali da contemperare, in attrito tra loro.

---

[3] S. RODOTÀ, *Tecnologie e diritti*, cit., p. 42.

[4] Sulla funzione dei principi, che la dottrina riconduce sostanzialmente a quella normativa, quella interpretativa e quella integrativa, la letteratura è vasta. Si rimanda più approfonditamente, per un sapiente ed esaustivo inquadramento, unito ad una rilettura critica che esplora anche altre differenti funzioni, l'opera di G. ALPA, *I principi generali*, cit., pp. 17 ss.

[5] S. RODOTÀ, *Tecnologie e diritti*, cit., p. 42.

1.3. Principi e tecnica legislativa

Sulla scorta di tali considerazioni, ricorda l'insigne giurista, non si può ignorare l'importanza della «*tecnica legislativa* adoperata. Oggi, poiché l'esperienza del passato mostra la rapida obsolescenza delle discipline troppo rigide e sposta l'attenzione su interventi istituzionali forniti di una elevata flessibilità, si può proporre che l'ambiente giuridico favorevole ad una adeguata disciplina della circolazione delle informazioni sia caratterizzato dai seguenti elementi: *a)* una disciplina legislativa di base, costituita essenzialmente da "*clausole generali*" e da norme procedurali; *b)* norme particolari, possibilmente contenute in leggi autonome, riguardanti l'attività di particolari soggetti o la disciplina di particolari categorie di informazioni; *c)* un'autorità amministrativa indipendente, eventualmente dotata di poteri di adattamento dei *principi contenuti nelle clausole generali* a situazioni particolari; *d)* una disciplina del ricorso all'autorità giudiziaria, non solo nei sistemi in cui ciò è richiesto da norme costituzionali, ma in via generale, per radicare anche in questa materia principi analoghi a quelli di un *Bill of Rights* o del *Due Process*, secondo la linea che tende ad avvicinare la materia qui considerata a quella dei diritti civili; *e)* la previsione di un controllo diffuso, affidato alla iniziativa di singoli e di gruppi»[6].

Seguendo tale impostazione, che poi è quella riscontrabile negli anni a venire nell'ordinamento europeo e in quello nazionale, Rodotà intravedeva la strategia istituzionale per favorire, attraverso il giusto equilibrio tra i diversi elementi, quanto necessario per governare in maniera efficace e flessibile i mutevoli assetti che la società e l'economia presentava al cospetto dei continui mutamenti dettati dall'innovazione tecnologica.

In materia di protezione dei dati personali l'assetto maturo, delineatosi con l'avvento del Reg. UE 679/2016 (*General Data Protection Regulation*, GDPR), espone con forza la legislazione per *principi*, individuati all'art. 5, seguita da disposizioni normative particolari, ovvero dalle "regole" giuridiche in cui si articola la disciplina di dettaglio.

1.4. Dai principi in materia di protezione dei dati personali all'*Internet Bill of Rights* e l'enfasi sulla necessità di una «riscrittura delle tavole dei valori»

V'è poi un'ulteriore considerazione che Stefano Rodotà prospettava nelle sue richiamate pagine, in cui guardava alla necessità di misurarsi nuovamente con i valori di fondo, di cui i principi sono espressione: la norma, racchiusa nel principio, non è mai scollegata dal valore che essa esprime, ma di fronte all'evoluzione socio-economica e istituzionale imposta dalla tecnologia occorre pur sempre rimisurare i valori di riferimento, se necessario ripensarli o declinarli nuovamente, con le peculiarità che i mutamenti intervenuti richiedono. Così, sempre in *Tecnologie e diritti*, rimarcava l'inadeguatezza della «linea della *deregulation* e del mercato»[7], così come della prospettiva legata al solo «rafforzamento delle difese individuali "passive", fatte di divieti di raccolta di determinate informazioni e di diritti "indisponibili" sot-

[6] S. RODOTÀ, *Tecnologie e diritti*, cit., pp. 95 s. (mie le enfasi in corsivo).
[7] S. RODOTÀ, *Tecnologie e diritti*, cit., p. 61.

tratti alle transazioni consensuali»[8], affermando invece con forza che «Siamo (…) di fronte alla necessità di stabilire quale debba essere il quadro dei principi fondamentali a cui far riferimento nella situazione mutata, non che cosa possa sopravvivere, in modo più o meno precario, del vecchio assetto istituzionale. L'età dell'informazione richiede anche una *riscrittura delle tavole dei valori*, proprio per garantire una piena espansione di quelli che riassuntivamente indichiamo con i termini di libertà e di democrazia»[9].

Il ripensamento e la riscrittura delle tavole dei valori in rapporto alle nuove tecnologie porterà successivamente Stefano Rodotà nel percorso di ricerca che lo ha indotto ad avanzare, decenni più tardi, la celebre e discussa proposta di modifica della Costituzione italiana, con l'introduzione dell'art. 21-*bis* («Tutti hanno eguale diritto di accedere alla Rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale»)[10], nonché, più recentemente, la proposta di introduzione di una vera e propria *Internet Bill of Right*, una Carta di diritti fondamentali per Internet[11], curata dallo stesso Rodotà e poi approdata alla Camera dei Deputati nel 2014 e nel 2015, nella veste della «*Dichiarazione dei diritti in Internet*»[12].

---

[8] S. Rodotà, *Tecnologie e diritti*, cit., p. 61. Ivi l'A. aggiunge che «Tutto questo rimane necessario, certamente: ma come un punto di partenza, non d'arrivo».

[9] S. Rodotà, *Tecnologie e diritti*, cit., pp. 60-61.

[10] La modifica della Carta costituzionale è stata ritenuta da diverse voci superflua di fronte all'ampio tenore dell'art. 21 Cost., ovvero dalla possibilità di lettura congiunta dell'art. 21 con l'art. 15 Cost., oltre che per la rilevanza dell'art. 3, co. 2, Cost., in ordine alla rimozione degli ostacoli di ordine economico e sociale per promuovere l'uguaglianza sostanziale tra i cittadini. Tra le voci critiche alla proposta di Stefano Rodotà si vedano, ad es., L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, 2012, 2-3, p. 283 ss.; R. Zaccaria, *Dal servizio pubblico al servizio universale*, in L. Carlassare (a cura di), *La comunicazione del futuro e i diritti delle persone*, Padova, 2000, pp. 12 ss.

[11] Si veda S. Rodotà, *Una Costituzione per Internet?*, in *Politica del diritto*, 2010, 3, pp. 337-351.

[12] Il testo è stato elaborato dapprima nel 2014 dalla «*Commissione per i diritti e i doveri in Internet*» costituita presso la Camera dei deputati (si veda *Il testo della dichiarazione dei Diritti di Internet*, in quattordici punti, pubblicato in bozza su http://www.rainews.it/archivio-rainews/articoli/Dichiarazione-dei-Diritti-di-Internet-Il-testo-0eafe894-2d2c-4c39-a2c4-f94e52416cc1.html consultato, da ultimo, in data 30 luglio 2022). Il nuovo testo della Dichiarazione, del 14 luglio 2015, è stato poi elaborato dalla Commissione per i diritti e i doveri relativi ad Internet a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione. Il documento è consultabile anche sul sito del Ministero dell'Interno all'url https://www.interno.gov.it/sites/default/files/allegati/dichiarazione_dei_diritti_internet_pubblicata.pdf (consultato, da ultimo, in data 30 luglio 2022). Il nuovo testo della Dichiarazione è stato presentato il 28 luglio 2015 alla Camera dei Deputati dall'allora presidente Laura Boldrini, alla presenza di Stefano Rodotà.
In un comunicato del 28 luglio 2015 presente sul sito del Ministero dell'Interno, intitolato «*Dichiarazione dei diritti in Internet, per una nuova cittadinanza sulla rete*» (reperibile *online* all'url https://www.interno.gov.it/it/notizie/dichiarazione-dei-diritti-internet-nuova-cittadinanza-sulla-rete consultato, da ultimo, in data 30 luglio 2022) –, si legge che «Dopo la consultazione pubblica lanciata lo scorso ottobre per assicurare la partecipazione più larga possibile all'individuazione dei principi da tutelare, è stata presentata oggi alla Camera dei deputati dalla Presidente Laura Boldrini, il nuovo testo della "Dichiarazione dei diritti in Internet". Una Commissione formata da parlamentari ed esperti del settore ha lavorato insieme, producendo una "sintesi" tra le diverse sensibilità in materia. La Presidente, illustrando il documento, ha sottolineato, in particolare, il contenuto degli articoli 2

In tale documento si trovano enunciati in quattordici articoli i diritti, le libertà e i principi da applicare con riferimento a Internet, sia per la tutela dei soggetti che operano tramite la Rete, sia per assicurare il funzionamento democratico delle istituzioni[13]. La Dichiarazione si colloca nella prospettiva – declinata nel Preambolo – di evitare «il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale», tenendo conto che «Internet si configura come uno spazio sempre più importante per l'autorganizzazione delle persone e dei gruppi e come uno strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e l'eguaglianza sostanziale. I principi riguardanti Internet tengono conto anche del suo configurarsi come uno

e 3: l'accesso ad Internet rappresenta un diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale. E l'aspetto della conoscenza ed educazione in rete: per questo, le istituzioni pubbliche promuovono attraverso il sistema dell'istruzione e della formazione, l'educazione all'uso consapevole di Internet e intervengono per rimuovere ogni forma di ritardo culturale che precluda o limiti l'utilizzo di Internet da parte delle persone.
Prossimo obiettivo annunciato dalla Boldrini, la presentazione di una mozione unitaria perché i principi inseriti in questa Dichiarazione siano promossi dal Governo nelle sedi internazionali.
Alla presentazione è intervenuto anche il professor Stefano Rodotà che ha evidenziato come siano troppe le limitazioni e le regole prodotte per la rete che ha bisogno, invece, di principi in prospettiva. Questa "Dichiarazione" si pone l'obiettivo anche di contribuire a costruire una "cittadinanza" nell'era di internet».

[13] La terminologia usata dalla Commissione europea, che si riferisce genericamente, nella Dichiarazione, sia a diritti che a principi digitali, impone un chiarimento sul rapporto tra gli uni e gli altri. Al riguardo C. CAMARDI, *Brevi riflessioni sull'argomentazione per principi nel diritto privato*, cit., par. 4, ha ricordato che «(…) strutturalmente i principi sono regole di comportamento ad ampio "spettro" di applicazione, non sono fattispecie (puntuali), non sono nemmeno regole generali (a fattispecie più ampia); si ricavano induttivamente da un insieme di regole particolari; ma derivano anche da enunciati espliciti spesso identificando in tal modo taluni principi supremi e/o fondativi della identità di un ordinamento e perciò talora nemmeno rivedibili in sede di procedimento di revisione costituzionale. Tanto per dire che già il semplice uso del termine "principio" allude a regole giuridiche di differente valore assiologico e pratico e a contesti operativi differenti sul piano della interpretazione. Strutturalmente i diritti fondamentali, invece, non sono regole di comportamento. Essi delineano una situazione giuridica di protezione tendenzialmente assoluta che reclama tutela di fronte all'interferenza altrui e rimedi effettivi in garanzia. Essi impongono spesso perciò obblighi di astensione o divieti di comportamenti, ai terzi come allo Stato, e stabiliscono una sfera di intangibilità di esclusiva pertinenza del titolare del diritto (tipicamente la dignità, o le modalità della propria vita personale o familiare). Ovvero includono anche una situazione attiva per realizzare la quale il titolare è provvisto di una specifica pretesa (il diritto di circolare e stabilirsi in ogni stato membro). Ovvero ancora conferiscono al titolare strumenti di difesa per contenere l'altrui interferenza quando questa sia giustificata da una norma di legge (i diritti esercitabili a fronte del trattamento consentito dei dati personali, o dei trattamenti medici). E così via, secondo le combinazioni che le varie generazioni di diritti rendono possibili.
Considerata in quanto tale, l'assimilazione tra principi e diritti fondamentali non è di per sé teoricamente improponibile. I principi includono "valori" e i diritti altrettanto, ma la corrispondenza valoriale non comporta che i due concetti possano esaurirsi l'uno nell'altro senza residui e ciò che resta fuori da tale parziale coincidenza è quanto basta per tenere ancora concettualmente distinte le due figure, quantomeno sul piano rimediale».
La connessione tra "principi" e "diritti fondamentali" è ampliamente esplorata da G. ALPA, *I principi generali*, cit., pp. 63 ss. ed è, del resto, in un chiaro senso di continuità con la tesi assiologica dei principi, che ha in Dworkin il principale riferimento.

spazio economico che rende possibile innovazione, corretta competizione e crescita in un contesto democratico».

In tale Dichiarazione emerge uno stretto legame tra diritto alla protezione dei dati personali e i nuovi diritti e principi fondamentali nella Rete, che rappresentano la "riscrittura" delle tavole dei valori nel senso indicato da Rodotà.

I quattordici articoli sono rispettivamente dedicati al «*Riconoscimento e garanzia dei diritti*» (art. 1), al «*Diritto di accesso*» (art. 2), al «*Diritto alla conoscenza e all'educazione in rete*» (art. 3), alla «*Neutralità delle rete*» (art. 4), alla «*Tutela dei dati personali*» (art. 5), al «*Diritto all'autodeterminazione informativa*» (art. 6), al «*Diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici*» (art. 7), ai «*Trattamenti automatizzati*» (art. 8), al «*Diritto all'identità*» (art. 9), alla «*Protezione dell'anonimato*» (art. 10), al «*Diritto all'oblio*» (art. 11), ai «*Diritti e garanzie delle persone sulle piattaforme*» (art. 12), alla «*Sicurezza in rete*» (art. 13) e, infine, al «*Governo della rete*» (art. 14). Viene offerta una regolamentazione essenziale, quanto a contenuti, che rimangono generali nella portata, ma specifici nella formulazione, tanto da essere "autoapplicabili" per la maggior parte, benché alcuni contenuti appaiano indirizzati in senso programmatico[14]. Si tratta comunque di diritti, libertà e principi volti a fissare i fondamenti delle garanzie *online*, in una società digitale animata da *bit*, aventi come presupposto di funzionamento il trattamento elettronico delle informazioni, incluso (inevitabilmente) quelle di natura personale. Si spiega l'intima e indissolubile connessione tra *data protection law* e diritti, libertà e principi pensati per il mondo digitale, indicati nella Dichiarazione dei diritti in Internet. È una connessione che emerge chiaramente nell'intero testo della Dichiarazione, tanti nell'articolato (che molto attinge dalla disciplina europea in materia di protezione dei dati personali)[15], quanto nel suo Preambolo.

Proprio in quest'ultimo si trova ben rimarcato che «(…) L'Unione europea è oggi la regione del mondo dove è più elevata la *tutela costituzionale dei dati personali*, *esplicitamente riconosciuta dall'articolo 8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet*, anche in una prospettiva globale». Del resto, come amava ricordare Stefano Rodotà, il diritto alla protezione dei dati personali è diritto fondamentale dell'uomo ma è anche esso stesso precondizione per l'esercizio di altri diritti fondamentali e la pregnanza di tale affermazione è ancor più forte là dove le interazioni avvengono di necessità attraverso operazioni informatiche su dati trattati in formato elettronico o digitale[16].

---

[14] In tema di norme "(auto)applicabili" cfr. C. Camardi, *Brevi riflessioni sull'argomentazione per principi nel diritto privato*, cit., pp. 11 ss.

[15] Si pensi, nel testo della Dichiarazione, ai riferimenti al diritto di accesso, al principio di trasparenza e a quello di autodeterminazione informativa, al diritto alla protezione dei dati personali, al diritto all'identità e al diritto all'oblio, al diritto all'anonimato e quello alla sicurezza, nonché al diritto alla protezione avverso i trattamenti automatizzati, e così via, tutti rinvenibili direttamente e indirettamente nella Dir. 95/46/CE, poi abroga, e nel Reg. UE n. 679/2016 (GDPR).

[16] Cfr. S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, in *Europa e diritto privato*, 2004, n. 1, p. 4, ove viene testualmente ribadito che «il rispetto del diritto

Il testo prosegue rimarcando che «Questa Dichiarazione dei diritti in Internet è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale. Internet si configura come uno spazio sempre più importante per l'autorganizzazione delle persone e dei gruppi e come uno strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e l'eguaglianza sostanziale.

I principi riguardanti Internet tengono conto anche del suo configurarsi come uno spazio economico che rende possibili innovazione, corretta competizione e crescita in un contesto democratico.

Una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale».

Del resto Rodotà aveva ricordato, nel suo contributo dedicato ad *Una costituzione per Internet?*, la significatività dell'«*Internet Bill of Rights*, una proposta maturata all'interno delle iniziative dell'ONU sulla società dell'informazione (…) che si è venuta consolidando attraverso il lavoro di diversi gruppi, *dynamic coalitions* spontanee e informali che hanno poi trovato forme di unificazione e metodi comuni, che si sono manifestati negli *Internet Governance Forum* promossi in questi anni proprio dall'ONU. Ma l'*Internet Bill of Rights* non è concepito, da chi lo ha immaginato e lo promuove, come una trasposizione nella sfera di Internet delle tradizionali logiche delle convenzioni internazionali e degli stessi percorsi di costituzionalizzazione finora conosciuti. La scelta dell'antica formula del *Bill of Rights* ha forza simbolica, mette in evidenza che non si vuole limitare la libertà in rete ma, al contrario, mantenere le condizioni perché possa continuare a fiorire. Per questo servono garanzie "costituzionali". Ma, conformemente alla natura di Internet, il riconoscimento di principi e diritti non può essere calato dall'alto. Deve essere il risultato di un processo, di una partecipazione larga di una molteplicità di soggetti che possono intervenire in modo attivo, grazie soprattutto ad una tecnologia che mette tutti e ciascuno in grado di formulare progetti, di metterli a confronto, di modificarli, in definitiva di sottoporli a un controllo e a una elaborazione comuni, di trasferire nel settore della regolazione giuridiche forme e procedure tipiche del "metodo *wiki*", dunque con progressivi aggiustamenti e messe a punto dei testi proposti. Siamo così al di là un altro schema tradizionale, che contrappone percorsi *bottom-up* a quelli *top-down*. Si instaurano relazioni tra pari, la costruzione diviene orizzontale. Nel corso di questo processo si potrà approdare a risultati parziali, all'integrazione tra codici di autoregolamentazione e altre forme di disciplina; a normative comuni per singole aree del mondo, come di nuovo dimostra l'Unione europea, la regione del pianeta dove più intensa è la tutela dei diritti; e come potrebbe avvenire per materie

alla protezione dei dati personali si configura come una *precondizione* per il pieno godimento di altri diritti fondamentali».

dove già è stata raggiunta una maturità culturale e istituzionale, come quella della protezione dei dati personali»[17].

2. L'affermazione dei principi nel GDPR

L'Unione europea ha colto, in materia di protezione dei dati personali, la via del ricorso ai principi come tecnica legislativa, declamandoli da ultimo nell'art. 5 GDPR, rubricato «*Principi applicabili al trattamento di dati personali*», ove si trova stabilito, al par. 1, che «I dati personali sono: *a)* trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("*liceità, correttezza e trasparenza*"); *b)* raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("*limitazione della finalità*"); *c)* adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("*minimizzazione dei dati*"); *d)* esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("*esattezza*"); *e)* conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("*limitazione della conservazione*"); *f)* trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("*integrità e riservatezza*")».

Al par. 2 del medesimo articolo si trova invece declinato un altro principio, quello di *accountability* (o di *responsabilizzazione*), là dove si afferma che «Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")».

Si tratta di un'enunciazione di principi applicabili in materia che, come auspicato da Stefano Rodotà, precedono le norme particolari di settore con le quali viene a realizzarsi una tecnica legislativa ben congegnata. Così, ad esempio, al principio di liceità di cui all'art. 5, par. 1, lett. *a)*, GDPR fanno seguito le regole sulle condizioni di liceità del trattamento enunciate agli artt. 6-10 GDPR. Al principio di trasparenza indicato nella medesima lett. *a)* cit. fanno seguito le norme di dettaglio sull'informativa di cui agli artt. 13 e 14 e quelle sul diritto di accesso di cui all'art. 15 ed altre. Al

[17] S. Rodotà, *Una Costituzione per Internet?*, cit., pp. 343 s. Sul "costituzionalismo" di Internet si vedano, più recentemente, anche le riflessioni di T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Dir. inf.*, 2020, 3, pp. 465-484.

principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. *f)*, fanno seguito le norme di dettaglio contenute all'art. 32, relativo all'obbligo di adozione delle misure di sicurezza, ed altre (si pensi, ad esempio, all'art. 35, relativo alla valutazione di impatto), così come al principio di responsabilizzazione di cui all'art. 5, par. 2, fanno seguito le disposizioni puntali di cui all'art. 24, anch'esso in tema di responsabilizzazione, ove il principio di carattere generale viene trasposto nella regola di dettaglio, che impone al titolare l'adozione di specifiche misure tecniche e organizzative per assicurare e dimostrare la *compliance* al GDPR. E così via.

Qui i principi valgono, nella loro portata ordinante, sia ad indicare la direzione entro cui si muovono le regole di dettaglio, sia a governarne la portata applicativa, in quanto l'applicazione delle norme di dettaglio viene ad essere orientata dall'interpretazione orientata secondo i principi ad essi corrispondenti. La portata ordinante dei principi va però ben oltre, perché essi consentono di individuare, mediante l'applicazione che ne fa l'interprete, la norma da applicare alla fattispecie concreta anche ove quest'ultima dovesse sfuggire alla regolamentazione offerta dalle norme particolari, anche ove fossero norme in cui sono contenute le regole specificamente dettate per fornire dettagli in ordine all'applicazione dei principi. Là dove non arrivano le regole di dettaglio contenute nelle norme particolari arrivano comunque i principi, che consentono all'interprete (es., al Garante o all'Autorità giudiziaria) di ricavare dal principio – in via interpretativa, appunto – la norma da applicare alla fattispecie concreta, pur in assenza di regole di dettaglio. In modo analogo, il principio, espresso in maniera ampia e generica, consente all'interprete di muoversi meglio di fronte ai mutamenti socio-economici e ai cambiamenti imposti dall'evoluzione tecnologica, fornendo all'interprete strumenti duttili e flessibili per applicare la norma alla fattispecie concreta, anche di fronte a scenari mutati, là dove le regole di maggior dettaglio potrebbero essere invece presto superate per via del fenomeno di obsolescenza delle disposizioni giuridiche, sopra richiamato.

Altri principi, invero, non sono declamati in apertura del GDPR, ma di essi se ne ha comunque traccia nel sistema e segnano ugualmente l'applicazione del diritto in materia di protezione dei dati personali. Così è, ad esempio, per il principio di necessità e, soprattutto, per il principio di proporzionalità, che non si presentano declinati in maniera puntuale nell'art. 5 GDPR. Talvolta si assiste ad una declinazione solamente per taluni aspetti peculiari, ma non dell'intero principio nella sua più ampia portata, come avviene ad esempio per il principio di necessità al cospetto dei declamati principi di "minimizzazione dei dati", di "limitazione delle finalità" e di "limitazione della conservazione". Altre volte, invece, sono presenti regole di dettaglio, ma non viene presentata l'enunciazione dello specifico principio ad esse corrispondenti: così, ad esempio, per le disposizioni particolari in materia di protezione dei dati sin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*), contenute nell'art. 25, rispettivamente al par. 1 e al par. 2, ove si fa riferimento all'obbligo per il titolare del trattamento di specifiche ulteriori misure tecniche ed organizzative da approntare in fase di delineazione dell'architettura del trattamento e per impostazione predefinita, senza tuttavia che vi sia l'affermazione esplicita del relativo principio di carattere generale, al di là dell'obbligo in questione.

In altre parole, la tecnica legislativa utilizzata per l'art. 25, in materia di *privacy by design* e *by default*, è diversa da quella utilizzata per l'art. 24, in materia di *ac-*

countability o *responsabilizzazione*: in quest'ultimo caso l'art. 24 contiene le regole di dettaglio che fanno seguito alla declamazione del principio contenuta nell'art. 5, par. 2, GDPR. Nel primo caso, invece, l'art. 25 contiene regole di dettaglio che non fanno seguito all'affermazione esplicita di un corrispondente principio, che tuttavia è considerato immanente nel sistema normativo, tant'è vero che alla *privacy by design* e *by default* come principio fa costante riferimento sia la dottrina, sia le istituzioni eurounitarie, sia infine il Garante per la protezione dei dati personali, nei provvedimenti in cui viene richiamato[18].

Vista l'importanza dei principi in tale materia, occorre evitare l'errore di tralasciare i principi inespressi. Occorre cioè concentrare l'attenzione e lo studio non solo su quelli enunciati *verbatim*, nell'art. 5 GDPR, ma anche sugli altri principi rilevanti in tale settore del diritto, ricavabili dal sistema normativo al di là delle scelte enunciative operate dal legislatore eurounitario.

3. Prospettive ed obiettivi della ricerca sull'applicazione dei Principi del GDPR

Accostarsi alla disciplina in materia di protezione dei dati personali attraverso la prospettiva di ricerca che mira a studiare i principi del GDPR consente opportunità di ricerca finora inesplorate, per lo meno a livello organico e sistematico.

L'approccio allo studio della materia viene generalmente condotto tramite l'analisi dell'intera disciplina normativa in materia di protezione dei dati personali o di singoli aspetti di essa.

Vista la funzione ordinante e adeguatrice dei principi e la capacità di fornire all'interprete, chiamato ad applicare il diritto nella fattispecie concreta, gli strumenti per orientare l'applicazione delle norme di settore, di colmare le loro eventuali lacune e di superare l'obsolescenza normativa delle disposizioni specifiche a fronte dell'imprevedibile evoluzione tecnologica, un'interessante prospettiva di ricerca è quella volta a studiare la disciplina analizzando tutti i principi rilevanti in tale settore del diritto, enunciati o meno dal legislatore, andando oltre la loro ricostruzione

[18] Quanto ai contributi dottrinali, anche prima dell'emanazione del GDPR non si esitava a parlare di «*privacy by design*» come "*principio*". Tra tutti si veda il contributo di U. Pagallo, *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in Gutwirth et al. (eds.), *European Data Protection: in Good Health?*, Springer, 2012. Tra i provvedimenti recenti del Garante che menzionano la *privacy by design* e *by default* come principio si rimanda, a titolo esemplificativo, a GPDP, Provv. 8 giugno 2023, doc. web n. 9921184 (verifica in ordine all'adeguamento di prescrizioni impartite dal Garante sul trattamento dei dati personali da parte dell'ISTAT), GPDP, Provv. del 24 marzo 2022, doc. web n. 9767057 (Parere su uno schema di decreto del Ministro dell'istruzione recante il regolamento sulle modalità di attuazione e funzionamento dell'Anagrafe Nazionale dell'Istruzione, ANIST), nonché a GPDP, Provv. 12 maggio 2022, doc. web n. 9778313 (Parere sullo schema di provvedimento del Direttore dell'Agenzia delle entrate recante "Accesso alla dichiarazione 730 precompilata da parte del contribuente e degli altri soggetti autorizzati" a partire dall'anno di imposta 2021) e, in tema di *privacy by design*, l'ordinanza ingiunzione resa da GPDP, provv. 24 marzo 2022, doc. web n. 9767635. Per l'aderenza della *data protection by design* e *by default* ai *principles* del GDPR si veda, infine, EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, vers. 2.0, adottate il 20 ottobre 2020.

normativa e il necessario inquadramento nel dibattito dottrinale ed istituzionale che ne hanno delineato la portata applicativa sul piano teorico, per andare ad analizzare come i singoli principi prendono forma nell'applicazione che di essi ne viene fatta al cospetto della fattispecie concreta, sul terreno della casistica, ad opera innanzitutto dell'autorità Garante per la protezione dei dati personali e, ove utile ai fini della ricostruzione del discorso, delle omologhe autorità straniere e dell'autorità giudiziaria.

Il diritto prende forma dall'applicazione che ne viene fatta nelle sedi deputate alla loro applicazione, secondo la prospettiva giusrealista[19], che vede nella "giurisprudenza" un vero e proprio formante del diritto[20], così come è formante del diritto anche la "para-giurisprudenza" espressa dalle *Authority* di settore chiamate a pronunciarsi sulla casistica concreta.

In questa prospettiva, obiettivo ultimo della ricerca – condotta presso l'Università di Bologna dal Gruppo di Ricerca in *Data Protection Law*, da me coordinato, collegato con il Corso di Alta Formazione in *Privacy e Data Protection Officer* affidato alla mia Direzione (https://site.unibo.it/dpo) –, è quello di analizzare l'effettiva rilevanza dei principi nell'applicazione concreta del diritto, verificando le modalità con cui le Autorità ricorrono ad essi nell'argomentazione giuridica e nella ricerca delle soluzioni rilevanti nella fattispecie concreta. Si vuole indagare come in concreto, da parte del diritto vivente, sia svolta la funzione "ordinante" e la funzione "adeguatrice" affidata ai principi rilevanti in materia di *data protection*.

4. Dalla protezione dei dati personali al diritto a trattare dati personali. La collocazione dei principi del GDPR nel panorama più esteso dei nuovi *Digital Rights and Principles*

La protezione dei dati personali è emersa come principio, nel panorama europeo, con l'affermazione del diritto alla protezione dei dati personali poi conclamato nell'art. 8 della Carta dei diritti fondamentali dell'UE. Si tratta di principio che ha acquisito una progressiva rilevanza, andando oltre le logiche protezionistiche a difesa dell'individuo dai rischi derivanti dal trattamento dei dati personali. È principio che colloca la persona al centro di un sistema di protezione e si può ben cogliere se si riflette sull'importanza strategica del diritto alla protezione dei dati personali rispetto ad altri principi o diritti della persona: pur essendo diritto fondamentale esso stesso è al contempo anche precondizione per l'esercizio di altri diritti fondamentali[21].

---

[19] Su giusrealismo e principi si veda G. ALPA, *I principi generali. Una lettura giusrealistica*, in *Riv. it. sc. giur.*, 2014, pp. 77 ss.

[20] Sui formanti del diritto cfr. R. SACCO, *Legal Formants: A Dynamic Approach to Comparative Law*, in *The American Journal of Comparative Law* (*Intallment I of II*), 1991, 39, 1, p. 1 ss. e ID., *Legal Formants: A Dynamic Approach to Comparative Law*, in *The American Journal of Comparative Law* (*Intallment II of II)*, 1991, 39, 2, p. 343 ss.

[21] S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, cit., p. 4.

Va poi considerato un altro importante aspetto. La disciplina di cui al GDPR e i principi in esso declinati seguono due direzioni, essendo rivolti sia alle esigenze di tutela delle persone fisiche di fronte al trattamento dei dati personali che le riguardano, sia alla libera circolazione di tali dati, tant'è che il diritto alla protezione dei dati personali oggetto di trattamento implica necessariamente anche il diritto al trattamento dei dati personali con cui il titolare legittimamente persegue finalità lecite e determinate, che ha dignità e rilevanza di diritto fondamentale[22]. Si tratta di due concomitanti "anime" della disciplina di settore[23], che non possono non essere messe a sistema, sia nella prospettiva del bilanciamento degli interessi[24], sia nella prospettiva della convergenza degli interessi in gioco che più di talvolta si presenta intorno alla medesima fattispecie di trattamento che lega il titolare e l'interessato[25].

Il diritto a trattare dati personali è espressione della libertà di circolazione dei dati, con cui si realizzano le finalità, determinate dal titolare – soggetto pubblico o privato – che sono alla base di ogni trattamento lecito. Sicché garantire la libertà fondamentale di trattare dati personali è, al contempo, garantire tutto ciò che legittimamente può essere perseguito tramite operazioni su dati, dalla libertà di espressione alla libertà di impresa, dall'azione istituzionale per la realizzazione di interessi collettivi alla realizzazione e allo sviluppo della propria personalità anche nei contesti sociali digitali in cui l'individuo si colloca, dalla libertà di ricerca e di insegnamento alla libertà di associazione, anche *online*, e così via.

C'è una stretta correlazione, oggi più di ieri, tra il (diritto al) trattamento di dati personali e i diritti digitali, perché se è vero che la disciplina sulla *data protection* prescinde dall'uso di strumenti elettronici di trattamento, potendosi applicare anche a trattamenti che vengono svolti con strumenti cartacei o comunque non informatizzati, è altrettanto vero che l'evoluzione tecnologica e la pervasività delle soluzioni che da essa ne sono scaturite per la società, le istituzioni e l'economia, comporta inevitabilmente che il trattamento dei dati personali ha il proprio terreno di elezione, nella prassi quotidiana, proprio nell'ambiente digitale, penetrato nelle nostre vite ormai in maniera capillare. Si pensi non solo all'uso dei *personal computer* ed ai *ta-*

---

[22] Sul diritto al trattamento dei dati personali si rimanda, *amplius*, a F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018.

[23] Il riferimento e a N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla* privacy, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 35 ss.

[24] F. Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 1, pp. 190-216.

[25] Non sempre la relazione tra gli interessi di cui sono portatore i protagonisti della fattispecie di trattamento (titolare e responsabile) è in posizione di conflitto. Talvolta è improntata alla convergenza. Si pensi, ad esempio, il paziente e il medico o il cliente dell'avvocato e l'avvocato medesimo o il cliente di una banca e l'istituto di credito che gli offre i servizi. In questi casi il trattamento dei dati personali viene ad essere posto in essere per finalità che realizzano interessi convergenti del titolare e dell'interessato, diversamente da quanto accade, ad esempio, dal trattamento effettuato dall'avvocato rispetto ai dati personali della controparte del proprio cliente, ove il conflitto tra gli interessi perseguiti dai soggetti protagonisti del trattamento impone di far leva sulle tecniche di bilanciamento per assicurare il proporzionale equilibrio tra i diversi diritti fondamentali in gioco, di rilevanza costituzionale. Per tale prospettiva di analisi e per le sue implicazioni si rimanda a F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit.

blet, ma anche agli *smartphone* ed alle *app*, all'*Internet of Things* (IoT), sia nella domotica che negli altri ambienti in cui viene sviluppato. Si pensi anche alle *smartTV* e allo *streaming* video anche per i canali televisivi tradizionali, si pensi inoltre agli altri elettrodomestici "intelligenti" come il forno ed il frigorifero, in grado di connettersi con *smatphone* e *tablet* e, più in generale, alla rete Internet. Anche il traffico telefonico viene spesso veicolato in ambiente ditale, ricorrendo ad *app* per le comunicazioni audio, video e per la messaggistica, com'è avvenuto con l'uso di *whatsapp*, ad esempio. Si pensi, più in generale, all'uso delle molteplici piattaforme digitali, con cui vengono svolte *online* anche quelle attività che, come per la teledidattica in tempo di *lockdown* imposto dalla pandemia per il Covid-19, tipicamente avvenivano senza l'intermediazione degli strumenti tecnologici. Si pensi ancora alla digitalizzazione del sistema giudiziario, con il processo civile telematico (PCT), e agli sviluppi della telemedicina, per non parlare dell'*Internet banking* e delle piattaforme di commercio elettronico e di *booking online*, ovvero, più in generale, del mercato unico digitale. Proprio sulle piattaforme *online* si sviluppano ambienti digitali in cui i singoli, le imprese, le istituzioni, interagiscono e svolgono la propria attività, a tal punto da rendere necessarie garanzie che preservino i diritti e le libertà fondamentali dei diversi soggetti che nel digitale hanno un inevitabile terreno di operatività.

Si pensi, ancora, agli inarrestabili progressi dell'intelligenza artificiale, con soluzioni pervasive e di grandissimo impatto per la società e per gli individui, sollevando questioni di non facile soluzione per il giurista[26].

Sorgono equilibri nuovi, per via dell'accentramento di poteri in capo a soggetti privati che controllano la tecnologia su cui tali attività vengono svolte e ciò rende chiaro, insieme ad altre considerazioni (quali ad esempio le esigenze di cybersicurezza e l'emersione di nuovi diritti in ambiente digitale, ed altro ancora), che l'approccio relativo alla tutela dei nuovi diritti digitali non può essere affatto quello della mera traslazione, nel digitale, dei soli diritti e delle sole libertà pensate per il tradizionale ambiente avulso dalla tecnologia, che ovviamente continuano a connotare anche l'ambiente digitale, ma che non appaiono di per sé sufficienti a governare i nuovi scenari tecnologici.

Siamo al cospetto di nuovi *Digital Rights* e di nuovi *Digital Principles*, che, sulla scia del pensiero di Stefano Rodotà, vanno individuati in aderenza alla tavola dei valori che connotano la società di riferimento e che, al cospetto dell'evoluzione tecnologica, va rimeditata e "riscritta", tenendo sempre a mente l'intima connessione

[26] Si veda, recentemente, il caso ChatGPT, affrontato dal Garante sia con il provv. n. 112 del 30 marzo 2023, doc. web n. 9870832, di limitazione provvisoria *ex* art. 58, par. 2, lett. f), GDPR, adottato nei confronti della società statunitense OpenAI L.L.C., che sviluppa e gestisce il predetto sistema di IA, sia con il successivo provv. n. 114 del 12 aprile, doc. web n. 9874702, con il quale, sospendendo il provvedimento di limitazione provvisoria, ha ingiunto una serie di prescrizioni volte a salvaguardare i diritti e le libertà fondamentali degli interessati al trattamento dei dati effettuato tramite ChatGPT. Proprio a seguito del caso affrontato dall'*Authority* italiana, l'EDPB ha attivato una specifica «*task force to foster cooperation and to exchange information on possible enforcement actions conducted by data protection authorities*» (EDPB, *EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT*, comunicato del 13 aprile 2023, disponibile *online* all'url https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en).

dei diritti e dei principi digitali con il diritto alla protezione dei dati personali e, come ho avuto modo di rimarcare, del diritto (o della libertà) a trattare dati personali.

5. La "riscrittura" della tavola dei valori ad opera dell'UE: la nuova «*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*»

5.1. Il solco tracciato da Stefano Rodotà e la "riscrittura" della tavola dei valori ad opera della Commissione europea. La Comunicazione «relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali» [*COM(2022)27 final*]

Nel solco profondo tracciato da Stefano Rodotà sembra muoversi ancora oggi l'Unione europea, intenzionata a procedere con la "riscrittura" della tavola dei valori da prendere in considerazione al cospetto della nuova dimensione tecnologica.

Il 26 gennaio 2022 la Commissione europea ha varato la Comunicazione «relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali» [COM(2022)27 final], al fine di «stabilire una serie di principi per una trasformazione digitale antropocentrica» (p. 1), da racchiudere in una «dichiarazione europea sui diritti e i principi digitali (…)» con la quale «si annuncerebbero una serie di intenzioni politiche comuni ai cittadini, alle imprese, alle pubbliche amministrazioni e ai responsabili politici» (p. 1)[27].

Nella Comunicazione cit. – relativa alla dichiarazione europea sui diritti e i principi digitali[28] – si rimarca che «I principi digitali illustrati nella dichiarazione vanno intesi come concetti essenziali, basati su valori comuni europei, e fungeranno da guida per un ambiente digitale antropocentrico, sicuro, inclusivo e aperto, che non escluda nessuno. L'obiettivo è garantire che i valori dell'Unione e i diritti e le libertà

[27] La dichiarazione sui principi digitali era stata anticipata dalla Comunicazione della Commissione europea del 9 marzo 2021 intitolata «*Bussola per il digitale 2030: il modello europeo per il decennio digitale*» [COM(2021)118 final], ove, nelle conclusioni, si trova affermato che « Il coinvolgimento e l'impegno del pubblico e di tutti i portatori di interessi sono fondamentali per realizzare una trasformazione digitale efficace. In tale contesto la Commissione avvierà, poco dopo la presente comunicazione, un ampio processo di consultazione sui principi digitali. Avvierà un dialogo con gli Stati membri, il Parlamento europeo, i partner regionali, economici e sociali, le imprese e i cittadini su elementi specifici della comunicazione nel corso del 2021, compreso il quadro della bussola con obiettivi e *governance* specifici. La Commissione istituirà un forum dei portatori di interessi, che sarà associato ad alcuni aspetti dei lavori per la bussola per il digitale 2030. La Commissione si baserà su queste misure di concertazione al fine di proporre ai colegislatori il programma di politica digitale entro il terzo trimestre del 2021 e spera di compiere progressi decisivi con le altre istituzioni in merito a una *dichiarazione sui principi digitali* entro la fine del 2021».

[28] La terminologia usata dalla Commissione europea, che si riferisce genericamente, nella Dichiarazione, sia a diritti che a principi digitali, impone un chiarimento sul rapporto tra gli uni e gli altri. Al riguardo si rimanda a quanto precisano *infra*, nella nota n. 13.

delle persone tutelati dal diritto dell'Unione siano rispettati e rafforzati *online* così come *offline*» (p. 1).

La Commissione ha basato la propria proposta su diversi elementi.

Innanzitutto ha preso atto di come la pandemia da Covid-19 abbia mutato radicalmente il ruolo e la percezione del digitale sia nella società che nell'economica, accelerando il processo di digitalizzazione già in atto. Tale accelerazione offre, nella prospettiva della Commissione, «opportunità senza precedenti», date dalla trasformazione, ad opera delle tecnologie digitali, di «ogni aspetto della nostra vita», n quanto il «ricorso ai mezzi digitali per il lavoro, l'istruzione, la vita sociale, l'intrattenimento, gli acquisti, l'accesso alla pubblica amministrazione, all'assistenza sanitaria o alla cultura è sempre più frequente».

Alla considerazione sulla pervasiva e capillare diffusione del digitale nel tessuto economico, sociale e istituzionale si aggiunge la presa d'atto di un innalzamento qualitativo degli strumenti tecnologici usati, che hanno potenzialità crescenti ed enormi. Nella Comunicazione cit. la Commissione richiama i «progressi tecnologi emergenti in settori quali l'intelligenza artificiale, l'analisi dei dati, la robotica, l'Internet delle cose e la loro integrazione in modelli imprenditoriali e sevizi e prodotti quotidiani», che «hanno contribuito a trasformare l'organizzazione dell'economia e della società», incrementando le opportunità per imprese, cittadini, lavoratori, consumatori, ma contribuendo anche ad aumentare il divario digitale nell'UE e l'avvento di nuovi rischi e l'incremento di quelli già esistenti, che possono mettere a repentaglio i valori democratici e le esigenze di sicurezza[29].

Ancora, la Commissione insiste sulla circostanza che l'interazione in ambiente digitale, da parte di imprese e persone, non deve comportare una compressione del godimento dei diritti o del livello di protezione rispetto a quando tali soggetti operano *offline*, per cui non può essere giustificata alcuna eccezione, nell'ambiente digitale, ai diritti e alle libertà già riconosciute *aliunde*. Nel richiamato ambiente digitale, tuttavia, i diritti e le libertà riconosciuti nell'UE andrebbero rafforzati, secondo la Commissione, e «quanto più le soluzioni tecnologiche che incidono sulle nostre vite diventano interconnesse, pervasive e complesse, tanto più urgente è l'esigenza di intensificare gli sforzi per conseguire un accesso aperto, equo e paritario agli strumenti, ai servizi, alle infrastrutture e alle competenze digitali con l'obiettivo ultimo di rafforzare le nostre democrazie» (p. 3).

In continuità con la direzione già tracciata dalla Commissione nella Comunicazione relativa alla bussola per il digitale 2030, anche nella Comunicazione per la

[29] La Commissione rimarca, a tal riguardo, che «Tali rischi sono aumentati in modo significativo, anche per quanto riguarda le violazioni della vita privata e dei *dati personali*, la diffusione di contenuti illeciti e nocivi e di prodotti non sicuri, nonché la disinformazione, la criminalità informatica e gli attacchi informatici, lo sfruttamento e l'abuso di esseri umani (compresi i minori), la sorveglianza di massa, le distorsioni algoritmiche che ostacolano l'accesso equo e non discriminatorio alle informazioni e al dibattito democratico e persino la censura vera e propria. Tali problemi colpiscono all'essenza dei diritti fondamentali e intaccano i progressi faticosamente conquistati in questo settore, sia nell'unione europea, sia a livello internazionale». Cfr. COMMISSIONE EUROPEA, *Comunicazione relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, COM(2022)27 final, p. 3.

dichiarazione dei diritti e dei principi digitali viene rimarcata la «visione dell'UE» per il decennio 2020-2030, che «è quella di una trasformazione digitale dell'Europa entro il 2030, in linea con i valori europei. In tale visione, imprese innovative e cittadini autonomi e responsabili coesistono in una società digitale antropocentrica, inclusiva, fiorente e sostenibile. Il "Percorso per il decennio digitale", adottato di recente, mira a rafforzare ulteriormente la nostra *leadership* digitale e a conferire maggiore autonomia e responsabilità ai cittadini e alle imprese, facendo così della trasformazione digitale il motore della crescita economica sostenibile e del benessere sociale in Europa. Tale obiettivo sarà conseguito, nello specifico, garantendo a tutti i cittadini l'accesso alla banda larga ad alte prestazioni, anche nelle aree rurali e isolate, sviluppando le capacità e le competenze digitali che consentano alla forza lavoro di partecipare pienamente all'economia digitale, digitalizzando le imprese e i servizi pubblici e rendendo questi ultimi più efficienti e facili da utilizzare a vantaggio di tutti nella nostra società. Un ciberspazio sicuro rafforza inoltre la fiducia delle persone nei confronti degli strumenti e dei servizi digitali. Consente di preservare la libertà di espressione e di informazione, compresa la libertà e il pluralismo dei media. Infine, in linea con la duplice transizione verde e digitale, la trasformazione digitale punterà anche a sfruttare il potere della tecnologia per intraprendere azioni per il clima, proteggere la biodiversità e ripristinare la natura, conformemente al *Green Deal* europeo, agli obiettivi di sviluppo sostenibile delle Nazioni unite e all'accordo di Parigi»[30].

In tale direzione, la Commissione europea, con la citata Comunicazione, ha inteso accogliere le richieste del Parlamento europeo e del Consiglio, proponendo di definire una serie di principi che abbiano la funzione di costituire una «guida per una trasformazione digitale sostenibile, antropocentrica e basata sui valori»[31].

Segnatamente, la Commissione ha precisato che «In tale contesto la dichiarazione propone principi digitali al servizio di tutti gli europei, con particolare riguardo ai seguenti elementi: una trasformazione digitale che mette al centro le persone; solidarietà e inclusione; libertà di scelta; partecipazione allo spazio pubblico digitale; sicurezza, protezione e conferimento di maggiore autonomia e responsabilità; e sostenibilità», con l'avvertenza che «La dichiarazione dovrebbe fungere anche da riferimento per i soggetti pubblici e privati nello sviluppo e nella diffusione di nuove tecnologie, Dovrebbe inoltre guidare i responsabili politici in uno sforzo congiunto volto a definire il percorso europeo verso un mondo digitale sostenibile, antropocentrico e inclusivo e ad ancorare saldamente gli interventi politici dell'UE a questo obiettivo. La dichiarazione ha il potenziale per diventare un punto di riferimento globale per molte questioni sociali ed etiche che emergono dalla trasformazione digitale. Gli stessi principi saranno al centro delle azioni che l'UE intraprenderà nei confronti dei suoi partner e in seno alle organizzazioni internazionali»[32].

[30] *Ibidem*, p. 4.
[31] *Ibidem*, p. 4.
[32] *Ibidem*, p. 4.

5.2. L'asserita (ma illusoria) natura meramente politica della Dichiarazione europea sui diritti e sui principi digitali

Rileggendoli da altra prospettiva, pare che tali "principi" digitali, più che vere e proprie «norme» giuridiche, con funzione ordinante o adeguatrice, siano stati pensati dalla Commissione per orientare in *funzione programmatica* gli sforzi dei diversi soggetti che, a vario livello, sono chiamati a forgiare il prossimo decennio all'insegna di una forte trasformazione digitale: mirano ad indicare la strada e ad orientare il percorso da intraprendere.

La Commissione, con la stesura della proposta di «Dichiarazione» dei *Digital Rights and Principles*, sembra avesse voluto introdurre un documento dalla natura non propriamente giuridica, ma essenzialmente politica, come espressamente chiarito al par. 3 della Comunicazione cit., intitolato «*La natura politica della dichiarazione europea sui diritti e i principi digitali*», e in ciò si registra una certa miopia dell'UE.

In esso si legge che «L'insieme dei principi digitali mirati a plasmare la società digitale europea è proposto sotto forma di una dichiarazione solenne congiunta del Parlamento europeo, del Consiglio e della Commissione (…)»[33]. Vero è che la Commissione si premura di precisare che «La dichiarazione si basa segnatamente sul diritto primario dell'UE, in particolare sul trattato sull'Unione europea (TEU), sul trattato sul funzionamento dell'Unione europea (TFUE), sulla Carta dei diritti fondamentali e sulla giurisprudenza della Corte di giustizia dell'Unione europea, nonché sul diritto derivato dell'UE»[34], ma poi rimarca espressamente che «Data la *natura politica della dichiarazione*, non tutti i principi rispondono a diritti direttamente applicabili: alcuni sono già sanciti dalla legislazione, altri possono richiedere ulteriori azioni, al livello appropriato. La dichiarazione deve essere letta in combinato disposto con gli atti e gli strumenti giuridici dell'UE, che lascia impregiudicati. Infatti la Commissione ha già presentato una serie di proposte normative e iniziative politiche nei settori di applicazione dei principi digitali, come indicato nel progetto di dichiarazione. Insieme al Parlamento europeo e al Consiglio, la Commissione intende continuare a portare avanti, ove necessario, azioni e iniziative volte a mettere in pratica i principi digitali che sottendono la trasformazione digitale»[35]. Ed ancora, si legge ulteriormente nella Comunicazione, «La dichiarazione sarà uno strumento di orientamento anche per l'azione diplomatica dell'UE e influirà sui nostri partenariati e sulle discussioni con i nostro partner internazionali»[36].

Il rapporto tra «*Diritti e Principi Digitali*» indicati nella Dichiarazione, quale documento di natura meramente "politica", e i diritti già riconosciuti nell'ordinamento europeo è, nella prospettiva della Commissione, enunciato in altra parte della Comunicazione, ove si trova ribadito che «i principi» digitali espressi nel documento di natura politica, qual è la dichiarazione europea sui diritti e i principi digitali, «non pregiudicano i diritti già previsti dal quadro giuridico dell'UE a tutela delle persone

[33] *Ibidem*, p. 5.
[34] *Ibidem*, p. 5.
[35] *Ibidem*, p. 6.
[36] *Ibidem*, p. 7.

online nell'Unione europea, e per i quali devono esistere rimedi giurisdizionali efficaci in tutta l'Unione. Non pregiudicano neanche i limiti legittimi posti all'esercizio di tali diritti legali al fine di conciliarli con l'esercizio di altri diritti, né le restrizioni necessarie e proporzionate nell'interesse pubblico. Se attuati attraverso iniziative politiche, tali principi saranno applicati insieme ai diritti e principi vigente e per l'interesse pubblico generale»[37].

Sembrerebbe trattarsi, ove si aderisse all'impostazione fornita dalla Commissione, di una "rivoluzione soffocata", con l'idea di voler affermare «principi» di valenza solamente politica al fine di definire successivamente, in distinti atti normativi, le «norme» concretamente applicabili in corrispondenza a tali "principi", a meno che tali norme non siano già ravvisabili, anche solamente in parte, nel tessuto normativo che l'UE ha realizzato finora, anche a livello "costituzionale", tramite – ad esempio – la Carta dei diritti fondamentali dell'UE e altre norme già fissate per disciplinare i rapporti intersoggettivi nell'ambiente digitale.

Si tratta però di impostazione non condivisibile. I diritti e i principi, se attengono alla sfera della personalità, sono da considerare diritti non "creati" dal legislatore, ma da questi "riconosciuti", secondo la felice impostazione di Francesco Galgano. Sicché la dichiarazione dei diritti e dei principi digitali finirebbe per travalicare, in tale ambito, la natura meramente politica a cui la Commissione europea vorrebbe confinarla, per avere una valenza anche giuridica.

Si va verso il riconoscimento di diritti fondamentali e principi che, seppur non consacrati nella Carta dei diritti fondamentali dell'UE e nei Trattati, emergono in tutta la loro forza come "norma" giuridica, in funzione sia ordinante che adeguatrice, a cui si accompagna, ovviamente, anche l'imperativo, per il legislatore, di rendere effettivi i contenuti del principio-norma, ove l'implementazione richieda sforzi at-

[37] *Ibidem*, p. 6.

tuativi in via programmatica[38], senza che con ciò venga meno la forza normativa e vincolante del principio[39].

L'operazione innovativa portata avanti dalla Commissione europea, indipendentemente dalle intenzioni dichiarate nel documento, avrà dunque l'effetto di affiancare il novero dei diritti esistenti e pacificamente riconosciuti, inserendo, in un elenco che rimane aperto[40], il riconoscimento esplicito di altri diritti e principi, declinati in ambito digitale, i quali tuttavia non possono non avere una portata giuridica, dovendosi considerare vano il tentativo della Commissione di sterilizzare la loro natura intrinsecamente giuridica e, ancora, di subordinarne l'applicazione all'adozio-

[38] L'intento programmatico dei principi contenuti nella (proposta di) dichiarazione sui diritti e sui principi digitali avanzata dalla Commissione europea (e successivamente recepita anche dal Parlamento europeo e dal Conglio), da cui le istituzioni europee intenderebbero desumere la natura meramente "politica" e "programmatica" della dichiarazione medesima, non può essere avallato, nel senso che dall'affermazione dei principi in essa contenuti, declinati come norme prive di riferimenti alla fattispecie, potranno ricavarsi norme autoapplicabili, mediante l'intervento dell'interprete, e norme non autoapplicabili (ma pur sempre *norme*), che invece esigono l'intervento di soggetti diversi dal giudice per poter essere tradotte sul piano dell'efficacia, quali, ad esempio, il legislatore europeo e/o nazionale, preceduti dai *decision maker*s politici, per le scelte da tradurre nel testo normativo, volto a dare concretezza a principi non autoapplicabili, racchiusi in norme programmatiche.
Si richiama, a tal proposito, l'osservazione di C. CAMARDI, *Brevi riflessioni sull'argomentazione per principi nel diritto privato*, cit., pp. 11 ss. e, ivi, spec. par. 3, resa con riguardo alle norme costituzionali, ma utile anche ai fini del discorso che qui si sta conducendo: «Il superamento della dicotomia tra norme (…) programmatiche e norme precettive e la sua sostituzione – semmai – con l'altra dicotomia che si è tentato di esplicitare tra norme immediatamente (auto)applicabili e norme che non lo sono, può in teoria rendersi ancora compatibile (…) con la struttura delle norme "a fattispecie". Tutte le volte in cui il principio costituzionale entra nei rapporti privati secondo quella che si chiama *Drittwirkung* mediata, infatti, si è in presenza di fattispecie che si allargano e vengono piegate alla tutela del bene protetto dal principio costituzionale. Ma il discorso può cambiare se l'applicazione diretta del principio viene invece intesa come strumento per superare (non la fattispecie legale prevista per la disciplina di un caso, bensì) la fattispecie come paradigma unico di disciplina di un caso, e ancor più per superare in radice l'idea che il principio applicabile dal giudice sia ricavabile esclusivamente da un "sistema di enunciati posti"».

[39] Come affermato da G. ALPA, *I principi generali*, cit., p. 299, «oggi si riconosce universalmente la natura normativa dei principi». Va chiarito che i principi hanno una indubbia valenza normativa, invero, anche qualora contengano una parte di natura programmatica, risolvendosi, in tal caso, in un obbligo di attuazione del "programma" inscritto nel principio (ai pensi, ad esempio, al principio di uguaglianza sostanziale contenuto nell'art. 3, par. 2, della Cost.). Ancora – e sotto altro profilo – i "principi" sono norme così come sono norme anche le "regole" poste nell'ordinamento giuridico, ma a fronte dell'identica natura (appunto "normativa"), gli uni e le altre presentano distinzioni su cui la dottrina è intervenuta ampiamente. Per un riepilogo dei principali tratti distintivi si veda G. VETTORI, *Regole e principi. Un decalogo*, cit., pp. 128 ss.

[40] Sul catalogo aperto dei diritti dell'uomo si veda F. GALGANO, *Trattato di diritto civile*, Milano, 2014 (3ª ed. curata e aggiornata da Zorzi Galgano), vol. I, p. 173; con specifico riferimento ai «principi» si veda invece G. ALPA, *I principi generali*, cit., p. 298, il quale, ritiene una mera «illusione del legislatore» l'affermazione secondo cui «i principi sarebbero un numero chiuso, circolante entro confini ben definiti. Ciò perché i principi si desumono dalle norme, e quindi non possono esistete (giuridicamente) se non hanno fondamento in esse. Anche qui il legislatore ha dimenticato, o ha finto di dimenticare, il ruolo dell'interprete, il quale è abile nel creare i principi e poi nell'ancorarli alle norme. I principi *non* sono un numero chiuso e quindi *non* sono inventariabili, è questa una considerazione antica, che trova ampie conferme nella prassi».

ne necessaria di norme volte a rendere applicabili i principi formalmente dichiarati come aventi solo natura politica, ma non giuridica[41].

Così, interpretativamente va affermata la portata normativa dei "nuovi" principi – che si affiancano a quelli già presenti nell'ordinamento, maturati soprattutto a partire dalla disciplina in materia di protezione dei dati personali – e spetterà all'interprete misurarsi con la loro applicazione nella casistica concreta, secondo la funzione ordinante e la funzione adeguatrice sopra delineata, ferma restando la concomitante spinta del legislatore, europeo ma anche nazionale nei singoli Paesi membri, ad adottare ulteriori norme di dettaglio (regole, in senso tecnico) per dare maggiore concretezza alla portata precettiva insita nel principio di portata generale[42].

In base a tale impostazione, che mi sembra preferibile sul piano ermeneutico e applicativo, può rileggersi il documento sintetico della Commissione europea, intitolato «*European Digital Rights and Principles*», con cui viene presentata la proposta di «*Declaration on European digital rights and principles*»[43]. Nella premessa di tale documento viene enunciato che, al fine di promuovere la transizione al digitale sulla base dei valori europei, «*it has proposed a set of European digital rights and principles (…). The suggested European digital rights and principles will complement existing rights, such as data protection, ePrivacy, and the Charter of Fundamental Rights. They will build on the experience of the European of Social Rights. And, they will provide guidance for the EU and Member States as they design digital rules and regulations*»[44].

5.3. La «*European Declaration on Digital Rights and Principles for the Digital Decade*» (2023/C 23/1)

Il testo della proposta di Dichiarazione è stato formalizzato dalla Commissione europea il 26 gennaio 2022, COM(2022)28 final, con il titolo «*European Declaration on Digital Rights and Principles for the Digital Decade*». Un anno più tardi, in data 23 gennaio 2023, con il medesimo titolo e con alcune modifiche nel testo, il

---

41 V., *supra*, nota n. 37.

42 Per usare il lessico riproposto da Umberto Breccia, la Commissione europea intende tali principi come «*direttivi*», anche se, mi pare, siamo di fronte a principi che, pur continuando ad essere «direttivi», si propongono al contempo anche come «*regolativi*». Cfr. U. Breccia, *Principi: luci e ombre nel diritto contemporaneo*, in *Riv. it. sc. giur.*, 2014 (numero speciale: *I principi nell'esperienza giuridica*. Atti del Convegno della Facoltà di Giurisprudenza della Sapienza, Roma, 14-15 novembre 2014), p. 125, ove si riprende «la suddistinzione dei principi generali in "principi direttivi" (in quanto "norme che formulano valori o obiettivi politici" e che hanno riferimento empirico a "politiche pubbliche") e in "principi regolativi" (in quanto norme "che sono al tempo stesso principi e regole" e che, com'è il caso della maggior parte "dei diritti fondamentali e del principio di uguaglianza", in quanto principi sono "oggetto di argomentazione" e, in quanto regole, sono "oggetto di applicazione")». Cfr. *amplius*, per tale distinzione, L. Ferrajoli, *La democrazia attraverso i diritti. Il costituzionalismo garantista come modello teorico e come progetto politico*, Roma-Bari, 2013, pp. 109 ss. e, ivi, spec. p. 111 s.

43 Commissione europea, *European Digital Rights and Principles*, documento aggiornato al 4 maggio 2022, reperibile *online* all'*url* https://digital-strategy.ec.europa.eu/en/policies/digital-principles (consultato da ultimo in data 10 agosto 2022).

44 Commissione europea, *European Digital Rights and Principles*, cit.

documento definitivo è stato pubblicato nella Gazzetta Ufficiale dell'UE nella forma della Dichiarazione congiunta del Parlamento europeo, del Consiglio e della Commissione europea. Il riferimento esplicito al decennio digitale che ci attende, che sarà segnato da una trasformazione forte del tessuto sociale ed economico, mostra l'approccio che l'Unione europea ha alla "riscrittura" dei nuovi diritti e dei nuovi principi: si intende porre le basi per governare la prima fase della transizione digitale, nella prospettiva decennale, per poi rivedere, definire meglio e probabilmente ampliare ulteriormente il catalogo dei diritti e dei principi "digitali", al di là del decennio che ci attende. Così, nel preambolo della Dichiarazione europea dei diritti e dei principi digitali per il "decennio digitale" si è inteso prendere atto che *«With the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicabile offline should be applied in the digital environment. The digital transformation should not entail the regression of tights. What is illegal offline, is illegal online* (…)»[45]. Non si tratta però di una mera trasposizione al mondo digitale di valori già presenti per il mondo *offline*: qui la sfida è diversa, perché accanto alle medesime esigenze di tutela tradizionali, da applicare al nuovo contesto, sorgono anche esigenze di tutela nuove, sia sul piano individuale (si pensi ai rischi derivanti all'individuo dalla soggezione a decisioni algoritmiche, solo per fare un esempio) sia sul piano collettivo (si consideri, a tal proposito, i problemi legati alla tenuta dell'assetto democratico, alla *governance* della rete e all'emersione di nuovi poteri, in cui i privati detengono spazi di sovranità e controllo, spesso superiori a quelli degli Stati nazionali, ma usati secondo logiche di profitto e non secondo le logiche del necessario perseguimento dell'interesse pubblico). Sempre nel Preambolo della Dichiarazione viene infatti specificato che «*The digital transformation affects every aspect of people's lives. It offers significant opportunities for a better quality of life, economic growth and sustainability*»[46], con l'ulteriore precisazione che «*The digital transformation also presents new challenges for our democratic societies, our economies and for individuals*»[47].

Vengono così indicati sei *Digital (Rights and) Principles* dalla Commissione, a cui vengono fatte corrispondere alcune statuizioni, sia per declinarne in maniera più circoscritta il senso, sia per offrire indicazioni in via programmatica, con attenzione sia alla società civile che al settore economico. *Verbatim*, nella Dichiarazione si esplicita l'«obiettivo» perseguito, che è quello di promuovere «*a European way for the digital transformation, putting people at the centre, built on European values and EU foundamental rights, reaffirming universal human rights, and benefiting all individuals, businesses, and society as a whole*»[48].

[45] *European Declaragion on Digital Rights and Principles for the Digital Decade*, Joint Declaration of European Parliament, Council and European Commission, in G.U.U.E., 23 gennaio 2023, C23/1 (*Preamble*, par. 3).

[46] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., *Preamble*, par. 2.

[47] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., *Preamble*, par. 3.

[48] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit.

5.4. Mettere le persone al centro della trasformazione digitale

Ogni *Digital Right and Principle* è racchiuso, nel testo della Dichiarazione, all'interno di uno specifico *Chapter*, per un totale di sei "Capi". Con riguardo al primo di essi, intitolato «*Putting people at the centre of the digital transformation*», si statuisce solennemente la visione antropocentrica, il che vale a ribadire, sul piano assiologico, la centralità del principio personalistico, caro alla nostra tradizione giuridica, tipicamente riscontrabile negli ordinamenti nazionali di area europea e in quello eurounitario, seppur con alcune vistose limitazioni dettate dal difficile contemperamento con le esigenze di natura economica che hanno segnato la stessa ragion d'essere dell'allora Comunità economica europea (CEE), poi divenuta Comunità europea (CE) e ora Unione europea (UE). Il *Chapter* I esordisce, infatti, con la dichiarazione che «*People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect of their fundamental rights*»[49].

Tale statuizione di principio afferma con forza l'ancillarità delle tecnologie rispetto alla persona e allo sviluppo delle sue «aspirazioni», individuali, sociali ed economiche. Diremmo, con sguardo attento al nostro ordinamento e, segnatamente, a quanto indicato all'art. 2 Cost., che il Principio in esame vada interpretato estendendo il testuale riferimento alle "aspirazioni", in modo da ritenere ricomprese in esse tutte le declinazioni dello sviluppo della personalità, incluso quelle che si esplicano all'interno delle formazioni sociali, che, nella prospettiva considerata dalla Dichiarazione, sono primariamente quelle costituite *online* o che con gli strumenti digitali facilitano le interazioni tra i soggetti che ne fanno parte (si pensi alle *virtual community* organizzate sulle piattaforme digitali relazionali, come i *social media*, nonché l'uso di piattaforme di comunicazione che tanto hanno facilitato le interazioni sociali ed economiche in tempo di pandemia da covid-19, primariamente nei periodi di *lockdown*)[50].

Nel documento illustrativo della proposta di Dichiarazione, la Commissione precisa, in particolare, il duplice ruolo delle tecnologie digitali, non solo come oggetto del diritto ad accedervi e a farne uso, in funzione strumentale per le aspirazioni individuali, sociali ed economiche di ciascuno, ma anche come strumento utile per l'esercizio assicurare l'esercizio dei diritti fondamentali agli individui e supportare la società democratica nel contesto digitale: le «*Digital technologies should protect people's rights, support democracy and ensure that all digital players act responsibly and safely. (…) Technology should serve and benefit all Europeans and empower*

[49] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., *Chapter* I.

[50] In materia si rinvia, *amplius*, a F. Bravo, Ubi societas ibi ius *e fonti del diritto nell'età della globalizzazione*, in *Contratto e impresa*, 2016, 6, pp. 1344-1390; F. Bravo, E-Health *e* social networks *per la realizzazione di* communities *socio-sanitarie in tema di malattie rare. Riflessioni giuridiche tra diritti fondamentali e responsabilità civile*, in C. Faralli-R. Brighi-M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth*, Torino, 2015, pp. 109-131.

them to pursue their aspirations. It should not infringe upon their security or fundamental rights»[51].

Il valore della persona, le possibilità di sviluppo della personalità, così come l'agire all'interno della società democratica, devono essere in ogni caso salvaguardati nella transizione all'ambiente digitale, sia assicurando in ambiente digitale il rispetto dei diritti maturati *offline*, sia individuando e garantendo ulteriori tutele, specifiche del mondo digitale (*online*), anche là dove non sia riscontrabile alcuna corrispondenza nel tradizionale contesto *offline*.

Accanto alla parte enunciativa del *Digital Principle*, il *Chapter* I della Dichiarazione prosegue con la parte programmatica, ove si afferma il correlativo impegno (della Commissione, del Parlamento e del Consiglio) a: (i) rafforzare il quadro democratico per la trasformazione digitale, nella prospettiva che ciò sia di beneficio di ogni persona e che possa migliorare la via di tutti di europei; (ii) adottare le misure necessarie ad assicurare che i valori dell'UE e i diritti (fondamentali) degli individui, riconosciuti dal diritto eurounitario, siano rispettati sia *online* che *offline*; (iii) promuovere azioni diligenti e responsabili per tutti i «*digital actors*», sia nel settore pubblico che nel settore privato, per un ambiente digitale sicuro e protetto; (iv) promuovere attivamente la visione europea antropocentrica della trasformazione digitale anche nelle relazioni internazionali in cui l'UE è impegnata[52].

5.5. Solidarietà e inclusione (connettività, condizioni di lavoro, istruzione, formazione e competenze digitali, condizioni di lavoro giuste ed eque, servizi pubblici digitali *online*)

Il secondo dei *Digital Principles*, individuato nel *Chapter* II della *Declaration*, concerne «*Solidarity and inclusion*», con riferimento al quale viene innanzitutto statuito che «*Technology should be used to unite, and not divide people. The digital transformation should contribute to fair and inclusive society and economy in the EU*»[53].

Nell'ambito di tale principio[54] vanno dunque considerati anche aspetti quali la connettività ad Internet e l'*open access*, l'educazione digitale e la promozione di

[51] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.

[52] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., *Chapter* I.

[53] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., *Chapter* II.

[54] Per un'ampia ed esaustiva trattazione sull'affermazione e sull'inquadramento del principio di solidarietà, nella sua evoluzione storica, nonché nei diversi ordinamenti (quello delineato dalla Costituzione di Weimar, dalle costituzioni totalitarie degli anni Trenta, dalle Costituzioni nazionali del secondo dopoguerra e dalle Costituzioni attuali, nonché quello delineato dalla nuova dottrina sociale della Chiesa e, infine, dal diritto europeo) si veda G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022 e ID., *Note sul principio di solidarietà come principio precettivo nel diritto interno e nel diritto dell'Unione europea*, in *Lo Stato*, 2022, 18, pp. 11-56 (nonché, in precedenza, ID., *Solidarietà*, in *Nuova giur. civ. comm.*, 1994, p. 368 ss.). La solidarietà – rimarca Guido Alpa – è una regola morale, un valore, un principio di valenza anche "normativa" e, dunque, anche un concetto giuridico, benché per lungo tempo sia stato confinato "nel mondo delle idee", quasi fosse "estraneo al diritto", per via della sua genericità, della sua ambiguità e della sua astrattezza, che lo ha fatto considerare per molto tempo "poco radicato nella realtà". Il principio di solidarietà, al contrario, è emerso in tutta la sua

adeguati *digital skills*, il diritto alla fruizione di servizi pubblici in ambiente digitale, incluso quelli relativi all'assistenza sanitaria, ma anche alla disconnessione nel caso di lavoro *online* per poter godere del giusto equilibrio con le esigenze della vita privata[55]. Ritorna qui, nell'ordinamento europeo, l'idea di Stefano Rodotà espressa con la già richiamata proposta di inserimento dell'art. 21-*bis* nella nostra Carta costituzionale, che prevedeva, per «tutti» un «eguale diritto» di *accesso ad Internet*, «in condizione di parità, con modalità tecnologicamente adeguate» e rimozione di «ogni ostacolo di ordine economico e sociale». S'è trattato, com'è noto, di una proposta che non ha portato, a livello nazionale, ad alcuna modifica sul piano normativo, ma che ora, per via delle scelte dell'UE, sembra destinata ad entrare con forza nell'ordinamento europeo, attraverso una progressiva formalizzazione dei nuovi "fondamentali" diritti e principi digitali.

Si consideri che nel *Chapter* II della Dichiarazione ora in esame, alla statuizione (principio) di carattere generale sopra trascritta fanno seguito ulteriori statuizioni, dedicate rispettivamente ai seguenti aspetti: (a) *Connettivity*; (b) *Digital education, training and skills*; (c) *Fair and just working conditions*; (d) *Digital public services online*.

La (a) connettività, come presupposto tecnico del diritto di accesso al mondo digitale, è condizione necessaria per poter godere dei "nuovi diritti e principi digitali". È anche indispensabile al fine di non essere escluso dalla vita sociale, economica e democratica che sta andando verso la transizione digitale. Con riguardo ad essa la *Declaration* statuisce che «*Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity*».

---

forza in un'evoluzione crescente, transitando dalla dimensione extragiuridica delle "idee" a vero e proprio principio normativo che pervade gli ordinamenti giuridici, incluso quello dell'UE. Come avverte efficacemente Alpa, anche oggi tale principio ha conservato una certa carica utopistica, ma è declinato in una molteplicità di regole del diritto privato e del diritto commerciale. Si vedano anche le stimolanti riflessioni di S. Rodotà, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2016, in particolare là dove ha insistito sul ripensamento di tale principio in un contesto almeno europeo, quale strada da percorrere per evitare la frammentazione sociale. Si veda anche, con specifico riferimento alla correlazione tra principio di solidarietà e protezione dei dati personali F. Bravo, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione,* in *Contratto e impresa*, 2023, 2, pp. 405-441; F. Bravo, *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf.*, 2023, 3, pp. 481 ss.; nonché, nell'ambito del presente volume, il cap. XIV, F. Bravo, *Il principio di solidarietà*.

[55] Si noti, nella *European Declaration on Digital Rights and Principles for the Digital Decade*, la grande estensione del concetto di solidarietà, con riferimento al quale la tecnologia diviene strumento idoneo a perseguirla. L'ordinamento europeo, proprio sul *principio di solidarietà*, ha percorso recentemente strade innovative anche in materia di *protezione dei dati personali*, introducendo una specifica disciplina sul *Data Altruism* nel Reg. UE 868/2022, noto come *Data Governance Act*, al cui art. 2, par. 1, n. 16, viene così definito: «*'data altruism' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest*».

Quanto al secondo aspetto, relativo (b) all'istruzione, alla formazione e alle competenze digitali, la Dichiarazione prevede che «*Everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills*», mentre, con riguardo alle (c) condizioni di lavoro giuste ed eque, si afferma che «*Everyone has the right to fair, just, healthy and safe working conditions and appropriate protection in the digital environment as in the physical work place, regardless of their employment status, modality or duration.*

Trade unions and employers' organisations play an important role in the digital transformation, particularly in relation to the definition of fair and just working conditions, including with regard to the use of digital tools at work».

Per l'ultimo aspetto, relativo ai (d) servizi pubblici digitali *online*, il *Chapter* II della Dichiarazione prevede infine che «*Everyone should have access to all key public services online across the EU. Nobody is to be asked to provide data more often than necessary when accessing and using digital public services*». La transizione al digitale comporta il trasferimento *online* dei servizi pubblici, ai quali deve essere assicurato l'accesso, almeno a tutti quelli essenziali. Qui il diritto di accesso ai servizi digitali è affiancato dal principio di minimizzazione dei dati, già previsto nel GDPR, ma declinato con differente sfumatura, visto che riguarda non gli aspetti qualitativi o quantitativi dei dati, bensì la reiterazione temporale della richiesta dei dati medesimi al fine di accedere ai servizi in questione.

Ciascuna di tali statuizioni di principio, sia quella di portata più generale relativa a "Solidarietà e inclusione", sia quelle più specifiche concernenti i diversi quattro aspetti poc'anzi richiamati, sono seguite da dichiarazioni di impegno, in via programmatica.

Quanto al principio di *Solidarity and inclusion*, nella sua statuizione di portata più ampia, viene ribadito l'impegno: (i) ad assicurare che le soluzioni tecnologiche siano progettate, sviluppate, diffuse e utilizzate nel rispetto dei diritti fondamentali e in modo tale da consentire l'esercizio di tali diritti e da promuovere la solidarietà e l'inclusione, (ii) a promuovere una trasformazione digitale «*that leaves nobody behind*» e che sia pertanto inclusiva nei confronti di tutti, promuovendo la diversità culturale e linguistica, realizzando la parità di genere e l'inclusione anche nei confronti di persone svantaggiate come gli anziani, le persone che vivono nelle zone rurali, le persone con disabilità, quelle emarginate, quelle vulnerabili o prive di diritti o privilegi («*disenfranchised people*»), oltre che di coloro che agiscono per proprio conto e non hanno soggetti che, in posizione di forza, possano rappresentarli nel rivendicare o nell'esercitare i propri diritti o nel pretenderne l'applicazione; (ii) a sviluppare *frameworks* adeguati affinché tutti gli attori del mercato, che traggono vantaggio dalla trasformazione digitale, si facciano carico delle proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi relativi a beni pubblici, servizi pubblici e infrastrutture pubbliche, a beneficio di tutti coloro che vivono nell'UE.

Lo sforzo programmatico per realizzare la (a) *Connectivity* viene invece tradotto nell'impegno (i) ad assicurare l'accesso ad una connettività di elevata qualità, con la disponibilità di un accesso ad Internet, per ogni persona nell'UE, comprese quelle con basso reddito, nonché (ii) a proteggere e promuovere una rete Internet

neutra e aperta, in cui contenuti, servizi e applicazioni non siano bloccati o degradati ingiustificatamente.

Quanto a (b) *Digital education, training and skills*, l'impegno indicato in via programmatica nella Dichiarazione è rivolto a: (i) promuovere un'istruzione e una formazione digitali di elevata qualità, anche al fine di colmare il divario digitale di venere; (ii) supportare gli sforzi volti a consentire a tutti i dicenti e docenti di acquisire e condividere le capacità e le competenze digitali necessarie, inclusa l'alfabetizzazione mediatica e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici; (iii) promuovere e sostenere gli sforzi volti a dotare tutti gli istituti di istruzione e di formazione di connettività, infrastrutture e strumenti digitali; (iv) dare a tutti la possibilità di adattarsi ai cambiamenti introdotti dalla digitalizzazione del lavoro, attraverso il miglioramento delle competenze e la riqualificazione professionale.

Quanto alle (c) *Fair and just working conditions*, in via programmatica la *Declaration* prevede di declinare il principio di solidarietà e di inclusione, in primo luogo, tramite l'impegno ad (i) assicurare a tutti la facoltà di disconnettersi e di godere di adeguate garanzie per un soddisfacente equilibrio tra lavoro e vita privata nell'ambiente digitale, nonché a (ii) garantire che, nell'ambiente lavorativo, la salute fisica e mentale dei lavoratori non sia in alcun modo messa a rischio e che (iii) siano comunque rispettati i diritti fondamentali dei lavoratori nell'ambiente digitale, incluso il diritto al rispetto della vista privata, il diritto di associazione, il diritto di contrattazione e azione collettiva, nonché la protezione dalla sorveglianza illecita e ingiustificata. Ulteriori specifici impegni riguardano le frontiere dell'intelligenza artificiale: su tale fronte le istituzioni europee intendono (iv) garantire che l'utilizzo dell'IA sul luogo di lavoro sia trasparente e segua un approccio basato sul rischio e che sia sempre accompagnata da adeguate misure di prevenzione per mantenere l'ambiente lavorativo sano e sicuro; altro impegno mira a (v) garantire la sorveglianza umana nelle decisioni importanti che interessano i lavoratori e il diritto di questi ultimi ad essere informati «del fatto di stare interagendo con sistemi di intelligenza artificiale»[56].

Infine, la sezione programmatica del *Chapter* II, dedicata a (d) *Digital public services online*, mira ad assicurare "solidarietà e inclusione" in tale specifico settore attraverso l'impegno della Commissione europea, del Parlamento e del Consiglio ad: (i) assicurare che a tutti coloro che vivono nell'UE sia offerta la possibilità di utilizzare un'identità digitale accessibile, volontaria, sicura e affidabile che consenta di accedere a una vasta gamma di servizi *online*; (ii) assicurare accessibilità e riuso di una vasta gamma di informazioni della pubblica amministrazione; (iii) agevolare e sostenere un accesso continuo, sicuro e interoperabile ai servizi pubblici digitali concepiti per soddisfare le esigenze delle persone in modo efficiente, incluso i servizi sanitari e assistenziali digitali, con particolare riferimento anche alle cartelle cliniche elettroniche.

[56] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., Chapter II, 6, lett. *e)*, vers. in italiano.

5.6. Libertà di scelta (interazioni con algoritmi e sistemi di intelligenza artificiale, un ambiente *online* equo)

Il terzo *Digital Principle* è relativo alla «*Freedom of Choice*» nel contesto digitale, con riferimento alla quale la Commissione, nel documento illustrativo che accompagna la Dichiarazione, afferma che «*People should benefit from a fair online environment, be safe form illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence*»[57] e che «*People should be empowered to make their own, informed choice online*»[58]. Tale principio mira ad arginare anche le possibili discriminazioni o altri possibili effetti pregiudizievoli che possono aversi in caso di esposizione a trattamenti basati su algoritmi e sistemi di intelligenza artificiale. La libertà di scelta, incluso quella di autodeterminazione, poggia spesso sull'esigenza di trasparenza dei sistemi algoritmici o automatizzati, a cui la persona si trova esposta, ma la trasparenza, di per sé, in molti casi non è risolutiva. Il principio in esame viene inteso in maniera più ampia, volendo assicurare, con esso, le esigenze di tutela della persona anche a prescindere dalla trasparenza medesima, in una visione marcatamente antropocentrica. Così, l'applicazione di tale principio imporrebbe, tra l'altro, che i sistemi algoritmici siano basati «*on suitable datasets to avoid unlawful discrimination and enable human supervision of outcomes affecting people*»[59] e che le tecnologie particolarmente avanzate, «*such as algorithms and artificial intelligence are not used to predetermine people's choices, for examples regarding health, education, employment, and their private live*»[60]. Inoltre, tale principio è correlato alle esigenze di salvaguardia della concorrenza e del mercato, giacché «*Freedom of choice also includes being free to choose which online services we use, based on objective, transparent and reliable information This in turn involves making sure everyone is empowered to compete and innovate in the digital world*»[61]. La Commissione mostra di voler far larga applicazione di tale principio, giacché include anche l'esigenza di garantire «*a safe, secure and fair online environment where fundamental rights are protected, and responsabilities of platforms, especially large players and gatekeepers, are well defined*»[62].

Nel testo della *European Declaration on Digital Rights and Principles for the Digital Decade* il principio di «*Freedom of choice*» viene affermato nel *Chapter* III, immediatamente suddiviso in due sezioni: la prima dedicata a «*Interactions with algorithms and artificial intelligence systems*», la seconda a «*A fair online environment*». Ciascuna delle due sezioni contiene le statuizioni generali di principio, seguite da dichiarazioni di impegno in via programmatica.

Nella sezione dedicata alle "Interazioni con algoritmi e sistemi di intelligenza artificiale" i principi statuiti nella Dichiarazone prevedono, in primo luogo, che l'IA «*should serve as a tool for people, woth the ultimate aim of increasing human*

[57] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.
[58] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.
[59] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.
[60] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.
[61] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.
[62] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.

well-being» e che, conseguentemente, «*Everyone should be empowered to benefit from the advantages of artificial intelligence systems inclusing by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights*».

Correlativamente a tali principi viene previsto, in via programmatica, l'impegno a (i) promuovere sistemi di IA antropocentrici, affidabili ed etici nell'intero corso del loro sviluppo, della loro diffusione e del loro utilizzo, in aderenza ai valori dell'UE, (ii) assicurare un adeguato livello di trasparenza in relazione all'uso degli algoritmi e all'IA, facendo in modo che le persone che interagiscono con essi siano autonomi e responsabili ed informati; (iii) assicurare che i sistemi algoritmici siano basati su insieme di dati (*datasets*) adeguati ad evitare discriminazione illeciti e consentano la supervisione umana di tutti i risultati che abbiano effetti sulla sicurezza delle persone e sui loro diritti fondamentali; (iv) assicurare che le tecnologie, in particolare quelle di IA, non siano usate per pregiudicare le scelte delle persone, ad esempio con riguardo alla salute, all'istruzione, all'occupazione lavorativa o professionale e alla loro vita privata; (v) prevedere garanzie e adottare misure adeguate, incluso la promozione di *standards* affidabili, per assicurare che in ogni momento i sistemi digitali e di IA siano sicuri e vengano usati nel pieno rispetto dei diritti fondamentali delle persone; (vi) adottare misure volte a garantire che la ricerca sull'IA rispetti i più elevati principi etici ed il diritto dell'UE applicabile a tali tecnologie.

Le tecniche di tutela sono qui mutuate dalla disciplina in materia di protezione dei dati personali, riecheggiando, quanto a trasparenza e diritto all'intervento umano, il sistema di protezione vantato dall'interessato nei confronti dei trattamenti automatizzati adottati al fine di prendere decisioni algoritmiche, sancito all'art. 22 GDPR.

Con riguardo alla trasparenza, in funzione dell'esercizio di scelte consapevoli in materia di algoritmi e intelligenza artificiale, va però rimarcato che il sistema di protezione auspicabile non può basarsi solamente sul principio di autodeterminazione, sia perché non è sempre possibile veicolare un livello di trasparenza adeguato, in quanto spesso le modalità di funzionamento dei sistemi basati sull'IA – soprattutto in caso di autoapprendimento – non è comprensibile a priori, né a chi ha realizzato il sistema di intelligenza artificiale, né a chi se ne serve; sia perché, anche qualora la trasparenza fosse sufficientemente veicolabile nei confronti dell'interessato, potrebbe non essere facilmente comprensibile il *set* informativo comunicato al soggetto esposto al trattamento algoritmico. Occorre dunque affiancare a tali sistemi ulteriori meccanismi di protezione di *public enforcement*, volti a garantire obblighi di sicurezza e di garanzia sulla base di parametri predefiniti a livello normativo o con specifici provvedimenti da parte di *authorities* di settore, da sottoporre a controllo da parte di queste ultime, indipendentemente dalle scelte dell'interessato in ordine all'adesione alla soluzione tecnologica nei cui confronti è esposto.

Quanto alla sezione dedicata a "Un ambiente digitale equo", il *Chapter* III della Dichiarazione contempla le affermazioni di principio secondo cui «*Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible and reliable information. Everyone should have the possibility to compete fairly and innovate in the digital environment*», con l'ulteriore precisazione che «*This should also benefit businesses, including SMEs*».

La libera determinazione è intesa, dunque, non solo in favore del destinatario delle tecnologie e dei servizi digitali, ma anche in favore di chi tali tecnologie le propone per competere sul mercato e, sotto tale profilo, finisce per toccare aspetti tipicamente riferibili all'autonomia privata e alla libertà di impresa e, per quanto attiene ad una sua più specifica declinazione, al diritto a trattare dati personali[63].

A livello programmatico la dichiarazione di tale principio è accompagnata dall'impegno istituzionale di (i) assicurare un ambiente digitale sicuro e protetto, basato sulla concorrenza leale, in cui siano tutelati i diritti fondamentali, siano garantiti i diritti degli utenti e dei consumatori nel mercato unico digitale e siano ben definite le responsabilità delle piattaforme, con particolare riferimento ai grandi *players* e ai *gatekeepers*. Un ulteriore impegno rimarcato nella Dichiarazione con riguardo all'ambiente digitale equo è quello volto a (ii) promuovere l'interoperabilità, la trasparenza le tecnologie aperte e gli standard aperti, quale modo per rafforzare ulteriormente la fiducia nella tecnologia e la capacità dei consumatori di compiere scelte autonome e informate.

5.7. Partecipazione allo spazio pubblico digitale

Con il quarto principio, dedicato alla «*Participation in the Digital Public Space*», a cui è dedicato il *Chapter* IV della Dichiarazione, si prevede, in maniera articolata, che «*Everyone should have access to a trustworthy, diverse and multilingual digital environment. Access to diverse content contributes to a pluralistic public debate and effective participation in democracy in a non-discriminatory manner.*

Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment.

Everyone should be able to access information on who owns or controls the media services they are using.

Online platforms, particularly very large online platforms, should support free democratic debate online. Given the role of their services in shaping public opinion and discourse, very large online platforms should mitigate the risks stemming from the functioning and use of their services, including in relation to misinformation and disinformation campaigns, and protect freedom of expression».

In tale ambito la tutela mira a salvaguardare lo "spazio pubblico digitale" sia come ambiente per realizzare la partecipazione e il coinvolgimento alla vita democratica di una comunità, sia come ambiente necessario per assicurare altri diritti e libertà fondamentali correlati, quali la «*freedom of expression and information*». V'è una evidente correlazione tra di essi: lo spazio digitale è il luogo in cui il pensiero e le opinioni possono formarsi, attraverso la possibilità della condivisione e del confronto, nonché attraverso il reperimento delle informazioni utili a formare i propri convincimenti ed è altresì il luogo in cui le proprie opinioni e il proprio pensiero, una volta formatosi, possa essere efficacemente veicolato a terzi, nelle forme tipiche della libertà di espressione e di informazione.

[63] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018.

Si tratta però di attività che sono rese possibili dalla necessaria intermediazione delle piattaforme, che accentrano poteri enormi, non solo sul piano delle facoltà e delle libertà individuali, ma anche su quelle di tenuta degli assetti democratici. È anche in considerazione di tali aspetti che il *Digital (Right and) Principle* in questione è stato consacrato nel testo della Dichiarazione. Il principio interviene in realtà in una direzione già solcata a livello normativo, rinvenendosi tracce in tal senso nei recenti regolamenti con cui si è inteso disciplinare la transizione al digitale e ad altri emanandi provvedimento normativi nel settore tecnologico, con una produzione ormai torrenziale da parte dell'UE[64].

A livello programmatico viene previsto l'impegno della Commissione europea, del Parlamento e del Consiglio a (i) continuare a salvaguardare tutti i diritti fondamentali *online*, in particolare la libertà di espressione e di informazione, che ricomprendere la libertà e il pluralismo dei *media*; (ii) supportare lo sviluppo e l'ottimale utilizzo delle tecnologie digitali per stimolare il coinvolgimento dei cittadini e la partecipazione democratica; (iii) adottare misure proporzionate per contrastare tutte le forme di contenuti illegali, nel pieno rispetto dei diritti fondamentali, compreso il diritto alla libertà di espressione e di informazione, senza imporre obblighi generali di sorveglianza o forme di censura; (iv) creare un ambiente digitale dove le persone sono protette contro la disinformazione, la manipolazione delle informazioni e altre forme di contenuti dannosi, incluso molestie e violenza di genere; (v) sostenere l'accesso effettivo a contenuti digitali che rispecchino la diversità culturale e linguistica dell'UE; (vi) rafforzare nelle perone l'autonomia e la capacità di compiere scelte libere e specifiche, limitando altresì lo sfruttamento delle vulnerabilità e dei pregiudizi, in particolare quelli generati da forme di pubblicità mirata[65].

5.8. Sicurezza, protezione ed *empowerment* (un ambiente digitale sicuro, protetto e tutelato, vita privata e controllo individuale sui dati, protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale)

Il quinto principio, «*Safety, security and empowerment*», viene declinato nel *Chapter* V della Dichiarazione in parola con statuizioni articolate in tre distinte sessioni: la prima intitolata «*A protected, safe and secure digital environment*», la seconda intitolata «*Privacy and individual control over data*» e la terza intitolata invece «*Protection and empowerment of children and young people in the digital environment*»[66].

---

[64] Cfr., *ex multis*, il Reg. UE 2022/206, relativo a un mercato unico dei servizi digitali (*Digital Services Act*), nonché il Reg. UE 2022/1925, relativo a mercati equi e contendibili nel settore digitale (*Digital Markets Act*). Si veda anche il Reg. UE 2019/1150, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione *online*.

[65] Il tema è avvertito anche sul fronte delle scelte elettorali, politiche e referendarie. In materia, anche per quanto attiene agli interventi normativi dell'UE, cfr. D. Sborlini, *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo*, in *Dir. inf.*, 2022, 6, pp. 1173 ss.

[66] La traduzione italiana del *Chapter* V è stata resa, a livello istituzionale, con una maggiore esplicitazione del termine «*empowerment*», nel senso di seguito specificato: «Capitolo V: sicurezza, prote-

All'interno della sessione dedicata a "un ambiente digitale sicuro, protetto e tutelato", la Dichiarazione contiene la statuizione del principio secondo cui «*Everyone should have access to digital technologies, products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability and authenticity of the information processed*». V'è qui un chiaro riferimento ai principi di sicurezza e di *privacy by design* enucleati da tempo nell'ambito della disciplina normativa in materia di protezione dei dati personali.

L'impegno affermato in via programmatica, corrispondente a tale statuizione di principio, è quello di (i) adottare ulteriori misure per promuovere la tracciabilità dei prodotti e assicurare che nel mercato unico digitale siano offerti solo prodotti sicuri e conformi alla normativa dell'UE, (ii) proteggere gli interessi delle persone, delle imprese e delle pubbliche istituzioni dai rischi di cibersicurezza e dalla criminalità informativa, compreso e violazioni di dati (*data breaches*), che in realtà hanno un'accezione più ampia, potendo essere ricollegate anche a violazione di dati personali non riconducibili a fenomeni criminosi, ma che comportino comunque una perdita o una distruzione dolosa o accidentale dei dati, una compromissione della riservatezza, con apprensione di dati da parte di soggetti non autorizzati o una mancanza di disponibilità dei dati personali qualora sia invece necessario procedere al loro trattamento. La Dichiarazione include poi in tale ambito anche la protezione dell'identità digitale contro il "furto" o la "manipolazione" dell'identità, nonché i requisiti di cibersicurezza per i prodotti connessi, immessi sul mercato unico; (iii) contrastare e far valere le responsabilità di quanti cerchino di minare la sicurezza *online* e l'integrità dell'ambiente *digitale* all'interno dell'UE e di quanti promuovano la violenza e l'odio attraverso gli strumenti digitali.

Nella sezione dedicata a "Vita privata (*privacy*) e controllo individuale sui dati", invece, si trova esplicitato che «*Everyone has the right to privacy and to the protection of their personal data. The latter right includes the control by individuals on how their personal data are used and with whom they are shared.*

Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and not to be subjected to unlawful online surveillance, unlawful pervasive tracking or interception measures.

Everyone should be able to determine their digital legacy, and decide what happens with their personal accounts and information that concerns them after their death».

Si ha, qui, una insistenza sul diritto alla protezione dei dati personali, nei suoi molteplici aspetti, già abbondantemente esplorati dalla disciplina di settore, con particolare riguardo all'art. 8 della Carta dei diritti fondamentali dell'UE e dal GDPR. Si trovano però ulteriori specificazioni, sia con riguardo alla tutela esercitabile anche nei confronti delle comunicazioni e delle informazioni che facciano uso dei propri dispositivi elettronici, sia con riguardo al diritto a non essere sottoposti ad un'illecita attività di sorveglianza o di intercettazione *online*. L'ultima parte delle statuizioni di principio sopra riportate hanno invece una portata additiva rispetto alla disciplina europea in tema di *data protection*, che esclude dall'ambito applicativo i dati relative

zione e conferimento di maggiore autonomia e responsabilità».

a persone decedute. Nel nostro ordinamento trovano una specifica e limitata disciplina, contenuta nel codice della *privacy* a seguito della novellazione avutasi in forza della riforma del 2018, ad opera del d.lgs. 101/2018, ma nel testo della Dichiarazione si va decisamente ben oltre, affermandosi il diritto alla *digital legacy*, non considerato nell'impianto del GDPR.

Anche la declamazione dei *rights and principles* di tale sezione viene accompagnata dalla formulazione di specifici impegni in via programmatica, che tuttavia appaiono riduttivi nel complesso, soprattutto nella parte in cui trascura la *digital legacy*. L'attenzione viene posta sull'impegno a (i) garantire che ogni persona abbia un controllo effettivo sui propri dati personali e non personali, in linea con la disciplina europea in materia di protezione dei dati personali e con le altre discipline pertinenti (si pensi al *Data Governance Act*, Reg. UE 868/2022), (ii) garantire l'effettiva possibilità per gli individui di trasferire facilmente i propri dati personali e non personali tra diversi servizi digitali, in linea con i diritti di portabilità già previsto nel GDPR, esteso anche ai dati non personali (secondo l'approccio volto a favorire il riuso dei dati, ampiamente rimarcato nel *Data Governance Act*), (iii) proteggere efficacemente le comunicazioni dall'accesso non autorizzato di terzi, (iv) vietare l'identificazione illecita e la conservazione illecita delle registrazioni delle attività svolte *online*.

Nella terza sezione del *Chapter* V, dedicata alla protezione dei bambini e dei e al conferimento di una loro maggiore autonomia e responsabilità nell'ambiente digitale, la Dichiarazione statuisce che «*Children and young people should be empowered to make safe and informed choices and express their creativity in the digital environment.*

Age-appropriate materials should improve experiences, well-being and participation of children and young people in the digital environment.

Specific attention should be paid to the right of children and young people to be protected from all crimes, committed via or facilitated through digital technologies».

Si tratta di aspetti particolarmente delicati, in quanto il livello di partecipazione all'ambiente digitale di giovani e bambini deve essere accompagnato da un adeguato regime di sicurezza, con standard di maggiore severità per la loro tutela, e rapportato in ogni caso alla capacità di agire prevista nei regimi giuridici degli Stati membri, evitando che, nell'ambiente digitale, venga scavalcata la funzione di chi esercita la responsabilità genitoriale sui minori.

L'impegno affermato nella dichiarazione, con riguardo ai principi individuati in tale sezione, è, innanzitutto, quello di (i) offrire a tutti i bambini e i giovani le opportunità per acquisire le necessarie capacità e competenze per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate, ad iniziare dall'alfabetizzazione mediatica e dallo sviluppo del pensiero critico. Gli ulteriori impegni mirano poi a (ii) promuovere esperienze positive per i bambini e per i giovani, in un ambiente digitale sicuro e adeguato alla loro età, nonché a proteggerli sia (iii) dai contenuti nocivi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi online, impedendo che lo spazio digitale sia utilizzato per commettere o facilitare reati a loro danno, sia (iv) dal tracciamento, dalla profilazione e dal *targeting* illegali, in particolare a fini commerciali. Ulteriore significativo impegno delle istituzioni europee in tale direzione mira al (v) coinvolgimento dei bambini e

dei giovani nell'elaborazione delle politiche digitali che li riguardano, facendo sì che l'ambiente digitale sia ideato e sviluppato sempre più tenendo conto anche delle loro necessità, delle loro caratteristiche e delle loro aspettative.

Nel complesso l'elaborazione del *Digital Principle* di cui al *Chapter* V è, dunque, ricco di sfumature. Se, da un lato, la sicurezza, la protezione dell'ambiente digitale e l'*empowerment* sono funzionali alle esigenze di tutela della persona e dei propri diritti e libertà fondamentali, dall'altro lato sono anche preordinate alla realizzazione di spazi in cui si sviluppa la socialità e l'economia, dando luogo ad aggregazioni sociali e a mercati. In questa prospettiva, la sicurezza dell'ambiente digitale è anche il presupposto per lo sviluppo della personalità individuale, per la realizzazione delle dinamiche sociali e dei processi democratici, ma anche per lo sviluppo e lo svolgersi dei nuovi mercati digitali, che proprio sui dati personali poggiano – ora più che mai – le loro solide basi.

5.9. Sostenibilità

Il sesto ed ultimo principio, individuato nel *Chapter* VI della Dichiarazione, è invece incentrato sulla «*Sustainability*». Con riguardo ad esso la Commissione, nel documento che accompagna la (proposta di) dichiarazione, ha avuto modo di rimarcare che «*Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices*. (…) *The digital and green transitions are closely linked. While digital technologies offer many solutions for climate change, we must ensure they do not contribute to the problem themselves. Digital products and services should be designed, produced, and disposed of in a way that reduces their impact on the environmental and society. There should also be more information regarding the environmental impact and energy consumption of such services*»[67].

Nel testo definitivo della Dichiarazione, il principio di sostenibilità viene affermato con due statuizioni. Nella prima, di carattere oggettivo, si ribadisce che «*To avoid significant harm to the environment, and to promote a circular economy, digital products and services should be designed, produced, used, repaired, recycled and disposed of in a way that mitigates their negative impact on the environmental and society and avoids premature obsolescence*». Con la seconda, di carattere soggettivo perché mira alla possibilità di esercizio di scelte responsabili nei confronti dell'ambiente, si afferma invece che «*Everyone should have access to accurate, easy-to-understand information on the environmental impact and energy consumption of digital products and services, their reparability and lifetime, allowing them to make responsible choices*».

In via programmatica si prevede, in corrispondenza di tale principio, che la Commissione europea, il Parlamento e il Consiglio si impegnino a: (i) favorire lo sviluppo e l'uso di tecnologie digitali sostenibili, che abbiano un impatto negativo minimo sulla società e sull'ambiente; (ii) incentivare scelte di consumo e modelli aziendali sostenibili e promuovere un comportamento sostenibile e responsabile del-

[67] COMMISSIONE EUROPEA, *European Digital Rights and Principles*, cit.

le imprese lungo tutte le catene globali del valore dei prodotti e dei servizi digitali, anche per contrastare il lavoro forzato *(forced labour*); (iii) promuovere lo sviluppo, la diffusione e l'uso attivo di tecnologie digitali innovative, che abbiano un impatto positivo sull'ambiente e sul clima, al fine di accelerare la c.d. transizione verde (*green transition*); ad, infine, (iv) promuovere norme e marchi di sostenibilità per i prodotti e i servizi digitali.

6. Una lettura circolare: dai *Digital Principles* ai principi in materia di protezione dei dati personali

6.1. La circolarità del discorso

Dal discorso finora condotto si possono tracciare alcune considerazioni conclusive, che si collocano in un percorso di riflessione connotato da una certa circolarità: muovendo dai principi in materia di protezione dei dati personali, l'indagine ha allargato i propri orizzonti ai nuovi principi elaborati nel mondo digitale, ma, come si vedrà, finisce poi per ritornare nuovamente ai principi rilevanti in materia di dati personali, che costituiscono il punto di partenza e di arrivo del ragionamento che si sta conducendo.

Nell'ambito di questo ragionamento circolare, mi preme condividere alcune riflessioni, emergenti dal quadro finora delineato.

6.2. Verso una "costituzionalizzazione" dei nuovi diritti e principi digitali

In primo luogo mi pare evidente che si sia aperta la strada che porta all'effettiva "costituzionalizzazione", a livello europeo, dei nuovi diritti e principi digitali[68].

[68] A tal riguardo si veda, ancora una volta, S. Rodotà, *Una Costituzione per Internet?*, cit., pp. 348 ss., per il quale «Cimentarsi con il problema della "*costituzione di Internet*", del modo complessivo in cui la tecnologia incontra il tema delle libertà e istituisce lo spazio politico, significa proprio fare i conti con processi reali. Le trasformazioni determinate dalla tecnologia possono essere comprese, e governate, solo se si è capaci di mettere a punto strumenti "prospettici", e se questo avviene ridefinendo i principi fondativi delle libertà individuali e collettive». Si tratta di una «(…) questione che riguarda non più la sola forma o procedura di una *costituzione per Internet*, ma pure i suoi *contenuti*. Qui *s'intrecciano finalità d'ordine generale, veri e propri principi direttivi, con la loro traduzione in specifici diritti*. Se, ad esempio, si muove dalla constatazione che Internet rappresenta il più largo spazio pubblico che l'umanità abbia conosciuto, la salvaguardia di questa sua "natura" implica l'irriducibilità alla dimensione sempre più assorbente del mercato, che vuol dire non solo un generico riconoscimento della *libertà in rete*, ma la concreta possibilità di esercitare "*virtù civiche*", dunque di dar corpo ad una *cittadinanza attiva*; di far sì che Internet rimanga una risorsa per la *democrazia* e non la forma congeniale ai nuovi populismi; di praticare forme economiche riconducibili alla logica del dono. Da qui la necessità di salvaguardare la *neutralità della rete*, anche come antidoto a ogni forma di censura e il suo potenziale "generativo", dunque l'effettiva sua capacità di produrre innovazione. Da qui la necessità di considerare l'*accesso a Internet* come un *diritto fondamentale della persona*, secondo una *linea costituzionale* che si ritrova in dichiarazioni del Parlamento europeo e del Consiglio d'Europa, in iniziative di Stati come la Finlandia, nel piano del Presidente Obama sul servizio universale. Ma il riconoscimento dell'accesso non può divenire una chiave che

Emerge la lungimiranza del pensiero di Stefano Rodotà. A distanza di molti anni dall'auspicata *Internet Bill of Rights* si è avuto il riconoscimento istituzionale della necessità di una "riscrittura" dei valori e dei principi applicabili ad Internet, prima con la nostrana Dichiarazione dei diritti di Internet, fatta propria dalla Camera dei Deputati, poi con la *European Declaration on Digital Rights and Principles*, promossa nel gennaio del 2022 dalla Commissione europea, destinata ad essere adottata congiuntamente dalla Commissione medesima, dal Parlamento europeo e dal Consiglio.

La parziale battuta d'arresto nei confronti di quanto auspicava Stefano Rodotà, registratasi con il mancato accoglimento della proposta di modifica della Costituzione italiana con la quale si voleva l'introduzione dell'art. 21-*bis* (su cui s'è riferito *supra*), pare destinata a essere superata attraverso il formale riconoscimento dei diritti e dei principi digitali con la Dichiarazione del Parlamento europeo, del Consiglio e della Commissione europea, la cui pubblicazione in G.U.U.E., avvenuta a gennaio 2023, costituisce senz'altro una tappa importante per la progressiva "costituzionalizzazione" dei nuovi principi e diritti fondamentali. Ed è proprio questo un aspetto decisivo: la visione dichiaratamente antropocentrica voluta dall'UE per lo sviluppo dell'ambiente digitale in Europa reclama un approccio deciso, volto a ripensare i diritti, le libertà e i principi fondamentali nel mondo digitale, su cui si innervano oggi le relazioni sociali ed economiche. Ciò porterà alla inevitabile "costituzionalizzazione" dei nuovi *Digital Rights and Principles*, con cui dovremo misurare l'intero sistema normativo[69].

---

apre una stanza vuota: da qui la necessità di considerare la *conoscenza come bene pubblico globale*, non solo rivedendo categorie tradizionali come quelle del brevetto e del diritto d'autore, ma evitando fenomeni di "chiusura" rispetto a questo *common*, che caratterizza appunto la nostra società come quella "della conoscenza", trasformando in risorsa scarsa un bene comune suscettibile della più larga utilizzabilità. Da qui la necessità di una *tutela dinamica dei dati personali*, nel senso che la garanzia non può essere soltanto quella tradizionale e statica relativa alla riservatezza, ma deve divenire *componente essenziale della cittadinanza digitale e della libera costruzione dell'identità* (considerando, per esempio, il diritto di anonimato, particolarmente rilevante nel caso del dissidente politico, e il diritto all'oblio), *passando così dal riconoscimento dell'autodeterminazione informativa ad una effettiva redistribuzione del potere in rete*. Tutto questo, ovviamente, deve essere considerato nella prospettiva della destrutturazione/ricostruzione del rapporto tra sfera pubblica e sfera privata. E proprio riflettendo su Internet possono essere individuate le vie di un *costituzionalismo globale* possibile, non affidato a una *vertical domestication*, con norme sovrastatuali incorporate nei diritti statuali, né semplicemente translocale. Dunque una costruzione del diritto per espansione, orizzontale, un insieme di ordini giuridici correlati, quasi una costituzione infinita» (*Ibidem*).

[69] La dottrina giuspubblicistica ha affermato la natura "costituzionale" dei nuovi diritti, anche ove non formalizzati in un testo scritto, ma evincibili in via interpretativa: «Emergono, infatti, dalla coscienza sociale, e a seguito dello sviluppo tecnologico, dei "nuovi diritti", i quali, sebbene non godano di un loro esplicito riconoscimento normativo, hanno un forte e chiaro "tono costituzionale", che li collocano, implicitamente, all'interno della costituzione, riservando all'interprete il compito di estrapolarli da essa. (…) La sfida che nel Ventunesimo secolo attende il costituzionalismo è, prevalentemente, quella riferita alla tecnologia, ovvero come dare forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica e i suoi derivati in punto di diritto». Così T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, cit., pp. 465 s.

Per la verità nella Dichiarazione, al punto n. 10 del Preambolo, si trova affermato che essa «ha *natura dichiarativa* e, in quanto tale, *non incide sul contenuto delle norme giuridiche o sulla loro applicazione*». Al contempo viene però rimarcato che la Dichiarazione «si basa segnatamente sul diritto primario dell'UE, in particolare sul trattato sull'Unione europea, sul trattato sul funzionamento dell'Unione europea, sulla Carta dei diritti fondamentali dell'Unione europea nonché sul diritto derivato e sulla giurisprudenza della Corte di giustizia dell'Unione europea», con l'ulteriore significativa precisazione che essa «trae inoltre spunto dal pilastro europeo dei diritti sociali e lo integra».

L'asserita natura "dichiarativa" del documento in questione, volto ad affermare principi e diritti nel nuovo contesto digitale, non è per la verità decisiva al fine di escludere anche una *natura "normativa"* alla Dichiarazione medesima. Se, come è dato evincere, siamo in presenza di principi e diritti fondamentali, che riguardano l'uomo in quanto tale, secondo la nota tesi rimarcata da Francesco Galgano, l'ordinamento non "crea" i diritti in questione, che sono preesistenti ad esso, in quanto connaturati con l'esistenza umana, ma si limita a "riconoscerli", ossia ad individuarli e a proteggerli[70]. La natura dichiarativa delle statuizioni non scalfisce, in tale ambito, la portata giuridico-normativa delle dichiarazioni con cui si effettua il riconoscimento dei nuovi diritti fondamentali dell'uomo nel contesto digitale. Né è di ostacolo il fatto che si tratti di "nuovi" diritti e principi fondamentali, in quanto il catalogo dei diritti fondamentali è, in tale costruzione, aperto al riconoscimento di diritti di nuova generazione, là dove si presenta un'esigenza di protezione dell'uomo in relazione al progresso tecnologico. Così è stato per il diritto alla *privacy*, teorizzato solamente nel 1890, e, più recentemente, per il diritto alla protezione dei dati personali, di cui all'art. 8 della Carta dei diritti fondamentali dell'UE. La circostanza che l'ordinamento giuridico provveda a riconoscere "nuovi" diritti in epoca più recente rispetto ai più tradizionali e vetusti diritti fondamentali non porta ad affermare che i diritti in questione siano diritti creati dall'ordinamento: aderendo alla tesi monista dei diritti fondamentali dell'uomo, che costituiscono forme di tutela dell'unitaria personalità umana, deve ammettersi che il rinvenimento di nuove esigenze di tutela, al cospetto dei mutamenti indotti dal progresso tecnologico, porta non alla "creazione" di un nuovo diritto, prima inesistente, ma al "riconoscimento" attuale di esigenze di tutela di quell'unitaria e preesistente personalità umana che il diritto fondamentale intende proteggere. L'operazione volta ad individuare, con intenti dichiarativi, nuovi *Digital Rights and Principles*, al cospetto del progresso tecnologico, fa dunque parte del processo di "riconoscimento" attuale di quei diritti e di quelle libertà fondamentali che afferiscono all'unitaria personalità umana, collocata nel suo ineliminabile contesto inter-relazionale, sociale ed economico. Siamo, in altre parole, al cospetto di dichiarazioni di "riconoscimento" di quei diritti che vanno ad ampliare il catalogo dei diritti fondamentali di rilevanza "costituzionale", nell'ambito del contesto digitale, oggi pervasivo.

Il Parlamento europeo, la Commissione europea e il Consiglio hanno affermato che la Dichiarazione avrebbe inoltre natura non solo dichiarativa, ma anche

[70] Cfr. F. Galgano, *Tratto di diritto civile*, vol. I, cit., pp. 171 ss.

politica. Neanche tale affermazione mi pare adeguata a scalfire la natura normativa dei diritti e dei principi declinati nella Dichiarazione medesima. Come s'è potuto esaminare *supra*, infatti, il documento in parola è strutturato in parti enunciative di principi e diritti, con statuizioni di portata generale, a cui si accompagnano, separati in maniera netta per ciascun principio e diritto, le dichiarazioni di impegno con cui si intende agire a livello programmatico. Saranno semmai le dichiarazioni di impegno ad avere una valenza politica e programmatica, non le statuizioni a monte, enunciative dei principi e dei diritti fondamentali in ambiente digitale, che conservano invece tutta la loro rilevanza sul piano giuridico-normativo. È in questo senso che va letta la parte iniziale del punto n. 12 del Preambolo, ove si previsa che «La promozione e l'attuazione della dichiarazione rappresentano un *impegno politico* e una responsabilità che condividono l'UE e gli Stati membri nell'ambito delle rispettive competenze e nel pieno rispetto del diritto dell'Unione (…)».

6.3. L'embrionale fase di "riscrittura" dei nuovi diritti e principi digitali e prospettive di successivo ampliamento

In secondo luogo, mi pare che il percorso di "riscrittura" dei nuovi *Digital Rights and Principles*, avviato in Italia con la «Dichiarazione dei diritti di Internet» e, nell'Unione europea, con la «Dichiarazione europea sui diritti e i principi digitali per il decennio digitale», sia solamente in fase embrionale, nel senso che il riconoscimento e la scrittura di tali diritti e principi fondamentali nel nuovo contesto tecnologico è solamente in una fase iniziale e sia destinato a proseguire, aumentando il novero dei diritti, delle libertà e dei principi fondamentali applicabili al mondo digitale. Ciò si lascia presagire anche al cospetto di evoluzioni tecnologiche ulteriori, destinate a diffondersi in maniera pervasiva nel tessuto sociale ed economico e a livello istituzionale, come sta avvenendo per l'intelligenza artificiale, la robotica, i processi decisionali basati su algoritmi e *big data*. Ci sarà un'ulteriore espansione e un'ulteriore ridefinizione, nel prossimo futuro, dei *Digital Rights and Principles*, nel cammino che porterà alla loro "costituzionalizzazione". Ciò, del resto, è in sintonia con il "catalogo" aperto dei diritti fondamentali e dei principi, su cui discuteva Francesco Galgano[71] e Guido Alpa[72].

6.4. Nuovi diritti e principi digitali e trattamento di dati personali

In terzo luogo si è potuto osservare come il primo nucleo dei diritti e principi fondamentali elaborati con riferimento al contesto digitale, sia nell'esperienza italiana che in quella europea – rispettivamente con la "Dichiarazione dei diritti di Internet" e con la "*European Declaration on Digital Rights and Principles for the Digital Decade*" – poggi su un nucleo elaborato e definito nel settore della protezione dei dati personali.

---

[71] Sul catalogo "aperto" di diritti fondamentali dell'uomo v. F. GALGANO, *Trattato di diritto civile*, vol. I, cit. p. 173.

[72] Sul numero "aperto" dei principi v. G. ALPA, *I principi generali*, cit., p. 298.

Occorre considerare che le tecnologie digitali necessitano ontologicamente, per il loro funzionamento, del trattamento di dati e quando – com'è inevitabile – tali dati afferiscono a persone fisiche identificate o identificabili, il trattamento di dati personali costituisce il presupposto stesso del funzionamento delle tecnologie digitali. Sicché il sistema di protezione della persona nell'ambiente digitale ha, come fulcro, la disciplina della *data protection*. Si comprende bene, dunque, la rilevanza dell'affermazione di Stefano Rodotà secondo cui il diritto alla protezione dei dati personali è non solo diritto fondamentale esso stesso, ma è anche precondizione per l'esercizio di altri diritti fondamentali[73]. È pertanto fisiologico che nella definizione dei nuovi diritti e principi digitali il loro nucleo sia costituito dai diritti e dai principi elaborati in materia di protezione dei dati personali.

Lo studio del diritto alla protezione dei dati personali e dei principi individuati in tale specifica materia è fondamentale per comprendere appieno i nuovi *Digital Rights and Principles* applicabili nel più vasto contesto del mondo digitale, dovendosi rinvenire un legame funzionale tra i primi e i secondi.

6.5. Valenza "interna" ed "esterna" dei principi in materia di protezione dei dati personali

Alla luce di tali considerazioni, lo studio dei principi in materia di protezione dei dati personali, in particolare quelli di cui al GDPR, ha una duplice valenza: una del tutto "interna" alla disciplina della *data protection*, in quanto volta a individuare l'inquadramento normativo, la portata del principio e, soprattutto, l'applicazione alla casistica concreta, nella prospettiva giusrealistica, al fine di far emergere in che modo vengano a realizzarsi la funzione "adeguatrice" e la funzione "ordinante" dei singoli principi, al cospetto delle norme disciplinanti la protezione dei dati personali: l'altra si ricollega alla comprensione e allo studio del più ampio ventaglio dei nuovi *Digital Rights and Principles*, generalmente applicabili ad ogni contesto digitale in cui le relazioni sociali, commerciali e istituzionali vengono a svolgersi.

L'intera ricerca condotta sui principi in materia di protezione dei dati personali, i cui esiti sono racchiusi in questo volume – pur mirando, in prospettiva, anche alla seconda delle due direzioni ora tracciate – si concentra sulla prima di esse, puntando all'analisi dei singoli principi rilevanti in tema di *data protection*, codificati e non codificati espressamente, sui quali poggia l'intera impalcatura della disciplina emanata in tale specifico settore, i cui principali riferimenti si hanno nell'art. 8 della Carta dei diritti fondamentali dell'UE e nel Reg. UE 679/2016 (GDPR), con particolare riguardo all'art. 5.

L'indagine su ogni principio individuato nel sistema normativo della *data protection* è tripartita, snodandosi dall'inquadramento normativo, anche in senso diacronico, alla portata del principio come emerge nel dibattito dottrinale e istituzionale, fino ad arrivare all'applicazione del singolo principio nella casistica. L'aderenza al

[73] Ancora una volta, il riferimento è a S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, cit., p. 4,

diritto vivente è fondamentale per comprendere come il principio viene interpretato ed applicato sul piano normativo, in funzione ordinante e adeguatrice[74].

6.6. Funzioni e caratteristiche dei principi in materia di protezione dei dati personali. "Principi-valore" e "principi-funzionali"

6.6.1. *La scelta sistematica del legislatore europeo: i principi nel GDPR*

Il GDPR, dopo l'impianto definitorio (che, con l'art. 4, chiude il Capo I sulle «*Disposizioni generali*», dedicato anche all'individuazione dell'oggetto e delle finalità della disciplina in parola, nonché all'ambito di applicazione materiale e territoriale del Regolamento), si premura di enunciare i singoli «*principi*» applicabili al trattamento di dati personali, anticipatori delle disposizioni di dettaglio contenute nelle restanti disposizioni di tale *corpus* normativo. Significativo è il titolo del Capo II, lapidariamente dedicato ai «*Principi*», il cui articolo di apertura, l'art. 5, è rubricato, in maniera più puntuale, «*Principi applicabili al trattamento di dati personali*», seguito dalle disposizioni sulle condizioni di liceità del trattamento[75].

Vengono in tal senso ripercorse, con diversi aggiustamenti, soluzioni già rinvenibili nel precedente impianto normativo, tanto nella direttiva 95/46/CE, quanto nelle norme di attuazione di cui – da ultimo – al d.lgs. 196/2003. Nella direttiva veniva tracciata la distinzione tra «*Principi relativi alla qualità dei dati*» (Sezione I, art. 6) e «*Principi relativi alla legittimazione del trattamento dei dati*» (Sezione II, art. 7). Una simile ripartizione era riscontrabile anche nella normativa di recepimento, nella quale, tuttavia, s'era perso sovente il riferimento testuale al lemma «*principio*»[76]. Nel GDPR viene mantenuto il riferimento ai «*Principi*», a cui viene

[74] Utilizzando le parole di N. LIPARI, *op. cit.,* pp. 119-120, si ricorda che «L'ottica dei principi ci aiuterà ad assumere – con i rischi, ma anche con le ricchezze che questo comporta – un ruolo attivo e costruttivo, diverso da quello, passivo e deduttivo, al quale siamo stati educati. (…) Non si può negare che il paradigma delle fonti è uno schema rigido, quello del *diritto vivente* riconduce alla dinamicità. Vivere significa proporsi uno scopo da raggiungere, un obiettivo da conseguire, un *valore* da difendere. Noi, come giuristi, siamo dentro questa vita, con tutta la duttilità che ciò comporta; non semplici lettori di traguardi da altri posti» (l'uso del corsivo è di chi scrive).

[75] In materia si vedano le riflessioni già illustrate, a tal riguardo, in F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 101-178 ed, *ivi*, spec. 103-111, che in queste pagine si riprendono, seppur nel diverso contesto del discorso che si sta conducendo in questa sede.

[76] I primi («*Principi relativi alla qualità dei dati*») contemplavano la necessità che i dati personali oggetto di trattamento venissero «trattati lealmente e lecitamente», «per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità», «adeguanti, pertinenti e non eccedenti rispetto alle finalità» della raccolta e del successivo trattamento, «esatti e, se necessario, aggiornati», nonché «conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati» (art. 6, par. 1, dir. 95/46/CE). Tali "principi" (indicati per lo più come principio di liceità e correttezza del trattamento, di finalità, di pertinenza, completezza ed aggiornamento, di stretta necessità, etc.) hanno avuto un'attuazione, nella legislazio-

intitolato il Capo II, nel quale si trovano collocate sia le norme sulle modalità del trattamento e sulla qualità dei dati (rinvenibili, segnatamente, al già citato art. 5, rubricato «*Principi applicabili al trattamento di dati personali*»), sia le norme sui diversi "presupposti legittimanti" il trattamento dei dati personali, che nel regolamento assumono la denominazione di "condizioni di liceità" del trattamento, tra le quali ricopre un ruolo di rilievo il consenso, anche se non in grado di assurgere a regola di carattere generale, essendo presupposto alternativo ed equiordinato rispetto agli altri previsti dal dettato normativo.

6.6.2. *La funzione dei principi in materia di protezione dei dati personali e l'aderenza diretta e indiretta al piano assiologico: "principi-valore" e "principi-funzionali"*

La scelta sistematica di far precedere l'enunciazione dei principi all'articolato normativo contenente le più specifiche regole disciplinanti la materia *de qua* è decisamente apprezzabile, sia per la riferita funzione "ordinante"[77] riconosciuta ai *principi*[78], con cui l'interprete del diritto è in grado di individuare le regole applica-

ne domestica, nell'ambito di disposizioni normative dedicate alla «*Modalità di raccolta e requisiti dei dati personali*» (cfr. art. 9 l. n. 675 del 1996 e, successivamente, art. 11 d.lgs. n. 196 del 2003, Codice in materia di protezione dei dati personali, poi abrogati). La seconda categoria di "principi" («*Principi relativi alla legittimazione del trattamento dei dati*»), invece, vale ad individuare il presupposto che legittima il titolare del trattamento a trattare i dati personali dell'interessato, sulla base di diversi criteri alternativi, nell'ambito dei quali era presente, *in primis*, il consenso dell'interessato, annoverato accanto ad altri presupposti di legittimazione, che – nell'impianto della direttiva cit. – apparivano equipollenti, non potendosi dirsi in rapporto di regola ed eccezione con il criterio del consenso. Nelle norme di recepimento della direttiva 95/46/CE, invece, il legislatore sembrava avesse voluto indicare – almeno formalmente – il criterio del «consenso» come "presupposto di legittimazione" o come "condizione di liceità" del trattamento per il trattamento svolto da parte di soggetti privati o di enti pubblici economici, facendolo assurgere a regola generale, alla quale poi sottrarre le ipotesi di eccezione, individuando i casi specifici di esclusione del consenso (v. artt. 11 e 12 l. n. 675 del 1996, nonché artt. 23 e 24 d. lgs. n. 196 del 2003, poi abrogati). Sul versante dei trattamenti effettuati da parte di soggetti pubblici, viceversa, il consenso era invece di norma escluso, anche quando il trattamento avesse ad oggetto dati sensibili, occorrendo tuttavia pur sempre che vi fosse un'espressa previsione di legge nella quale siano specificate le finalità di rilevante interesse pubblico perseguite (v. art. 20, co. 1, d. lgs. n. 196 n. 2003, poi abrogato), nonché che fossero specificati – sempre dalla legge o, in difetto, da un atto di natura regolamentare – i tipi di dati che potessero essere trattati e i tipi di operazioni eseguibili (cfr. G. Finocchiaro, Privacy *e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, p. 60). Sicché qui la regola generale era data dalla presenza di un rilevante interesse pubblico, individuato *ex lege*, che fungeva da presupposto di legittimazione (ma il consenso tornava ad essere richiesto qualora il trattamento di dati idonei a rivelare lo stato di salute fosse svolto in ambito sanitario da esercenti professioni sanitarie e organismi sanitari pubblici, *ex* art. 76, d.lgs. n. 196 n. 2003, per cui il consenso era ipotesi di eccezione nell'ambito del trattamento svolto da soggetti pubblici, con inversione rispetto a quanto avviene nei trattamenti svolti da privati o da enti pubblici economici).

[77] Parla di «funzione ordinante» (o stabilizzante) del diritto S. Romano, *Frammenti di un dizionario giuridico*, Milano, 1947, pp. 80 ss. Si veda anche quanto illustrato nel par. 1.2 del presente contributo.

[78] Sulle diverse funzioni dei principi v., *amplius*, G. Alpa, *I principi generali*, cit., pp. 17 ss., tra le quali vengono individuate quella «*normativa*», quella «*interpretativa*» e quella «*integrativa*», che si muovono nel solco della tradizione, nonché altre funzioni «che si sono affacciate solo di recente

bili al caso concreto anche là dove non ve ne siano per la fattispecie concreta, sia, al contempo, per la funzione "integrativa" e "adeguatrice" dei principi medesimi, che consentono di guidare l'interprete nell'applicazione delle clausole generali[79] e delle norme dettate per la disciplina delle fattispecie[80], offrendo un solido fondamento per la loro applicazione anche là dove la mutevolezza indotta dal progresso tecnologico[81] sia tale da richiedere necessari adeguamenti a livello interpretativo, non direttamente evincibili dalla norma regolante la fattispecie[82].

La dottrina ha chiarito che le funzioni generalmente attribuite ai principi sono normalmente ravvisabili nella funzione normativa (ordinante) e nella funzione interpretativa, a cui si aggiunge una «terza funzione fondamentale, aggregata alla prima o alla seconda, o considerata autonoma, la funzione "integrativa"»[83], o "adeguatrice",

---

nell'arena dei principi», quali quella «*costitutiva*», quella «*razionalizzatrice*», quella «*economica*», quella «*garantista*», quella «*ideologica (od euristica)*» e quella «*connettiva*». Avverte l'A. cit., *ivi* pp. 27 e 28, che le «diverse funzioni dei principi legittimano (…) l'interprete a considerarle tutte operanti attraverso formule combinatorie, di volta in volta applicate in modo consapevole o spesso anche in modo non consapevole, per via tralatizia e irriflessa. Questa coesistenza di significati e di ruoli esclude che le diverse tesi via via affacciatesi nell'itinerario accidentato dei principi possano considerarsi definitive o esaustive. In altri termini, i principi con funzione normativa costituiscono mezzi di autointegrazione del sistema giuridico, là dove l'interprete ritenga che sussistano lacune da colmare, o là dove – se le lacune fossero considerate finzioni –, la regola da applicare si possa ricostruire sulla base di un processo induttivo derivato da altre regole simili; essi costituiscono anche mezzo di orientamento interpretativo; ma in quanto incorporanti valori politici, sociali, morali, economici, essi costituiscono anche strumenti di eterointegrazione dell'ordinamento, attraverso la mediazione dell'interprete».

79 Cfr. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, 3ª ed., Napoli, 2006, p. 224, il quale, dopo aver ribadito la valenza normativa dei principi, ricorda come questi ultimi, in uno con le istanze provenienti dalla realtà sociale, riempiano di valori le clausole generali presenti nell'ordinamento giuridico, non aventi valenza assiologica autonoma e compiuta. Sul punto si v. anche P. PERLINGIERI e P. FEMIA, *Nozioni introduttive e principi fondamentali del diritto civile*, 2ª ed., Napoli, 2004, pp. 16-34 ed. *ivi*, spc. pp. 28 ss. e 30 ss.

80 P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, cit., pp. 540 ss.

81 S. RODOTÀ, *Tecnologie e diritti*, cit., p. 42.

82 Sul ricorso ai principi in sede interpretativa e sulla loro funzione adeguatrice o integratrice, si rimanda, primariamente, a R. DWORKIN, *Taking rights seriously*, cit., nonché a S. BARTOLE, *Princìpi generali del diritto (dir. cost.)*, in *Enc dir.*, XXXV, 1986, pp. 494 ss., e, ivi, spec. par. 9, intitolato «*La teoria di Dworkin sulla funzione integratrice dei princìpi*».

83 G. ALPA, *I principi generali*, cit., p. 18. Secondo S. BARTOLE, *Princìpi generali del diritto (dir. cost.)*, cit., in un discorso che recupera anche la prospettiva programmatica su cui s'è insistito nei precedenti paragrafi, in particolare a proposito della *European Declaration on Digital Rights and Principles for Digital Decade*, COM(2022)28 final, « si sostiene che tre sono i tipi di funzioni che i princìpi svolgono di volta in volta, e così si distingue una funzione integratrice da una programmatica e, ancora, da altra definita interpretativa [E. BETTI, *Interpretazione della legge e degli atti giuridici*, Milano, 1971, p. 305 ss.]. In partenza tutti i princìpi hanno – si dice – le funzioni ora indicate, ma in realtà esse risultano diversamente qualificate, e talora persino annullate in relazione alle peculiarità del rapporto che intercorre fra i singoli princìpi e l'ordinamento nel suo complesso. Ciò è specialmente vero per la funzione integratrice, che è nulla allorquando princìpi generali espressi si limitino a disciplinare il comportamento di organi legislativi in ordine alla regolamentazione "che questi a loro volta daranno a quella certa materia" [V. CRISAFULLI, *La Costituzione e le sue disposizioni di principio*, Milano, 1952, p. 41 ss.]. Si può invece dire che i princìpi hanno valenza in-

anche se, come ben chiarito da Guido Alpa, «Le funzioni dei principi comunque non si esauriscono qui: anzi, con il tempo e con la dinamicità dei rapporti interni e internazionali i principi hanno finito per acquisire funzioni nuove»[84].

Mi pare che, proprio in materia di protezione dei dati personali, se si analizzano le caratteristiche dei principi ivi contemplati, possano emergere nuove funzioni dei principi, che possono leggersi in relazione ai valori di riferimento che il principio esprime e alla loro diretta o indiretta aderenza ad essi.

Si nota, cioè, che i principi in materia di protezione dei dati personali sono taluni direttamente ancorati al valore che intendono esprimere e che possiamo indicare con «*principi-valore*»[85], mentre altri, che presentano caratteristiche differenti, non esprimo direttamente il valore di riferimento: non per questo, tuttavia, cessano di essere "principi", né dunque mutano per questo la loro natura in "clausole generali"[86], ontologicamente diverse dai "principi" per via della mancata necessaria rispondenza al valore di riferimento[87].

---

tegratrice quando possono essere utilizzati per dare regolamentazione a casi cui non corrispondono norme specifiche. Il che si verifica – ad esempio – allorché i princìpi appartengono alla categoria di quelli inespressi in quanto desunti da norme di specie già vigenti nell'ordinamento; ovvero quando princìpi espressi siano stati accompagnati o seguiti da una solo parziale attuazione; ovvero, infine, nei casi in cui alla enunciazione di uno o più princìpi, disciplinanti fondamentalmente una data materia, non abbia fatto seguito alcuna normazione di attuazione. Non sembrano, invece, soffrire alcuna attenuazione o riduzione le altre due funzioni, quale che sia la situazione in cui si fa ricorso ai princìpi. E, perciò, sempre, di norma, essi potrebbero essere utilizzati in funzione interpretativa, per attribuire a disposizioni già vigenti di incerta o dubbia accezione significati coerenti ai princìpi medesimi. Ed egualmente a tutti indistintamente il legislatore potrebbe fare appello per trarre indirizzi e orientamenti da perseguire nell'attività legislativa, in tal modo valorizzandoli nella funzione programmatica».

[84] G. Alpa, *I principi generali*, cit., p. 18.

[85] Per l'uso dell'espressione «principi-valori» si veda anche G. Alpa, *I principi generali*, cit., p. 48 e spec. p. 51.

[86] È utile qui richiamare N. Lipari, *Diritto civile e ragione*, Milano, 2019, p. 115, ove l'A. afferma criticamente che «il tentativo di assimilare i principi alle clausole generali è niente più (…) che un espediente dialettico per salvare la coerenza di vecchie categorie ricostruttive, perché i principi non possono essere ricondotti semplicemente a regole elastiche offerte alla duttilità evolutiva dell'esperienza. Enza dire che le clausole generali hanno pur sempre un loro definito confine rappresentato dal fine che la singola clausola intende salvaguardare, mentre il principio riflette un criterio di *valore* che esige, volta per volta, di essere equilibrato con altri indici assiologici, non determinabili in astratto, ma legati alla peculiarità del caso che si tratta di disciplinare» (l'uso del corsivo è di chi scrive).

[87] Sia i principi che le clausole generali, com'è noto, sono connotate da una valenza normativa (i primi costituiscono una norma, le seconde un "frammento" di norma) e da una certa vaghezza dei contenuti, per l'assenza di una fattispecie di riferimento, e del carattere ampio e generale della formulazione usata per indicare gli uni e le altre, demandando all'interprete (solitamente il giudice) il compito di eliminare l'indeterminatezza, applicando il principio o la clausola generale al caso concreto, riducendo l'originario ventaglio applicativo derivante dall'ampia e generica formulazione. Il principio, tuttavia, contiene in sé un riferimento (diretto o indiretto) ad un valore, muovendosi sul piano assiologico. La clausola generale, a differenza del principio, non è, generalmente, espressione di un valore o di un principio di riferimento, ma va vista con riguardo alla sua funzione: è espressione di una tecnica legislativa volta a rimettere all'interprete il compito di adattare la norma alla fattispecie concreta, attraverso un processo di valutazione integrativa. Può capitare, ovviamente, che il legislatore faccia uso di clausole generali, sul piano della tecnica legislativa, per rispondere all'e-

Come meglio chiarito nel prosieguo del discorso, in materia di protezione dei dati personali, infatti, si rinvengono "principi" che *non* sono *direttamente* collegati con il valore di riferimento, ossia non costituiscono una diretta espressione di tale valore, ma si collocano in una posizione ancillare ad esso. Dunque, non rimangono estranei alla prospettiva assiologica, ma compaiono nell'ordinamento in funzione strumentale ad altro principio direttamente collegato al valore di riferimento, al fine di giungere ad una piena attuazione di tale sottostante principio e, dunque, del valore ad esso corrispondente. Essendo "funzionali" (o strumentali) al principio-valore

---

sigenza normativa tipica dei principi. In tal caso clausola generale e principi possono avvicinarsi e sovrapporsi sul piano applicativo, pur risultando *ex se* ontologicamente distinti.

Come ben precisato da S. RODOTÀ, *Il tempo delle clausole generali*, cit., p. 721, è possibile distinguere le clausole generali dai principi giacché «se con tale termine ci si riferisce alle indicazioni riguardanti i valori fondativi di un ordinamento o di una sua parte» può allora dirsi che «le clausole generali non sono principi, anzi sono destinate ad operare nell'ambito designato dai principi». Le clausole generali ricavano dunque la valenza assiologica dal collegamento con i principi.

Per quanto attiene alla tesi assiologica dei principi, che molto deve a Dworkin, v. G. ALPA, *I principi generali*, cit., p. 36 ss. e pp. 47 ss., nonché N. LIPARI, *op. cit*., p. 115.

Sulla semantica delle clausole generali si veda invece lo studio di V. VELLUZZI, *Osservazioni sulla semantica delle clausole generali*, cit., p. 1 ss. e, ivi, spec. p. 9, ma anche V. VELLUZZI, *Le clausole generali. Semantica e politica del diritto*, cit., p 74 ss. e, ivi, spec. p. 78, ove, dopo aver ricordato la definizione di clausola generale, intesa come «un termine o un sintagma di natura valutativa caratterizzato da indeterminatezza, per cui il significato di tali termini o sintagmi non è determinabile (o detto altrimenti le condizioni di applicazione del termine o sintagma non sono individuabili) se non facendo ricorso a criteri, parametri di giudizio, interni e/o esterni al diritto tra loro potenzialmente concorrenti», rimarca che «i principi sono norme, affatto peculiari, ma norme, mentre le clausole sono termini o sintagmi, vale a dire elementi, componenti di norme. Il dibattito intorno alla relazione tra principi del diritto e clausole generali è stato spesso sviluppato da una prospettiva infelice nella quale non si teneva conto della differenza appena segnalata. Al contrario, basandosi su di essa è possibile riportare la questione del rapporto tra principi del diritto e clausole generali sulla strada della loro non necessaria sovrapposizione/coincidenza». Ancora, l'A. precisa che «Non ogni volta che si ha a che fare con una clausola generale si ha a che fare *ipso facto* con un principio, la mera presenza di un termine valutativo non comporta la qualificazione dell'enunciato normativo che lo contiene e del suo significato come principio. Allo stesso modo non ogni principio è clausola generale, vale a dire che non è un elemento necessario dei principi essere costituiti anche da termini valutativi. Non v'è quindi una necessaria sovrapposizione tra clausole generali e principi, e per essere più precisi non v'è nemmeno una necessaria distinzione tra principi del diritto e clausole generali». Infine, conclude l'A. cit., «di regola le clausole generali operano all'interno dei confini fissati dai principi, purché si chiarisca che in tal guisa i principi sono considerati norme di particolare rilevanza per un ordinamento giuridico o per un settore dello stesso e che tale rilevanza non dipende dalla presenza nella loro formulazione di termini valutativi; e aggiungendo che le clausole generali che non hanno il carattere necessario per assurgere al ruolo di principio operano, di conseguenza, all'interno del quadro delineato dai principi medesimi». Tali ultime argomentazioni riprendono il pensiero di S. RODOTÀ, *Il tempo delle clausole generali*, cit., p. 721. Uscendo dal formalismo tipico degli studi sulla semantica, la prospettiva di Velluzzi si ricollega dunque con l'impostazione assiologica, che assegna al principio il ruolo di norma di carattere generale espressiva di un "valore", rimanendo invece la clausola generale non (necessariamente) collegata ad esso. La clausola generale, come pure s'è detto (si veda, in tal senso, anche la ricostruzione offerta da P. PERLINGIERI-D. FEMIA, *op. cit*., p. 30), è un frammento vago di norma, contraddistinta da un parametro di valutazione incerto per via del significato vago della clausola medesima, mentre il principio è una norma, contraddistinta da un parametro di valutazione certo, dato dal valore di riferimento, sebbene sia incerto il livello di soddisfazione, in concreto, della norma-principio e del corrispondente valore di riferimento.

che mirano a rendere effettivo, non possono essere considerati "clausole generali" disancorate dal valore di riferimento, ma, pur risolvendosi in espressione di carattere generale, sono ordinate all'affermazione del principio-valore, alla cui realizzazione protendono. Nell'ambito di tale costruzione, mi riferirò ad essi con l'espressione "*principi-funzionali*".

6.6.3. (segue) *L'individuazione dei "principi-valore" e "principi-funzionali" nel GDPR*

I *principi* aventi funzione di *valore* sono chiaramente indicati, ad esempio, nel *considerando* n. 1 del GDPR, nel quale v'è anche il richiamo sistematico all'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea, nonché all'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea, ove si trova l'affermazione del diritto alla protezione dei dati personali quale diritto fondamentale[88]. Nella medesima direzione, esplicitamente l'art. 1, par. 2, del GDPR stabilisce, in conformità ai valori espressi dalla Carta e dal Trattato, che «Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare del diritto alla protezione dei dati personali». Si tratta però di diritto che va armonizzato, contemperato e bilanciato con gli altri diritti fondamentali, secondo un criterio

[88] Il principio fondamentale che esplicita il valore di riferimento si trovava esplicitato, per la prima volta nel nostro diritto interno, all'art. 1 del Codice in materia di protezione dei dati personali, anche se il medesimo diritto era stato estratto deduttivamente dal sistema (generalmente riconducibile all'art. 2 Cost.) e, comunque, frutto di un'evoluzione che ha avuto una tappa importante nella Convenzione di Strasburgo del 28 gennaio 1981 (ratificata dalla l. n. 98 del 21 febbraio 1989), ove «veniva preso atto della nuova esigenza di tutela della persona a fronte del crescente impiego degli strumenti della tecnologia informatica , idonei a schedare la generalità dei cittadini per le più svariate finalità di controllo e di sfruttamento». C.M. Bianca, *Note introduttive*, in C.M. Bianca-F.D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della* privacy»), Padova, 2007, tomo I, p. XIX. Ricorda ancora l'A. cit. che alla «Convenzione di Strasburgo, che aveva enunciato il principio della tutela dei diritti e delle libertà fondamentali della persona e, in particolare, del diritto al rispetto della vita privata a fronte del trattamento automatizzato dei dati personali, ha fatto seguito la Direttiva 95/46/CE (…) del 24 ottobre 1995, tempestivamente attuata in Italia dalla l. del 1996», con un'estensione della tutela anche alla protezione dei dati personali oggetto di trattamenti non automatici, oltre che automatici. L'evoluzione normativa ha poi portato all'affermazione del diritto alla protezione dei dati personali all'interno della Carta di Nizza del 2000 (Carta dei diritti fondamentali dell'UE) e nel TFUE, nonché, nel diritto interno, all'esplicita declamazione di tale diritto in apertura del Codice in materia di protezione dei dati personali (d.lgs. n 196 del 2003, nel testo precedente alla riforma avutasi ad opera del d.lgs. n. 101/2018). Infine, quale ultimo atto di tale evoluzione, il diritto alla protezione dei dati personali ha trovato un'ulteriore consacrazione nel nuovo regolamento (UE) n. 679 del 2016, del 27 aprile 2016, entrato in vigore il 24 maggio 2016 ed applicabile dal 25 maggio 2018, «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)». Per l'individuazione degli interessi tutelati e dei valori sottesi alle scelte legislative *in subjecta materia* cfr. la lettura giusrealista proposta da G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in V. Cuffaro-V. Ricciuto-V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, pp. 3 ss.

non solo di "ragionevolezza"[89], ma anche di "proporzionalità"[90], tenendo conto anche della sua «funzione sociale»[91]. In tal senso è esplicito il *considerando* n. 4 del GDPR: «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di *proporzionalità*. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

L'approccio indicato nel *considerando* citato si riflette sui contenuti normativi del GDPR, ad iniziare dall'art. 1, parr. 1 e 3, ove viene enunciato che il regolamento in parola stabilisce non solo «norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali», ma anche «norme relative alla libera circolazione di tali dati» (art. 1, par. 1), la quale, nell'Unione europea, «non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati» (art. 1, par. 3). Abbiamo dunque, *in primis*, un "*principio-valore*", che trova la sua enunciazione nell'art. 8 della Carta dei diritti

[89] Sulla ragionevolezza nel diritto privato v., in particolare: S. TROIANO, *Ragionevolezza nel diritto dei contratti*, Padova, 2005; ID., voce «*Ragionevolezza (diritto privato)*», in *Enc. dir.*, 2013, pp. 763 ss.; A. RICCI, *Il criterio di ragionevolezza nel diritto privato*, Padova, 2007; F. PIRAINO, *Per una teoria della ragionevolezza nel diritto civile*, in *Europa e diritto privato*, 2014, n. 4, pp. 1287 ss.; G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015; S. PATTI, *Ragionevolezza e clausole generali*, 2ª ed., Milano, 2016. Con riferimento al criterio di ragionevolezza nella giurisprudenza della Corte costituzionale e in quella comunitaria si vedano, rispettivamente, F. MODUGNO, *La ragionevolezza nella giustizia costituzionale*, Napoli, 2007; G. TESAURO, *La ragionevolezza nella giurisprudenza comunitaria*, Napoli, 2012.

[90] Sul principio di proporzionalità cfr. P. DE SENA, *Proportionality and human rights in international law: some … "utilitarian" reflections*, in *Rivista di diritto internazionale*, 2016, n. 4, pp. 1009 ss.; S. BOLLINO, *Il principio di proporzionalità come metodo di valore universale. Un'analisi delle sue forme applicative in sede di ponderazione e di sussunzione degli interessi in gioco*, in *Diritto e processo amministrativo*, 2013, n. 4. Con un approccio decisamente critico si veda, invece, S. TSAKYRAKIS, *Proportionality: An assault on human rights?*, in *International Journali of Constitutional Law*, 2009, n. 3, pp. 468 ss. Va rimarcato che alcuni studi hanno già avuto modo di analizzare le connessioni tra il criterio di ragionevolezza e quello di proporzionalità: in tal senso cfr. M. CARTABIA, *I principi di ragionevolezza nella giurisprudenza costituzionale italiana*, relazione svolta nell'ambito della Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola, in Roma, Palazzo della Consulta, 24-26 ottobre 2013, consultabile all'Url http://www.cortecostituzionale.it/documenti/convegni_seminari/RI_Cartabia_Roma2013.pdf (consultata da ultimo in data 31 marzo 2017), ora in A. GIORGIS-E. GROSSO-J. LUTHER (a cura di), *Il costituzionalista riluttante. Scritti per Gustavo Zagrebelsky*, Torino, 2016; inoltre, seppur con settoriale riferimento all'ambito dei diritti reali, ma con interessanti spunti di rilievo generale, cfr. R.M. BOVA, *Proporzionalità e ragionevolezza nel diritto di proprietà*, in *Rassegna di diritto civile*, 2010, n. 3.

[91] Proprio con riguardo alla «funzione sociale» di cui al considerando in esame vedasi il recente contributo di A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, n. 2, p. 586 ss.

fondamentali dell'UE, che individua il diritto alla protezione dei dati personali quale diritto fondamentale, da coordinare con la "costellazione" dei diritti fondamentali e dei valori su cui si fonda il nostro sistema giuridico, europeo e nazionale[92].

Connessi a tale "*principio-valore*" si rinvengono poi, su un altro piano, una serie di diversi "principi", non aventi valenza assiologica (in quanto non espressivi, in sé, di determinati valori), ma funzionalmente collegati con il "principio-valore" di riferimento (in quanto volti a garantirne l'applicazione)[93].

Il rapporto tra tali tipologie diverse di "principi" (che si trovano collocati su piani diversi: quello "assiologico" e quello, per così dire, "funzionale" al piano assiologico, senza essere a questo estraneo) si riscontra chiaramente all'interno del medesimo testo dell'art. 8 della Carta, ove:

a) nel par. 1, viene riconosciuto il diritto fondamentale («Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano»), nel quale è insito il *valore* in sé tutelato dall'ordinamento giuridico;

b) nel par. 2 vengono fissati "principi" e diritti aventi valenza strumentale, in quanto funzionalmente preordinati a garantire forme di tutela al "principio-valore" dichiarato al par. 1 e ad orientarne l'applicazione, distinguendosi tra "principi" relativi alle *modalità di trattamento* e "principi" volti ad individuare il *fondamento di legittimità* per il trattamento dei dati. Così, viene *ivi* stabilito che «Tali dati [di carattere personale] devono essere trattati secondo il principio di lealtà, per finalità determinate in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni indivi-

---

[92] Nell'indagare il rapporto tra diritti fondamentali, pregevoli sono le osservazioni di P. Zatti, *Maschere del diritto, volti della vita*, Milano, 2009, p. 44, per il quale «Il modo di ragionare che inevitabilmente si impone in questa zona, non è quello applicativo che utilizza i diritti come una schiera di strumenti allineati in uno scaffale, tra i quali devo scegliere quello appropriato, e tra i quali può sussistere una gerarchia lineare: ma quello che li considera in termini di costellazione (…). Costellazione significa che i diritti "costellati" si sostengono e si definiscono a vicenda: talvolta l'uno appare fondante dell'altro, talaltra, proprio per questo, ne costituisce il limite. Come in una costellazione di vettori, la risultante è una variabile che dipende dalla forza assegnata a ciascuno e dalla direzione in cui si applicano, così in una costellazione di diritti il risultato è variabile, ed è necessariamente una conclusione "retorica" cioè di utilizzazione dei simboli cui assegniamo maggiore o minore forza per sostenere una conclusione; insomma, interpretazione». Riecheggiano a tal riguardo anche le parole di Luigi Mengoni, che nella relazione introduttiva al seminario dedicato a «I problemi del metodo nella ricerca civilistica oggi in Italia», svoltosi a Roma il 30 settembre – 1° ottobre 1988 per iniziativa della Rivista critica del diritto privato, avvertiva come «Sotto la pressione delle trasformazioni sociali e della tendenza al policentrismo propria della società contemporanea, il sistema del diritto civile va perdendo la tradizionale struttura piramidale basata sullo schema logico regola-eccezione. Anziché quale criterio di sviluppo di concetti a catena, riferiti a un medesimo principio, il sistema tende a costituirsi come criterio di coesistenza e di reciproca delimitazione di principi diversi, ciascuno dotato di un proprio ambito normativo, e così ad assumere una struttura circolare». Così L. Mengoni, *Relazione illustrativa*, in Aa.Vv., *Il metodo della ricerca civilistica*, Napoli, 1990 (*Riv. crit. dir. priv.*, 1990, n. 1-2), p. 24.

[93] Sulla distinzione tra «*principi-valori*» e «*principi-orientativi*» con riferimento alla disciplina in materia di protezione dei dati personali di cui al d.lgs. n. 196 del 2003 v. F. Piraino, *Il codice della* privacy *e la tecnica del bilanciamento di interessi*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, tomo I, pp. 715 ss.

duo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica» (art. 8, par. 2, Reg. cit.);

c) sempre in funzione di tutela del "principio-valore" dichiarato nel par. 1, l'art. 8 cit. riconosce poi (sempre – significativamente – all'interno della Carta dei diritti fondamentali dell'UE, avente il medesimo valore giuridico dei Tratti europei) la necessità di istituire un'autorità indipendente in materia di protezione dei dati personali, che abbia un compito di controllo e supervisione volto a garantire il rispetto delle regole sulla protezione dei dati personali, nella consapevolezza che il potere di autodeterminazione e di controllo dell'interessato è insufficiente a garantire l'effettività del diritto fondamentale *de quo* (par. 3: «Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente»).

Il rapporto tra "*principio-valore*" e "*principi-funzionali*" è da leggersi, invero, in un'evoluzione del sistema (e delle tecniche) di protezione della persona, con il passaggio da una tutela di tipo statico, negativa, com'è tipicamente quella offerta dal tradizionale diritto «al rispetto della propria vita privata e familiare» di cui all'art. 7 della Carta, ad una tutela dinamica, assicurata dal «diritto alla protezione dei dati personali» *ex* art. 8, su cui sono innestati attivi poteri di intervento privatistici e pubblicistici, garantiti proprio dalla presenza dei "*principi-funzionali*" a cui s'è fatto riferimento[94].

Così, nell'impianto del GDPR, accanto al "*principio-valore*" che enuncia e ribadisce il diritto alla protezione dei dati personali (da coordinare, come già precisato, con la "costellazione" degli altri diritti fondamentali riconosciuti dall'ordinamento europeo)[95], rinveniamo una serie di "*principi*" non (direttamente) espressivi

[94] L'evoluzione registratasi nel sistema di protezione dei diritti fondamentali e l'accostamento di una tutela dinamica accanto a quella, tradizionale, statica, si trova ben annotata da S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, cit., p. 2 s.: «Il fatto, indubitabile, che la nostra vita sta ormai diventando uno scambio continuo di informazioni, che viviamo in un flusso continuo di dati, ha attribuito importanza crescente alla protezione dei dati, portandola sempre più verso il centro del sistema politico-istituzionale. Questa evoluzione è ben visibile nella Carta dei diritti fondamentali dell'Unione europea, dove si opera una distinzione tra il tradizionale diritto "al rispetto della propria vita privata e familiare" (art. 7) e il "diritto alla protezione dei dati personali" (art. 8), che si configura così come un diritto fondamentale nuovo ed autonomo. La distinzione non è di facciata. Nel diritto al rispetto alla vita privata e familiare si manifesta soprattutto il momento individualistico, il potere si esaurisce sostanzialmente nell'escludere interferenze altrui: la tutela è statica, negativa. La protezione dei dati, invece, fissa regole sulle *modalità* del trattamento dei dati, si concretizza in poteri di intervento: la tutela è dinamica, segue i dati nella loro circolazione. I poteri di controllo e d'intervento, inoltre, non sono attribuiti soltanto ai diretti interessati, ma vengono affidati anche ad una autorità indipendente (8.3): la tutela non è più soltanto nelle mani dei soggetti interessati, ma coinvolge permanentemente una specifica responsabilità pubblica. Siamo così di fronte anche ad una redistribuzione di poteri sociali e giuridici. Si coglie qui il punto d'arrivo di una lunga evoluzione del concetto di *privacy*, dall'originaria sua definizione come *diritto ad essere lasciato solo* fino al diritto di mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata. Si contribuisce in maniera determinante al processo di "costituzionalizzazione della persona"».

[95] Il coordinamento tra diritti fondamentali non va valutato solo nel senso del bilanciamento tra confliggenti valori da contemperare, ma anche nel senso della connessione tra valori complementari o "vicini". Come ricorda S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, cit., p. 2, «Già nell'art. 1 della l. 675/1996 si era proceduto ad una significativa integrazione, proprio sul piano dei principi, di quanto previsto dall'art. 1 della Direttiva europea

di un valore intrinseco, ma *funzionali* alla realizzazione del "principio-valore di riferimento" e capaci, nel loro insieme, di determinare il passaggio da una tutela statica ad una tutela dinamica (ed improntata ad una maggiore effettività) dei diritti fondamentali, secondo logiche prospettate sin dagli inizi degli anni '80 del secolo scorso in documenti internazionali, ma che vedono ora, nel nuovo regolamento europeo, il compimento di tale evoluzione ad uno stadio più maturo[96].

Il Capo II del GDPR, composto degli articoli da 5 a 11, e intitolato «*Principi*», pare riferirsi proprio a tale seconda categoria di "principi", privi di un diretto valore assiologico ma comunque collegabili ad esso, che possono essere distinti in due differenti tipologie:

95/46, facendo esplicito riferimento alla necessità di rispettare, insieme alle libertà ed ai diritti fondamentali menzionati nella Direttiva, anche la "dignità delle persone fisiche". Una apertura importante ed una intuizione anticipatrice: proprio con il riferimento al principio di dignità, infatti, si apre la Carta dei diritti fondamentali dell'Unione europea proclamata a Nizza nel 2000. E questo gioco di rimandi è continuato».

[96] Quanto all'originaria formulazione dei "principi" funzionalmente collegati al "principio-valore" ed alla loro (intravista) capacità di ridelineare il sistema di protezione della persona, accordando una tutela non più solamente statica ma anche dinamica, si ricordano – in epoca antecedente all'emanazione della nostra prima legge in materia di protezione dei dati personali – le ricerche svolte con acume da S. Rodotà, *Tecnologie e diritti*, cit., pp. 61 ss., là dove rimarcava che «per cercare di cogliere le tendenze in atto o in embrione, si possono scegliere alcuni documenti espressivi di quanto appare ormai consolidato e di quel che sta emergendo. L'attenzione deve essere rivolta, da una parte, ai principi affermati; e, dall'altra, agli strumenti necessari per assicurare la loro effettività. Per individuare un nucleo comune nell'attuale disciplina giuridica della protezione dei dati, si utilizzano spesso due testi con rilevanza internazionale: la Convenzione del Consiglio d'Europa del 28 gennaio 1981, per la protezione delle persone in relazione alla elaborazione automatica dei dati a carattere personale, e la Raccomandazione dell'OCSE del 23 settembre 1980, concernente le linee direttive riguardanti la protezione della vita privata e la circolazione transnazionale dei dati a carattere personale. Dai punti comuni di questi due testi si desumono diversi principi: 1) *principio di correttezza* nella raccolta e nel trattamento delle informazioni; 2) *principio di esattezza* dei dati raccolti, a cui si accompagna l'obbligo di un loro aggiornamento; 3) *principio della finalità* della raccolta dei dati, che deve poter essere conosciuta prima che la raccolta abbia luogo, e che si specifica nel rapporto tra dati raccolti e finalità perseguita (*principio di pertinenza*); nel rapporto tra finalità della raccolta e utilizzazione dei dati (*principio della utilizzazione non abusiva*); nella eliminazione, o nella trasformazione in dati anonimi, delle informazioni non più necessarie (*principio del diritto all'oblio*); 4) *principio della pubblicità* delle banche dati che trattano informazioni personali, di cui deve esistere un registro pubblico; 5) *principio dell'accesso individuale*, al fine di conoscere quali siano le informazioni raccolte sul proprio conto, ottenerne copia, pretendere la correzione di quelle sbagliate, l'integrazione di quelle incomplete, l'eliminazione di quelle raccolte illegittimamente; 6) *principio della sicurezza* fisica e logica delle raccolte dei dati». Rodotà, dopo aver passato in rassegna i "principi" enucleati nei richiamati testi di carattere internazionale, concludeva evidenziando che in «questa elencazione si può cogliere una commistione tra principi di base e strumenti per l'effettività di tali principi. (…) Si coglie così il passaggio da una impostazione negativa e passiva ad una positiva e dinamica della protezione dei dati individuali. La tecnica giuridica adoperata non è più quella dell'attribuzione al privato di un diritto azionabile davanti ad un organo *ad hoc* solo nel caso di una sua violazione. Ora al privato viene attribuito un potere di controllo diretto e continuo sui raccoglitori delle informazioni, indipendentemente dalla esistenza attuale di una violazione. Muta così la tecnica di protezione della *privacy* e l'attenzione si sposta verso la messa a punto di regole sulla circolazione delle informazioni» (S. Rodotà, *Tecnologie e diritti*, cit., pp. 63-46).

a) quelli, di carattere operativo, insistenti sulle modalità del trattamento (annoverati all'art. 5 del GDPR, rubricato «*Principi applicabili al trattamento di dati personali*»);

b) quelli volti ad individuare il fondamento che legittima il trattamento dei dati personali e, dunque, ne rappresenta il *presupposto legittimante* ovvero, ricorrendo ad altra terminologia, la *condizione di liceità* (artt. 6 ss. del Reg. cit.).

6.6.4. *Importanza ed opportunità della "rilettura" dei principi alla luce del diritto vivente, nonché dell'individuazione e della ricostruzione sistematica delle* rules of construction *ad essi riferibili*

I principi in materia di protezione dei dati personali si collocano, dunque, nel più ampio quadro normativo che disciplina tale materia, fungendo anche da collante a livello sistematico.

L'applicazione di quelli che abbiamo definito "principi-funzionali", aderenti al "principio-valore" a cui sono funzionalmente collegati, impone di analizzare anche la prospettiva che governa la loro applicazione: più che le tecniche di bilanciamento, normalmente adottate quando concorrono più "principi-valore" da coordinare, siamo di fronte alla "cooperazione" tra principi diversi, ma collegati dall'unitaria funzionalizzazione rispetto al medesimo valore di riferimento.

Sicché lo studio dei principi-funzionali, unitariamente coesi sul piano assiologico al principio-valore a cui sono strumentalmente collegati, conduce ad una concorrente applicazione tra principi di natura eterogenea, che l'interprete deve saper padroneggiare. Così, i principi-funzionali sono da collocare nella direzione applicativa del principio-valore a cui sono correlati, fa sì che essi "vadano a caccia in branco" e non solo "in coppia", come invece avviene qualora entrino in gioco "principi-valore" contrapposti[97].

Così, i principi-funzionali in materia di protezione dei dati personali previsti all'art. 5 GDPR e gli altri evincibili in via interpretativa dal sistema normativo (si pensi ad esempio al principio di *privacy by design* e *privacy by default*, oltre che al principio di necessità e a quello di proporzionalità) vanno applicati in maniera coordinata tra loro per giungere all'applicazione del *data protection law* al caso di specie, una volta determinata la loro portata normativa, in funzione "ordinante" o "adeguatrice".

Da tale impostazione si aprono nuovi orizzonti di ricerca.

Lo studio dei principi-funzionali, dunque, mira a comprendere anche le loro effettive relazioni reciproche, non già nella sola prospettiva del bilanciamento degli interessi – pur ravvisabile qualora il "principio-valore" legato alla protezione dei dati personali si misura con altri contrapposti "principi-valori", come quello relativo

[97] Il riferimento è qui all'efficace lessico di Guido Alpa, nella parte in cui evidenzia l'importanza delle "coppie di principi" (nel senso che abbiamo indicato con l'espressione "principi-valore"), là dove ha affermato che «I principi "vanno a caccia in coppia" perché gli istituti giuridici sono il risultato del contemperamento o del compromesso di valori tra loro non compatibili. Un principio spesso opera in coppia con un principio contrapposto senza che questo implichi necessariamente la presenza di un'antinomia o di una totale indeterminazione normativa, perché si possa decidere quale principio debba prevalere nel caso in decisione».

alla libertà di impresa e di valorizzazione dei dati o di manifestazione del pensiero –, ma, appunto, nella prospettiva del loro coordinamento unidirezionale verso la piena tutela del principio-valore a cui i principi-funzionali sono strumentalmente piegati.

Inoltre, lo studio dell'applicazione che viene fatta dei "principi-funzionali" al cospetto della fattispecie concreta – con l'esame dei significativi provvedimenti delle autorità di controllo e, ove necessario, dell'autorità giudiziaria –, consente poi di comprendere anche l'effettiva vitalità dei principi medesimi e le modalità con cui essi vengono impiegati nell'argomentazione giuridica utilizzata per risolvere gli aspetti controversi che emergono nella fattispecie concreta.

L'analisi dei principi-funzionali evincibili dal GDPR consente inoltre di ottenere un solido supporto per la comprensione e lo studio dell'intera materia, in quanto l'intera normativa è ad essi sempre riconducibile. Sicché lo studio dei principi in materia di protezione dei dati personali apre ad ulteriori opportunità di ricerca, in quanto le riflessioni sui principi fondanti la disciplina in esame può rappresentare quell'impalcatura su cui proseguire le ulteriori analisi, ad esempio per lo studio dei singoli istituti *in subjecta materia* o sui principi collegati, nella prospettiva avviata con l'*European Digital Rights and Principles for Digital Decade*.

Ulteriore orizzonte di ricerca mira ad indagare e ricostruire in chiave sistematica le molteplici *rules of construction* che occorrono per applicare il principio alla fattispecie concreta. Va tenuto a mente, infatti, che – secondo una nota distinzione comunemente accettata in dottrina – "principi" e "regole" hanno entrambi una natura normativa, ma conservano tratti distintivi specifici, ripercorrendo i quali possono trarsi importanti indicazioni in materia di protezione dei dati personali, utili a determinare anche le opportunità della ricerca sui principi.

Proprio sulla distinzione tra "regole" e "principi" sé osservato, in dottrina, che – badando alla loro struttura e alla loro funzione –, «(…) Le prime esigono conformità ad una fattispecie e sono frutto di una tipizzazione legislativa. I secondi hanno una dimensione diversa. Orientano in presenza di problemi altrimenti non facilmente risolvibili»[98]. Richiamando la nota teoria di Dworkin, si può a tal riguardo sostenere, con riferimento al principio, che «*it makes sense to ask how important or how weighty it is. Rules not have this dimension*»[99]. Ancora, la dottrina citata mette in risalto che «Le norme che contengono diritti e (…) principi se non sono precise, determinate e se hanno necessità di essere completate da qualche altra autorità, non fondano di per sé diritti obblighi e doveri. Hanno necessità di un'attività ulteriore della legge o del giudice. Nel primo caso il problema è attenuato. Nel secondo al giudice si richiede una particolare tecnica argomentativa. Deve creare una *rule of construction*, una regola di decisione rigorosa e convincente (…). Nella *rule of construction* si concreta in modo tangibile il limite e la funzione creativa del giudicare. Che esige conformità ad un ordine giuridico in modo peculiare. Impone in taluni casi

[98] G. Vettori, *Regole e principi. Un decalogo*, cit., p. 128.

[99] Il pensiero e le parole di Dworkin si trovano riportate anche nella ricostruzione operata da G. Vettori, *Regole e principi. Un decalogo*, cit., p. 128.

decisioni *extra legem*, ma *intra jus*, quando la risposta implichi un problema di vita che le regole non hanno previsto o e che non può essere risolto con l'analogia»[100].

V'è però da dire che tale caratteristica dei principi, tuttavia, non è sempre rinvenibile nei termini sopra enunciati. Talvolta la *rule of contruction* (come spesso avviene in materia di protezione dei dati personali) viene affidata al soggetto tenuto all'applicazione del principio (com'è per il titolare del trattamento dei dati personali, tenuto ad osservare i principi di cui all'art. 5, par. 1 e 2, GDPR), mentre l'autorità posta in funzione di controllo della corretta applicazione del diritto (l'autorità Garante per la protezione dei dati personali o l'autorità giudiziaria) interviene *ex post*, al fine di verificare se la condotta posta in essere dal soggetto tenuto ad aderire alla norma inscritta nel principio (appunto, il titolare del trattamento) sia effettivamente conforme alla corretta applicazione che di tale principio debba essere fatta, secondo il controllo esercitato (dal Garante o dal giudice) per verificare l'aderenza della fattispecie concreta ai parametri insiti nel principio di tenore generale. In altre parole, la *rule of construction* può essere inscritta (*ex ante*) dall'operatore tenuto a tradurre il principio nella prassi applicativa e, successivamente, confrontata con la *rule of construction* dell'autorità chiamata a verificare (*ex post*) la correttezza della prima rispetto alla seconda: si pensi, ad esempio, all'operatività del principio di *accountability* o di responsabilizzazione di cui all'art. 5, par. 2, GDPR, che impone al titolare del trattamento di determinare le scelte in ordine alla corretta applicazione dei principi di cui all'art. 5, par. 1, GDPR, salvo poi ad essere chiamato a darne conto, ove tali scelte siano considerate difformi dalla *rule of construction* determinata dall'autorità garante in materia di protezione dei dati personali o dall'autorità giudiziaria.

Ancora, la citata dottrina rimarca che «L'irrompere dei principi supera in molti casi il problema delle lacune e l'impiego dell'analogia. Per un motivo chiaro. L'assenza di una regola in presenza di un principio, non crea il vuoto ma implica una decisione basata su di una diversa argomentazione. Certo un principio attinge sempre elementi fuori di sé. Per evitare elementi devianti (il sacro, l'ideologia) occorre grande attenzione alla giuridicità del fatto che emerge da una pluralità di fonti (…). Tutto ruota attorno a nuove tecniche argomentative che conoscano e sappiano utilizzare tutte le potenzialità del sistema integrato delle fonti e i precedenti delle Corti nazionali ed europee»[101]. È questo un aspetto rilevante, soprattutto per i principi in materia di protezione dei dati personali: là dove le regole fissate nelle norme specifiche di settore non siano adeguate o sufficienti a governare la fattispecie, soccorrono pur sempre i principi in funzione "ordinante", che valgono a costruire la norma attraverso non l'analogia, ma attraverso una diversa argomentazione che mira ad esplicitare, sulla base di un criterio valutativo rimesso all'interprete, quale debba essere la *rule of construction* per adattare il principio, nella sua formulazione di carattere generale, alla fattispecie concreta: è attività rimessa sia all'operate (titolare del trattamento) chiamato ad applicare il principio prima del controllo da parte dell'autorità competente (il Garante o l'autorità giudiziaria), sia all'autorità medesima, che dovrà determinare la propria *rule of construction* e confrontarla con quella posta in essere dall'operatore, per verificare la correttezza della prima

[100] *Ibidem*, p. 128.
[101] *Ibidem*, p. 128.

rispetto al sistema, secondo l'interpretazione che il legislatore, fissando il principio, ha voluto rimettere all'autorità medesima.

Sulla scorta di tali considerazione si comprende bene l'importanza di una raccolta degli orientamenti del Garante per la protezione dei dati personali, anche attraverso l'attività di massimazione dei provvedimenti, al fine di ricostruire le *rules of construction* da ritenersi aderenti al sistema normativo delineato in materia di *data protection*, secondo l'interpretazione dell'Autorità di controllo, a cui viene sostanzialmente rimesso il compito di "creare" l'insieme di regole necessarie all'applicazione del principio sul piano operativo, ossia quello di aderenza alle fattispecie concrete.

Ancora, s'è detto che «Il problema se esista già una regola o una tutela tipica e su come in tal caso il principio operi non va posto in astratto, ma calato nel concreto di precetti da sottoporre al vaglio dell'effettività richiesta da fonti costituzionali interne (…), comunitarie (…) e sovranazionali (…)»[102]. Con specifico riferimento ai principi delineati nel GDPR, oltre al sistema delle fonti sopranazionali, eurounitarie e nazionali rilevanti in materia di protezione dei dati personali, il vaglio in questione va "calato" anche "nel concreto" delle *rules of construction* esplicitate dal Garante (e dall'autorità giudiziaria) nei provvedimenti resi per le decisioni di fattispecie concrete e stratificatesi nel corso del tempo: si tratta di un insieme di "regole" specificative delle modalità di applicazione dei principi, di fonte "para-giurisprudenziale" (e giurisprudenziale), che hanno un'indubbia rilevanza sul piano teorico e applicativo.

Infatti, «L'argomentazione necessita di tecniche e di strumenti nuovi Non una scatola degli attrezzi, ma una condizione dei fini che è compito della scienza giuridica promuovere e saldare»[103], tenendo conto che «Non occorrono sentenze di cento pagine, ma un ragionamento stringente capace di convincere e di porsi in sintonia con un ordine oggettivo (…)»[104]. Ci vale anche a definire «antidoti precisi»[105] contro il rischio di abuso derivante dall'applicazione dei principi e tali antidoti sono «il fatto e l'argomentazione. La ricostruzione puntuale ed esatta della fattispecie concreta indica subito i termini entro cui deve articolarsi la riposta al problema della vita. La tecnica argomentativa darà conto di come dovranno essere impiegate regole e principi. (…) Le une e gli altri vanno sottratti all'astrattezza. Dovrà essere isolato il dato normativo specifico e il principio da cui si trae la *rule* e si dovrà motivare come questa *rule* può risolvere il caso»[106].

Si tratta di riflessioni che mettono in risalto l'importanza dell'istituzione di strumenti che possano raccogliere le *rules of construction* per l'applicazione dei principi alla fattispecie concreta e renderne agevole il reperimento e la fruizione per l'intera comunità[107].

---

[102] *Ibidem*, p. 128.
[103] *Ibidem*, p. 128.
[104] *Ibidem*, p. 128.
[105] *Ibidem*, p. 128.
[106] *Ibidem*, p. 128.
[107] In tale direzione si segnala, accanto all'importante opera di raccolta dei provvedimenti del Garante sul sito istituzionale dell'Autorità di controllo in materia di protezione dei dati personali, la creazione di una banca-dati *open access* dedicata alla massimazione e ai commenti ai provvedimenti del Garante, portata avanti dall'*Osservatorio Privacy* collegato al Corso di Alta Formazione in «*Privacy e Data Protection Officer*» dell'Università di Bologna, consultabile all'indirizzo www.dataprotection-privacy.it.

Capitolo II
Il principio di liceità

*Giacomo Bianchedi - Cristina Modica**

SOMMARIO: 1. Inquadramento normativo. – 1.1. I riferimenti normativi alla liceità del trattamento nel GDPR e nella Carta dei diritti fondamentali dell'UE. – 1.2. La rilevanza dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo del 1950. – 1.3. La liceità del trattamento nella Convenzione n. 108 del 1981 e nella Convenzione n. 108+, aggiornata con Protocollo emendativo del 2018. – 1.4. La liceità del trattamento nella Direttiva 95/46/CE. – 1.5. La liceità del trattamento nella l. n. 675/96. – 1.6. La liceità del trattamento nel d.lgs. n. 196/03 (Codice in materia di protezione dei dati personali), antecedentemente alla novellazione del 2018. – 1.7. Novellazione del Codice in materia di protezione dei dati personali ad opera del d.lgs. n. 101 del 2018 e principio di liceità del trattamento. – 2. Portata applicativa del principio. – 2.1. Inquadramento teorico ed interpretazione dottrinale ed istituzionale del principio di liceità. – 2.2. Condizioni di liceità rimesse alla valutazione dell'interessato: il consenso. – 2.2.1. In particolare, il consenso dei minori. – 2.3. Condizioni di liceità rimesse alla valutazione congiunta tra interessato e titolare: esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato. – 2.3.1. In particolare, la commercializzazione dei dati personali tra consenso e contratti di scambio. – 2.4. Condizioni di liceità rimesse alla valutazione del legislatore: adempimento di un obbligo legale, salvaguardia di interessi vitali dell'interessato o di un'altra persona, esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. – 2.4.1. In particolare, il trattamento effettuato dalla pubblica amministrazione. – 2.4.2. In particolare, i trattamenti nel contesto dell'epidemia. – 2.5. Condizioni di liceità rimesse alla valutazione del titolare: il legittimo interesse del titolare o di un terzo. – 2.5.1. In particolare, il *marketing* diretto e i *cookies*. – 3. Applicazione del principio nella casistica. – 3.1. Il principio di liceità nella casistica nazionale. – 3.1.1. La liceità del consenso nella commercializzazione di dati personali e nelle pratiche di *marketing*. Il caso «Ad Spray» innanzi al Garante per la protezione dei dati personali e alla Corte di Cassazione. – 3.1.2. L'illiceità del trattamento avente ad oggetto operazioni di recupero del consenso alle campagne di *marketing*. Il caso «Wind Tre» innanzi al Garante per la protezione dei dati personali e alla Corte di Cassazione. – 3.1.3. Ancora sulla liceità del consenso al trattamento dei dati personali quale controprestazione della fornitura di servizi erogati senza richiesta di compenso. Il caso «Facebook» innanzi all'AGCM e al giudice amministrativo (TAR e Consiglio di Stato). – 3.1.4. Liceità del trattamento e consenso dei minori nella società digitale. Il caso «Tik Tok» nei diversi provvedimenti del Garante. – 3.2. La casistica internazionale sulla «*lawfulness of processing*». – 3.2.1. Liceità del trattamento, approvazione dei *cookies* e validità del consenso. Il caso della SA spagnola sul vettore «Vueling Airlines». – 3.2.2. (*segue*): e la pronuncia della CGUE sul caso «Planet49». – 3.3. Le *app* di *contact tracing* nella pandemia da Covid-19 in Europa e in Italia. – 3.4. (*segue*): Le Linee Guida dell'*European Data Protection Board* (EDPB). – 3.5. (*segue*): Le *app* di *contact tracing* nei provvedimenti del Garante.

---

* Pur essendo lo scritto, nel suo complesso, frutto di riflessioni comuni, sono da attribuire a Giacomo Bianchedi i par. 1 e 2 e a Cristina Modica il par. 3.

1. INQUADRAMENTO NORMATIVO

1.1. I riferimenti normativi alla liceità del trattamento nel GDPR e nella Carta dei diritti fondamentali dell'UE

Il principio di liceità trova la propria attuale fonte normativa nel GDPR all'art. 5, par. 1, dove, tra i principi applicabili al trattamento di dati personali, è previsto, alla lett. *a)*, che i dati personali siano «trattati in modo lecito (…)».

L'accezione di «liceità» è ampia ed ha molteplici sfumature semantiche. Il GDPR esplicita tale principio nel successivo art. 6, interamente dedicato alla «*Liceità del trattamento*», ove, con riguardo ai dati personali comuni, si stabilisce che «il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle (…) condizioni» ivi previste, tra cui il consenso e le altre condizioni di liceità ad esso alternative[1].

Ove il trattamento abbia ad oggetto dati particolari, le condizioni di liceità sono indicate invece all'art. 9 («*Trattamento di categorie particolari di dati personali*») ed anche in questo caso viene annoverato il consenso, a cui seguono ulteriori condizioni di liceità alternative al consenso medesimo[2], con facoltà attribuita agli

---

[1] L'art. 6, par. 1, GDPR, segnatamente, individua le seguenti condizioni di liceità del trattamento per i dati comuni: «(…) *a)* l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; *b)* il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; *c)* il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; *d)* il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; *e)* il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; *f)* il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (…)».
Con riferimento, in particolare, alle basi giuridiche su cui si fondano i trattamenti legittimati dall'adempimento di un obbligo legale [art. 6, par. 1, lett. *c)*] e sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri [art. 6, par. 1, lett. *e)*], l'art. 6, par. 3, precisa che la base deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento, con la possibilità che essa contenga disposizioni specifiche per adeguare l'applicazione delle norme del GDPR.

[2] L'art. 9 del GDPR stabilisce, al par. 1, la regola generale per cui «è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Tale divieto, tuttavia, non opera nei casi di deroga previsti dal successivo par. 2, ossia quando: *a)* l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al par. 1; *b)* il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; *c)* il trattamento è necessario per tutelare un interesse vitale dell'in-

Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute[3].

Del consenso, quale condizione di liceità, viene offerta una disciplina specifica agli artt. 7 e 8, rispettivamente dedicati alle «*Condizioni per il consenso*» e alle «*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*»[4].

Una diversa previsione concerne invece il trattamento di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza, che, ai sensi dell'art. 10 del GDPR, «deve avvenire soltanto sotto il controllo dell'autorità pubblica e se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati (…)».

La necessità del consenso o di altro «presupposto legittimo» prevista dalla legge viene contemplata anche all'art. 8 della Carta dei diritti fondamentali dell'UE, rubricato «*Protezione dei dati di carattere personale*», ai sensi del quale «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati (…) in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge (…)».

---

teressato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; *d)* il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli *ex* membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; *e)* il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; *f)* il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; *g)* il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; *h)* il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al par. 3; *i)* il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; *j)* il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'art. 89, par. 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

[3] Cfr. art. 9, par. 4, GDPR.

[4] In tema di condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione la disposizione di cui all'art. 8 del GDPR va letta unitamente all'art. 2-*quinquies* del Codice in materia di protezione dei dati personali, come novellato dal d.lgs. n. 101 del 2018, in ordine al quale si rinvia a quanto precisato, *infra*, nel prosieguo della trattazione.

A livello dei *considerando* del GDPR, il n. 39 parte dal presupposto, affermato nel già richiamato art. 5, par. 1, lett. *a)* del GDPR, che qualsiasi trattamento di dati personali debba essere «lecito e corretto». Il significato del principio di liceità emerge, nel Regolamento, anche dalla lettura del *considerando* n. 40, nel quale il legislatore europeo ha chiarito che «Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato[5] o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri (...) tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso»[6].

Lasciando, per il momento, al prosieguo della trattazione l'esame della portata applicativa del principio di liceità del trattamento[7], è utile ripercorrere la genesi e l'evoluzione normativa del principio in questione e soffermarsi su una visione d'insieme nel contesto delle altre disposizioni normative sovranazionali e nazionali.

All'attuale assetto normativo, disciplinato attraverso lo strumento del regolamento, si è giunti infatti per la necessità di recepire il diritto alla protezione dei dati personali all'interno della Carta di Nizza[8] e per la presa d'atto del mutato contesto economico, sociale, politico e tecnologico[9], oltre che della frammentazione applicativa della Dir. 95/46/CE nei vari Stati membri[10].

1.2. La rilevanza dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo del 1950

La Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, sottoscritta a Roma il 4 novembre 1950 (CEDU), si limitava a sancire, all'art. 8, il diritto di ogni persona al rispetto della propria vita privata e familiare e il divieto di ingerenza delle autorità pubbliche nell'esercizio di tale diritto, salvo che in virtù di previsioni di legge ed in forza di misure necessarie alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale o alla protezione dei diritti e delle libertà altrui.

---

5 A cui sono dedicati i successivi *considerando* n. 42 e n. 43.

6 I successivi *considerando*, dal n. 44 al n. 49, richiamano le basi giuridiche diverse dal consenso ritenute legittime per il trattamento dei dati comuni, elencate, come si è già avuto modo di evidenziare, agli artt. 6 e 9. I *considerando* dal n. 51 al n. 54 si riferiscono, invece, alla necessità di una specifica protezione per i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, rimarcando che tali dati personali non dovrebbero essere oggetto di trattamento, in previsione di un generico divieto (previsto all'art. 9, par. 1, del regolamento), a meno che non siano previste deroghe specifiche legate all'espressione del consenso da parte dell'interessato oppure in relazione ad esigenze specifiche espressamente previste per legge (nel par. 2 del medesimo articolo).

7 V. par. 2.

8 Cfr. *considerando* n. 1 e n. 4 del GDPR.

9 Cfr. *considerando* n. 5, n. 6 e n. 7 del GDPR.

10 Cfr. *considerando* n. 9 del GDPR.

Tale articolo è pacificamente applicabile anche alla disciplina in tema di trattamento dei dati personali e, anche grazie alla giurisprudenza della Corte europea dei diritti dell'uomo[11], ha assunto particolare rilevanza ai fini dell'individuazione della liceità del trattamento, in una prospettiva di tutela multilivello dei diritti fondamentali[12].

1.3. La liceità del trattamento nella Convenzione n. 108 del 1981 e nella Convenzione n. 108+, aggiornata con Protocollo emendativo del 2018

Fin dalla Convenzione n. 108 sulla protezione degli individui rispetto al trattamento automatizzato di dati a carattere personale, firmata a Strasburgo il 28 gennaio 1981, veniva specificato, all'art. 5, rubricato «*Qualità dei dati*», che i dati a carattere personale oggetto di elaborazione automatica dovessero essere, in particolare, «ottenuti ed elaborati lealmente e legalmente» [lett. *a)*], oltre che «registrati per fini determinati e legittimi» [lett. *b)*].

Nel 2018, il testo della citata Convenzione è stato aggiornato e modernizzato – anche al fine di adeguarlo alle prescrizioni introdotte nell'UE con il GDPR – mediante un Protocollo emendativo[13], assumendo così la denominazione di *Convenzione 108+*.

Le modifiche, oltre a comportare l'ampliamento della portata applicativa della Convenzione anche ai trattamenti non automatizzati, includono una migliore specificazione, sempre al menzionato art. 5, dei presupposti di legittimità del trattamento («*legitimacy of data processing*»), in aggiunta a quelli già previsti di qualità dei dati, individuando le relative basi giuridiche nel consenso (che, secondo quanto già previsto nel GDPR, anche per la Convenzione n. 108+ deve essere «*free, specific, informed and unambiguous*») oppure in altre «*legitimate basis laid down by law*».

Il modello offerto dalla disciplina dell'UE in materia di protezione dei dati personali è permeato in maniera evidente nell'ordinamento internazionale.

1.4. La liceità del trattamento nella Direttiva 95/46/CE

A livello della Comunità europea, il primo strumento normativo fondamentale in tale materia si ebbe con la Direttiva 95/46/CE del Parlamento europeo e del

---

[11] Si veda ad esempio la casistica cit. da F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 146 nota n. 65 e, segnatamente, Cedu, 6 aprile 2010, n. 184/06, *Saaristo et al. c. Finlandia*; Cedu, 21 febbraio 2002, n. 42409/98, *Schussel c. Austria*; Cedu, 24 giugno 2004, n. 5932/00, *Van Hannover c. Germania et al.*

[12] L'art. 8 della CEDU viene invocato anche dalla giurisprudenza nazionale. Si veda, per un esempio, il caso "*Segafredo*", affrontato in Cass., sez. I, 29 gennaio 2016, n. 1748, ampiamente trattato da F. Bravo, *Le condizioni di liceità del trattamento*, cit., pp. 146 ss. e F. Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, pp. 34-58.

[13] Firmato dall'Italia il 5 marzo 2019 e ratificato con l. n. 60 del 22 aprile 2021, «*Ratifica ed esecuzione del Protocollo di modifica alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, fatto a Strasburgo il 10 ottobre 2018*», pubblicata in G.U. n. 110 del 10 maggio 2021.

Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, destinata ad essere sostituita solo nel 2016 ad opera del GDPR, applicabile a far data dal 25 maggio 2018.

Il Capo II della Direttiva si occupava di delineare i limiti posti agli Stati membri per dettare le condizioni generali di liceità dei trattamenti di dati personali.

Così, l'art. 6, riprendendo il testo della citata Convenzione 108, stabiliva che, tra i principi relativi alla qualità dei dati, gli Stati membri dovessero disporre che i dati personali fossero «trattati lealmente e lecitamente» [lett. *a)*] e «rilevati per finalità determinate, esplicite e legittime» [lett. *b)*].

Anche nella Dir. 95/46/CE, così come ora nel GDPR, l'affermazione della liceità del trattamento era accompagnata da norme di dettaglio, volte a precisare, con riguardo ai dati comuni e ai dati sensibili, le specifiche condizioni di liceità del trattamento, individuate nel consenso o in altri presupposti di legittimazione[14].

[14] Il successivo art. 7 dettava i principi relativi alla legittimazione al trattamento dei dati, prevedendo le seguenti condizioni, ossia che: *a)* la persona interessata avesse manifestato il proprio consenso in maniera inequivocabile, oppure *b)* il trattamento fosse necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona, oppure *c)* il trattamento fosse necessario per adempiere un obbligo legale al quale era soggetto il responsabile del trattamento, oppure *d)* il trattamento fosse necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure *e)* il trattamento fosse necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui era investito il responsabile del trattamento o il terzo a cui venivano comunicati i dati, oppure *f)* il trattamento fosse necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui venivano comunicati ì dati, a condizione che non prevalessero l'interesse o i diritti e le libertà fondamentali della persona interessata.
L'art. 8, poi, prevedeva il generico divieto di trattamento dei c.d. dati particolari (definiti come quelli idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o che sono relativi alla salute e alla vita sessuale), salvo che non ricorresse una delle eccezioni previste dai parr. 2 e 3. Quanto al par. 2 occorreva che: *a)* la persona interessata avesse dato il proprio consenso esplicito a tale trattamento, salvo nei casi in cui la legislazione dello Stato membro prevedesse che il consenso della persona interessata non fosse sufficiente per derogare al divieto di cui al par. 1, oppure; *b)* il trattamento fosse necessario per assolvere gli obblighi e i diritti specifici del responsabile del trattamento in materia di diritto del lavoro, nella misura in cui il trattamento stesso fosse autorizzato da norme nazionali che prevedessero adeguate garanzie, oppure; *c)* il trattamento fosse necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata si trovasse nell'incapacità fisica o giuridica di dare il proprio consenso; o *d)* il trattamento fosse effettuato, con garanzie adeguate, da una fondazione, un'associazione o qualsiasi altro organismo che non perseguisse scopi di lucro e rivestisse carattere politico, filosofico, religioso o sindacale, nell'ambito del suo scopo lecito e a condizione che riguardasse unicamente i suoi membri o le persone che avessero contatti regolari con la fondazione, l'associazione o l'organismo a motivo del suo oggetto e che i dati non venissero comunicati a terzi senza il consenso delle persone interessate; o *e)* il trattamento riguardasse dati resi manifestamente pubblici dalla persona interessata o fosse necessario per costituire, esercitare o difendere un diritto per via giudiziaria. Quanto al par. 3, ai fini dell'applicazione delle eccezioni, occorreva che: il trattamento dei dati fosse necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura e quando il trattamento dei medesimi dati venisse effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale, comprese le norme stabilite dagli organi nazionali competenti, o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente.

1.5. La liceità del trattamento nella l. n. 675/96

L'Italia, come noto, aveva dapprima recepito la Direttiva 95/46/CE con la l. 31 gennaio 1996 n. 675, più volte modificata nel tempo, il cui art. 9 stabiliva che i dati personali oggetto di trattamento dovessero essere «trattati in modo lecito e secondo correttezza» [lett. *a)*] e «raccolti e registrati per scopi determinati, espliciti e legittimi» [lett. *b)*].

L'art. 11 ammetteva il trattamento dei dati personali, in via generale, solo con il consenso espresso dell'interessato, salvo il ricorrere di uno dei casi di esclusione della necessità del consenso previsti dal successivo art. 12, ossia quando il trattamento: *a)* riguardava dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; *b)* era necessario per l'esecuzione di obblighi derivanti da un contratto del quale era parte l'interessato o per l'esecuzione di misure precontrattuali adottate su richiesta di quest'ultimo, ovvero per l'adempimento di un obbligo legale; *c)* riguardava dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque; *d)* era finalizzato unicamente a scopi di ricerca scientifica o di statistica ed era effettuato nel rispetto dei codici di deontologia e di buona condotta; *e)* era effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità (con applicazione, in tale caso, del relativo codice di deontologia); *f)* riguardava dati relativi allo svolgimento di attività economiche raccolti anche ai fini di informazione commerciale o di invio di materiale pubblicitario, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; *g)* era necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non potesse prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere; *h)* era necessario ai fini dello svolgimento delle investigazioni difensive di cui alla l. 7 dicembre 2000 n. 397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati fossero trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; *h-bis)* era necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalessero i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.

I dati sensibili (ossia quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita

---

Agli Stati membri era comunque attribuita la facoltà, purché fossero previste le opportune garanzie, di stabilire, per motivi di interesse pubblico rilevante, ulteriori deroghe oltre a quelle sopra elencate, sulla base della legislazione nazionale o di una decisione dell'autorità di controllo (art. 8, par. 4).
I trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza potevano essere effettuati solo sotto controllo dell'autorità pubblica, o se venivano fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che potevamo essere fissate dallo Stato membro in base ad una disposizione nazionale che prevedesse garanzie appropriate e specifiche (art. 8, par. 5).

sessuale) potevano essere trattati solo con il consenso scritto dell'interessato, a pena di nullità, e previa autorizzazione del Garante (art. 22, co. 1)[15].

I dati inerenti alla salute, nello specifico, potevano essere trattati anche senza l'autorizzazione del Garante (oltre che senza il consenso dell'interessato) da parte degli esercenti le professioni sanitarie e degli organismi sanitari pubblici, limitatamente ai dati e alle operazioni indispensabili per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato. Qualora tali finalità riguardassero un terzo o la collettività, in mancanza del consenso dell'interessato, tornava ad essere necessaria l'autorizzazione preventiva del Garante (art. 23).

Infine, i dati relativi ai provvedimenti di cui all'art. 686 c.p.p. (iscrizioni nel casellario giudiziale) potevano essere oggetto di trattamento solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specificasse le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni autorizzate.

Una disciplina specifica, poi, era dettata per il trattamento di dati particolari nell'esercizio della professione di giornalista (art. 25) e da parte di soggetti pubblici (art. 27)[16].

---

[15] Il co. 4 dello stesso art. 22 prevedeva tuttavia la sola necessità dell'autorizzazione preventiva del Garante (prescindendo quindi dal consenso dell'interessato) nei seguenti casi: *a)* qualora il trattamento fosse effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, confessioni e comunità religiose, per il perseguimento di finalità lecite, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità avevano contatti regolari con l'associazione, ente od organismo, sempre che i dati non fossero comunicati o diffusi fuori del relativo ambito e l'ente, l'associazione o l'organismo determinasse idonee garanzie relativamente ai trattamenti effettuati; *b)* qualora il trattamento fosse necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non potesse prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere; *c)* qualora il trattamento fosse necessario ai fini dello svolgimento delle investigazioni difensive di cui alla l. 7 dicembre 2000 n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, di rango pari a quello dell'interessato quando i dati fossero idonei a rivelare lo stato di salute e la vita sessuale, sempre che i dati fossero trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

[16] Segnatamente, l'art. 27 («*Trattamento da parte di soggetti pubblici*») stabiliva che: «1. Salvo quanto previsto al comma 2, il trattamento di dati personali da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti.
2. La comunicazione e la diffusione a soggetti pubblici, esclusi gli enti pubblici economici, dei dati trattati sono ammesse quando siano previste da norme di legge o di regolamento, o risultino comunque necessarie per lo svolgimento delle funzioni istituzionali. In tale ultimo caso deve esserne data previa comunicazione nei modi di cui all'articolo 7, commi 2 e 3 al Garante che vieta, con provvedimento motivato, la comunicazione o la diffusione se risultano violate le disposizioni della presente legge.
3. La comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati o a enti pubblici economici sono ammesse solo se previste da norme di legge o di regolamento. (…)».

1.6. La liceità del trattamento nel d.lgs. n. 196/03 (Codice in materia di protezione dei dati personali), antecedentemente alla novellazione del 2018

Nel successivo d.lgs. 30 giugno 2003 n.196, recante il Codice in materia di protezione dei dati personali e abrogativo della precedente l. n. 675/1996, il principio di liceità trovava espressione nell'art. 11, ai sensi del quale i dati personali oggetto di trattamento dovevano essere «trattati *in modo lecito*» [lett. *a)*] e «raccolti e registrati per scopi determinati, espliciti e legittimi» [lett. *b)*].

Mentre per i trattamenti effettuati da soggetti pubblici era previsto appositamente il Capo II del Titolo III della Parte I, l'art. 23 confermava, per i trattamenti da parte di privati ed enti pubblici economici, la regola generale del consenso espresso dell'interessato, che doveva essere reso in forma scritta solamente a fini probatori per il trattamento di dati comuni e in forma scritta *ad substantiam* per il trattamento di dati sensibili[17].

Infatti, per quanto riguarda i dati sensibili, l'art. 26 consentiva il trattamento solo con il consenso scritto dell'interessato, a pena di nullità, e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché

[17] Erano comunque previste deroghe dal successivo art. 24 (oltre a quelle previste per specifici settori dalla Parte II), ossia quando il trattamento: *a)* fosse necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; *b)* fosse necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; *c)* riguardasse dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità stabiliti dalle leggi, dai regolamenti o dalla normativa comunitaria per la conoscibilità e pubblicità dei dati; *d)* riguardasse dati relativi allo svolgimento di attività economiche, trattati nel rispetto della normativa in materia di segreto aziendale e industriale; *e)* fosse necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguardasse l'interessato e quest'ultimo non potesse prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, si prevedeva che il consenso fosse manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato; *f)* con esclusione della diffusione, fosse necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati fossero trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; *g)* con esclusione della diffusione, fosse necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalessero i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato; *h)* con esclusione della comunicazione all'esterno e della diffusione, fosse effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'art. 13; *i)* fosse necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'art. 6, co. 2, del d.lgs. 29 ottobre 1999 n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

dalla legge e dai regolamenti. In deroga alla regola che precede, il comma 4 dello stesso art. 26 prevedeva specifici casi in cui sarebbe stata necessaria la sola autorizzazione preventiva del Garante (prescindendo quindi dal consenso dell'interessato)[18].

Infine, l'art. 27 prevedeva che il trattamento di dati giudiziari da parte di privati o di enti pubblici economici fosse consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specificasse le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

1.7. Novellazione del Codice in materia di protezione dei dati personali ad opera del d.lgs. n. 101 del 2018 e principio di liceità del trattamento

Nell'ordinamento italiano, l'adeguamento del Codice alle disposizioni del GDPR è avvenuto tramite il d.lgs. 10 agosto 2018 n. 101, sostanzialmente abrogando le norme generali che si sovrapponevano al Regolamento, effettuando un integrale richiamo al Regolamento per quanto riguarda le condizioni di liceità del trattamento, salvo specifiche disposizioni solo per alcuni aspetti, riguardanti, tra l'altro: (i) il trattamento effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 2-*ter* del c. *privacy*); (ii) il consenso del minore in relazione ai servizi della società dell'informazione (art. 2-*quinquies* del c. *privacy*); (iii) il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante (art. 2-*sexies* del c. *privacy*); (iv) il trattamento di dati relativi a condanne penali e reati (art. 2-*octies* del c. *privacy*); (v) i trattamenti in ambiti specifici, ai quali è dedicata la Parte II.

---

[18] Si tratta dei seguenti casi: *a)* quando il trattamento era effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità avevano contatti regolari con l'associazione, ente od organismo, sempre che i dati non fossero comunicati all'esterno o diffusi e l'ente, associazione od organismo determinasse idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'art. 13; *b)* quando il trattamento fosse necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguardava l'interessato e quest'ultimo non poteva prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso era manifestato da chi esercitava legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimorava l'interessato; *c)* quando il trattamento fosse necessario ai fini dello svolgimento delle investigazioni difensive di cui alla l. 7 dicembre 2000 n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati fossero trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati erano idonei a rivelare lo stato di salute e la vita sessuale, il diritto doveva essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; *d)* quando fosse necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111.

2. Portata applicativa del principio

2.1. Inquadramento teorico ed interpretazione dottrinale ed istituzionale del principio di liceità

Come visto nel paragrafo precedente, nel GDPR viene mantenuto il riferimento ai «principi», sotto la cui dicitura, che intitola il Capo II, vengono raccolte sia le norme sulle modalità del trattamento e sulla qualità dei dati che le norme sui diversi «presupposti legittimanti» il trattamento dei dati personali, ora denominate «condizioni di liceità».

Nonostante l'utilizzo di una terminologia complessivamente non lontana dalla precedente Direttiva, la portata innovativa del Regolamento è stata sottolineata dall'unanimità dei commentatori, in particolare, per un diverso approccio basato sull'*accountability* e su un maggior ricorso al *risk management* e per aver assestato in maniera diversa, rispetto al passato, il necessario bilanciamento di interessi, collettivi oltre che individuali, derivante dalle esigenze della modernità[19].

Il GDPR esplicita con chiarezza la rilevanza assunta, al pari del diritto sopra indicato, dalle esigenze legate alla circolazione dei dati rendendo così necessario un bilanciamento tra le due nature del dato oggetto del trattamento: diritto fondamentale da garantire, da un lato, e bene economico dal quale poter trarre un'utilità, dall'altro[20].

Il GDPR, infatti, sancisce espressamente che il diritto alla protezione dei dati personali, che aveva assunto nella Carta di Nizza l'autonoma rilevanza di diritto fondamentale alla stregua dei tradizionali diritti della personalità[21], non è (più) una prerogativa assoluta, «ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità», fra cui la libertà di pensiero, di espressione e di informazione e la libertà di impresa, a cui diviene funzionale la libera circolazione dei dati[22].

Altrettanto eloquente del mutato contesto, nonché, come si vedrà, della perdita della centralità del ruolo del consenso, è l'art. 1, par. 3, GDPR, ai sensi del quale «la libera circolazione dei dati personali nell'Unione non può essere limitata

---

[19] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 111 e 126.

[20] Cfr. N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 35 ss.; F. Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà «fondamentali», tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, p. 209 ss.; ma anche C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del contratto dei dati personali*, in *Contratto e impresa*, 2020, 2, p. 5, che parla della «natura fondamentalmente binaria dei dati personali».

[21] Cfr. art. 8 della Carta dei diritti fondamentali dell'UE.

[22] Cfr. *considerando* n. 4, GDPR. Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 111.

né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»[23].

Il pluralismo di interessi considerato dal Regolamento si traduce, per quanto qui interessa, nella presenza, accanto al consenso dell'interessato, di molteplici condizioni di liceità del trattamento dei dati personali altrui, le quali – appunto – bilanciano l'interesse del *data subject* con interessi diversi, propri del titolare o di terzi[24].

Pertanto, al fianco della tradizionale impostazione volta a descrivere le condizioni di liceità come elementi in grado di ripristinare la giuridicità del trattamento, altrimenti antigiuridico[25], si afferma ora che al verificarsi dei presupposti e delle condizioni previste dalla normativa, il trattamento dei dati personali altrui assurga all'esercizio di un vero e proprio «diritto al trattamento di dati personali», dinamicamente correlato, ma non per forza contrapposto, con il diritto dell'interessato alla protezione dei dati personali[26].

Come anticipato nel par. 1, l'art. 8 della Carta dei diritti fondamentali dell'UE non contiene riferimenti alla «liceità» ma richiede comunque che il trattamento avvenga sulla base di un «fondamento legittimo» (il consenso dell'interessato o altro fondamento alternativo), sottoposto a «riserva di legge necessaria».

In dottrina è stato evidenziato che l'utilizzo del termine «liceità» nel GDPR, dal punto di vista semantico, può essere ritenuto significativo sotto una duplice accezione: da un lato, quella positiva di conformità all'ordinamento, non limitato alla sola disciplina in esame[27] ma comprensivo delle norme dettate in altri settori[28]; dall'altro lato, quella negativa di difetto di liceità, nel senso cumulativo di contrarietà all'ordinamento e lesione degli interessi protetti[29].

Da ciò è derivata l'attribuzione al concetto di liceità di due significati, strutturalmente diversi ma concettualmente collegati, che si traducono a loro volta in quello

---

[23] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 131; F. BRAVO, *Il «diritto» a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 210 e ss.; F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà «fondamentali», tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, cit., p. 209 ss.

[24] Cfr. D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, 12, pp. 2783 ss.

[25] Utilizzando, di caso in caso, le categorie delle esimenti del consenso dell'avente diritto, dell'esercizio di un diritto, dell'adempimento di un dovere, dello stato di necessità, dell'esigenza di salvaguardare un superiore interesse pubblico, a beneficio della collettività.

[26] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 119 e 120.

[27] Interpretazione restrittiva che, altrimenti, potrebbe tradursi in un pleonasmo normativo; si v. diffusamente F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 112 ss.

[28] Il riferimento è alla Costituzione, al Codice civile, allo Statuto dei lavoratori, ecc., nonché ai principi generali dell'ordinamento giuridico. Cfr. P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, vol. I, pp. 411 e 412.

[29] In questo senso si veda, ancora, F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, cit., pp. 111 ss. e, ivi, spec. p. 116 ss.

che è stato definito un «processo bifasico di valutazione»[30]: i) la presenza di almeno uno dei «presupposti di legittimazione» («condizioni di liceità» nella terminologia dell'art. 6 GDPR, ove sono elencati), in assenza dei quali il trattamento non può ritenersi legittimamente svolto; ii) selezione dei trattamenti ammessi dall'ordinamento, mediante la valutazione della conformità o meno al diritto in relazione alla lesione o meno di altri interessi e valori concorrenti o contrapposti e al loro necessario bilanciamento [art. 5, par. 1, lett. *a)*, GDPR].

Secondo questa ricostruzione dogmatica, dunque, le «condizioni di liceità» del trattamento, che verranno approfondite nei paragrafi che seguono, costituiscono dei «meccanismi, predeterminati dal legislatore europeo, per effettuare un primo vaglio, a monte, nel procedimento selettivo che porta alla giusta composizione degli interessi contrapposti, di cui sono portatori, in primo luogo, l'interessato e il titolare del trattamento»[31].

Senza dimenticare il diverso orientamento che ha, invece, sottolineato il carattere univoco del giudizio di liceità, è stato comunque efficacemente evidenziato che il rapporto tra l'art. 5 e l'art. 6 del GDPR va letto «in progressione numerica invertita, posto che, prima di definire "il modo" con cui eseguire il trattamento, occorre individuare "le condizioni" che lo rendono *ex ante* lecito»[32].

All'art. 6, relativo ai dati comuni, va correlato, in un rapporto di continenza[33], l'art. 9 che, come visto nel par. 1, enumera le ipotesi che legittimano il trattamento, altrimenti vietato, delle categorie particolari di dati personali.

L'art. 9 si presta alle medesime considerazioni svolte per l'art. 6, seppure il confronto tra le due norme evidenzi alcune peculiari scelte legislative, come l'indicazione di condizioni per il trattamento dei dati particolari non sempre più rigorose di quelle dettate per i dati comuni[34] e, soprattutto, la citata formulazione in negativo, che può essere però spiegata facilmente con l'«intento di scongiurare applicazioni in via analogica e interpretazioni estensive con riguardo ai dati appartenenti a categorie particolari, dato che le condizioni di liceità verrebbero a configurarsi formalmente come norme di eccezione»[35].

Le condizioni di liceità del trattamento, nel GDPR, assumono un'analoga valenza[36], dovendosi considerare tra loro equipollenti ed alternative, come si ricava

---

[30] Definizione fornita da F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, cit., p. 121, al quale si rimanda per maggiori approfondimenti.

[31] Cfr. F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, cit., pp. 124-125; F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 114.

[32] Cfr. D. Poletti, *op. cit.*, pp. 2783 ss.

[33] Cfr. D. Poletti, *op. cit.*, pp. 2783 ss.: «nel senso che l'art. 6 enuncia le condizioni di liceità valide per il trattamento di tutti i dati personali, mentre l'art. 9 rende inapplicabile, nei casi elencati, il divieto generale di trattamento delle categorie particolari di dati».

[34] Tanto da sollevare l'interrogativo se la relazione tra le due norme debba essere intesa in via «alternativa» o «di cumulo»; cfr. D. Poletti, *op. cit.*, pp. 2783 ss. e L. Bolognini-E. Pelino, *Condizioni di liceità*, in L. Bolognini-E. Pelino-C. Bistolfi (a cura di), *Regolamento privacy europeo*, Milano, 2016, p. 277.

[35] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 119.

[36] Ad eccezione, a ben vedere, del trattamento dei dati necessario a proteggere un interesse vitale dell'interessato o di terzi che, secondo il *considerando* n. 46, dovrebbe avere luogo in linea di prin-

dall'art. 6 che richiede il ricorrere di «almeno una» di queste condizioni, senza, dunque, che possa più configurarsi un rapporto di regola-eccezione tra di esse[37].

Volendo tracciare una demarcazione generale, si può osservare come le condizioni di liceità siano orientate secondo due direttrici, il consenso e la necessità, quest'ultima tuttavia in grado di comprendere ipotesi disomogenee tra loro e non ordinate sistematicamente[38].

È appena il caso di evidenziare che il parametro della necessità del trattamento compone così (al di fuori del consenso) la stessa nozione di liceità e, mantenendo valido il monito del Gruppo di lavoro *ex* art. 29 che ne aveva suggerito – seppure sotto la vigenza della Direttiva – un'interpretazione in senso rigoroso[39], si può concludere che debba «ritenersi esclusa la liceità di un trattamento quando le finalità prescelte possano essere raggiunte in maniera alternativa, senza ricorrere all'impiego di dati personali, anche nel rispetto del principio di minimizzazione»[40].

In letteratura, vari sono stati i tentativi di fornire una classificazione, tentando ad esempio di ricondurre le condizioni di liceità in tre diverse categorie di legittimazione: i) la legittimazione contrattuale; ii) la legittimazione legale e iii) la legittimazione comparativa[41].

In modo non dissimile, nella presente trattazione si è scelto di fare riferimento al centro valutativo al quale la normativa attribuisce il bilanciamento dei diversi interessi coinvolti e ciò in linea con l'orientamento già tacciato dalla dottrina[42].

Infatti, premesso che la scelta della condizione di liceità di un determinato trattamento spetta al titolare e rientra nella sua responsabilizzazione il dovere di dimostrare la correttezza e la validità della scelta, nelle ipotesi in cui la base giuridica sia rappresentata dal consenso dell'interessato [art. 6, par. 1, lett. *a)*, GDPR], l'ordinamento rimette a quest'ultimo il «ruolo di valutatore di tale bilanciamento, accordando rilevanza al potere di autodeterminazione informativa»[43].

Nel caso del contratto o di misure precontrattuali adottate su richiesta dell'interessato [art. 6, par. 1, lett. *b)*, GDPR], il bilanciamento di interessi è rimesso alla valutazione congiunta di titolare ed interessato, mentre nell'ipotesi in cui il trattamento si fondi sul legittimo interesse del titolare [art. 6, par. 1, lett. *f)*, GDPR], tale bilanciamento è rimesso al titolare stesso.

---

cipio in via residuale, ossia unicamente quando il trattamento non possa essere fondato su un'altra base giuridica.

37 F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 130.

38 Cfr. C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., p. 6.

39 GRUPPO DI LAVORO EX ART. 29, *Opinion* n. 6/2014

40 Cfr. D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, cit., pp. 2783 ss.

41 Cfr. M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 221.

42 Si veda, in tal senso, F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, cit., pp. 101 ss., nonché F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 110 ss.

43 Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 143.

Infine, il bilanciamento dell'assetto degli interessi è effettuato direttamente dal legislatore nelle altre condizioni di liceità, ossia l'adempimento di un obbligo legale [art. 6, par. 1, lett. *c)*, GDPR], la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica [art. 6, par. 1, lett. *d)*, GDPR] e l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri [art. 6, par. 1, lett. *e)*, GDPR].

Scopo del presente paragrafo è l'esame dei principali aspetti teorici emersi per ciascuna condizione di liceità, per poi esaminarne nel successivo par. 3 i risvolti applicativi nella casistica maggiormente rilevante.

2.2. Condizioni di liceità rimesse alla valutazione dell'interessato: il consenso

Nelle norme di attuazione della Direttiva 95/46/CE il consenso dell'interessato assumeva, almeno formalmente, un valore di regola generale, della quale gli altri criteri alternativi rappresentavano l'eccezione.

A ben vedere, tale rapporto regola-eccezione non traeva la sua fonte nel testo della Direttiva ma risultava il frutto di una scelta del legislatore italiano[44], criticata in particolare da quella parte di dottrina che ha stigmatizzato la «ritrosia a prendere atto che sull'attività contrattuale svolta nel fenomeno dei dati personali insistessero, per la natura così speciale del bene, due discipline, in ragione della coesistenza in quella vicenda negoziale, di situazioni relative ed assolute, un diritto delle obbligazioni ed un diritto assoluto della personalità»[45].

Con l'entrata in vigore del Regolamento, è stata ribadita l'assenza di un ruolo centrale ed esclusivo attribuito all'autonomia privata ed in particolare al consenso dell'interessato, trattandosi «solo di uno dei criteri alternativi volti a dare fondamento legittimo all'attività di trattamento posta in essere dal titolare e, al contempo, operare quale meccanismo di primo livello nella selezione degli interessi protetti dall'ordinamento giuridico»[46].

Com'è stato correttamente osservato, «[n]on si deve infatti ritenere che il consenso costituisca sempre il fondamento più adeguato perché [come si vedrà *amplius* nel prosieguo, *n.d.a.*] svariati possono essere i casi nei quali questo risulti solo apparente, non capace pertanto di legittimare il trattamento»[47].

La centralità del consenso rimane tuttavia nel dibattito dottrinale, diviso tra i fautori di un approccio personalistico e i sostenitori di un approccio contrattuale-dispositivo, proprio perché mantiene «il ruolo di strumento giuridico di composizione del conflitto tra autodeterminazione della propria personalità e libertà informatica»[48],

---

[44] Si v., in particolare, gli artt. 23 e 24 del c. *privacy*, ora abrogati.

[45] V. Ricciuto, *La patrimonializzazione dei dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 29.

[46] F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 130.

[47] Cfr. C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., p. 8.

[48] S. Mazzamuto, *Il principio del consenso e il problema della revoca*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, I, p. 994.

rimettendo all'interessato la valutazione in ordine al bilanciamento tra gli interessi alla protezione o alla circolazione dei dati, a fronte delle condizioni di liceità alternative in cui «è lo stesso legislatore che ha provveduto a determinare i meccanismi di selezione degli interessi in gioco, bilanciandoli aprioristicamente sulla base di scelte di politica legislativa, lasciando in ogni caso all'interessato l'esercizio dei poteri di monitoraggio e controllo»[49].

La centralità del dibattito sul consenso si coglie appieno se si considera che nella sua interpretazione si traducono i diversi «modelli di lettura» del diritto alla protezione dei dati personali, rispetto ai quali nel corso degli anni si è assistito ad esegesi diverse, «tutte verosimilmente plausibili a seconda del "modello" di riferimento adottato dall'interprete, ancorché nessuna di esse è stata ritenuta di per sé completamente "appagante"»[50].

Con riferimento alla previgente normativa, il dibattito era focalizzato attorno ai due poli di chi attribuiva al consenso valenza «autorizzatoria» e chi «negoziale-dispositiva».

Rimandando per una completa analisi delle diverse ricostruzioni dogmatiche alle rispettive opere[51], in questa sede ci si limita a ricordare che il primo dei due orientamenti, muovendo dal presupposto dell'inquadramento del diritto alla protezione dei dati personali tra i diritti fondamentali della persona e dell'applicabilità dei caratteri di assolutezza, indisponibilità, intrasmissibilità ed imprescrittibilità propri di questi ultimi, ha classificato il consenso dell'interessato come «atto di autorizzazione», in forza del quale il titolare è legittimato a trattare i dati personali, con conseguente liceità della loro circolazione (altrimenti illecita), senza che cessi l'appartenenza dei dati all'interessato, quali attributi della sua personalità.

A tale valenza autorizzatoria alcuni autori hanno aggiunto una «funzione di regolamentazione», quale «atto dirett[o] a definire modalità e condizioni del trattamento, vincolando sensibilmente l'attività del titolare»[52], mentre altri autori hanno sottolineato la natura fondamentalmente «adesiva» del consenso dell'interessato, il quale si trova a prestare il proprio «assenso»[53] ad un trattamento la cui determinazione delle finalità, modalità e caratteristiche è rimessa al titolare ed è tendenzialmente omogenea per una serie indefinita di interessati[54].

---

[49] F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 134.

[50] Così F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 134, ove richiama il rilievo di S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, 6, pp. 621 ss. Si veda anche V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., p. 40.

[51] Per una efficace disamina del dibattito dottrinale e per la relativa bibliografia si rimanda a F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 135-140.

[52] Cfr. F. CAFAGGI, *Qualche appunto su circolazione, appartenenza e riappropriazione dei dati personali*, in *Danno e resp.*, 1998, pp. 619 ss.

[53] Termine utilizzato ora anche dal GDPR nella definizione stessa di consenso, contenuta all'art. 4, par. 1, n. 11, v. *infra*.

[54] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 136.

In una posizione affine alla precedente merita di essere citato l'orientamento dottrinale che ha fatto espressamente riferimento alla fattispecie del concorso dell'avente diritto con valore di scriminante, sul modello dell'art. 50 c.p.[55].

Una diversa impostazione dottrinale, invece, come anticipato, ha privilegiato la natura negoziale e dispositiva del consenso dell'interessato, muovendo dalla ritenuta necessità di lettura della disciplina «non esclusivamente in termini di tutela della persona, bensì di regolamentazione di un settore dell'attività», per cui «il consenso, più che costituire una sorta di rinuncia dell'avente diritto alla propria *privacy*, esprime invece la condizione soggettiva per la reificazione dei dati personali, che per suo tramite entrano per così dire sul mercato in quanto beni suscettibili di autonoma considerazione economica»[56].

Nell'ambito di tale dibattito dottrinale occorre ora fare riferimento all'art. 7 («*Condizioni per il consenso*»), all'art. 8 («*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*») e, a livello definitorio, all'art. 4, par. 1, n. 11 che descrive il consenso come «qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

La formulazione letterale dell'ultima norma citata, coordinata con il *considerando* n. 32[57], ha indotto parte della dottrina a qualificare il consenso dell'interessato, nell'accezione del GDPR, come «autorizzazione integrativa» (e non costitutiva) «avente l'effetto di rimozione di un limite all'esercizio di un diritto o di un potere già acquisito dal titolare del trattamento»[58], nel senso che l'interessato non «trasferisce ad altri un potere che fa capo a sé medesimo, ma (...) con il proprio assenso all'altrui attività di trattamento, rimuove un ostacolo o un limite al potere o alla facoltà che l'ordinamento già accorda al titolare del trattamento, in funzione del perseguimento di propri interessi, lecitamente perseguiti»[59].

---

[55] Cfr. S. Patti, *sub art. 23*, in C.M. Bianca-D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno, 196 ("Codice della privacy")*, Padova, 2007, tomo I, p. 553.

[56] Cfr. V. Cuffaro, *A proposito del ruolo del consenso*, in V. Cuffaro-V. Ricciuto-V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1999, p. 121.

[57] Ai sensi del quale «Il consenso dovrebbe essere espresso mediante un atto dispositivo inequivocabile (...) con il quale l'interessato manifesta l'intenzione di accettare il trattamento dei dati personali che lo riguardano (...)».

[58] Per l'approfondimento di questa interpretazione si rimanda diffusamente a F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 140-150.

[59] In particolare, meritano di essere riportate, a supporto di questa impostazione, le riflessioni per cui «l'attività di trattamento rimane lecita anche quando il consenso non sia previsto o venga revocato e il trattamento sia basato su altre condizioni di liceità alternative» e, essendo il consenso revocabile, la revoca «porta nuovamente a "ricostituire" il limite (o l'ostacolo) all'esercizio dei poteri di predisposizione del trattamento, con la conseguenza che il trattamento non possa essere legittimamente svolto, a meno che non muti la base giuridica verso un altro fondamento legittimo, alternativo al consenso dell'interessato». Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 144.

Rimandando ai paragrafi successivi l'analisi del rapporto tra consenso così inteso e contratto, si esaminano ora i requisiti che il GDPR, con le norme citate, detta per il consenso dell'interessato.

Il consenso, innanzitutto, deve essere «informato», ossia preceduto dalla comunicazione all'interessato di tutte le informazioni previste dagli artt. 13 e 14 GDPR, la cui rilevanza e funzionalità rispetto ad una valida manifestazione della propria autodeterminazione informativa si percepiscono considerando che, generalmente, l'interessato può prestare il proprio consenso solo acconsentendo (o negando) al trattamento predisposto dal titolare o, al più, selezionando a quali finalità aderire nel caso ne siano prospettate diverse[60].

Il consenso deve, inoltre, essere «specifico», ossia espresso «per una o più specifiche finalità»[61], per il perseguimento delle quali il trattamento deve essere determinato in tutte le sue caratteristiche (oggetto, finalità, ambito di circolazione dei dati, durata, modalità, ecc.)[62].

A tale proposito, il *considerando* n. 32 chiarisce che il consenso si applica a tutte le attività di trattamento svolte per la stessa finalità, senza, dunque, che l'interessato possa escludere selettivamente alcune di esse[63], mentre, qualora il trattamento persegua più finalità, ciascuna di esse richiede un consenso specifico[64].

Un ulteriore requisito fondamentale del consenso, per la sua validità, è che sia «libero», ossia, come chiarito dal Gruppo di lavoro *ex* art. 29[65], che sia prestato in virtù di una «scelta effettiva» in capo all'interessato, senza che la sua manifestazione di volontà sia coartata od influenzata da condizionamenti[66] derivanti da uno squilibrio di potere (si pensi alla soggezione nei confronti del datore di lavoro oppure di un'autorità pubblica)[67] oppure da pregiudizi per il rifiuto o la revoca[68].

Particolari problemi interpretativi sono scaturiti, come testimonia anche il conflitto ermeneutico tra Garante e Corte di Cassazione[69], dalla lettura dell'art. 7,

---

60 Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 151.

61 Come espressamente indicato dall'art. 6, par. 1, lett *a)*, GDPR.

62 Cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., p. 1016.

63 Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 152.

64 A tale proposito viene in rilievo il concetto di «granularità» del consenso, ossia la necessità di distinte manifestazioni di volontà dell'interessato, rilevante anche sotto il profilo della libertà perché diversamente, chiedendo un unico consenso per diverse finalità, il consenso non può ritenersi libero. Cfr. Gruppo di lavoro *ex* art. 29, Linee guida sul consenso ai sensi del Regolamento (UE) 2016/679, del 28 novembre 2017, modificate il 10 aprile 2018 (WP 259 rev. 01), 11; cfr. EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 5 maggio 2020.

65 Gruppo di lavoro *ex* art. 29, Linee guida sul consenso ai sensi del Regolamento (UE) 2016/679, cit.; cfr. EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, cit.

66 Il Gruppo di lavoro *ex* art. 29, nelle citate Linee guida sul consenso, utilizza il termine «condizionalità» per individuare tutte le ipotesi di un'«azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in vari modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio (...)».

67 Esempi forniti dalle stesse Linee guida sul consenso, *cit.*

68 Sul punto il *considerando* n. 42 fornisce maggiori criteri ermeneutici, oltre a chiarire che il Regolamento «non esclude tutti gli incentivi, tuttavia spetta il titolare del trattamento dimostrare che il consenso è stato prestato liberamente in tutte le circostanze».

69 Che verrà approfondito, *infra*, nel successivo par. 3, al quale si rimanda.

par. 4, GDPR, il quale precisa che «nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione del contratto».

Infine, sempre da un punto di vista sostanziale, il consenso deve essere «inequivocabile», ossia consistere in una manifestazione di volontà espressa mediante atto positivo che non possa lasciare dubbi sulla sua effettiva esistenza, da cui deriva il corollario per cui non possono «configurare consenso il silenzio, l'inattività o la preselezione di caselle» effettuata dal titolare del trattamento[70].

Sotto il profilo formale, una novità del Regolamento è rappresentata dal fatto che il consenso non richiede ora una forma scritta *ad substantiam* né *ad probationem*, con il limite, sopra richiamato, della sua forma espressa ed inequivocabile ed il contraltare rappresentato dalla necessità per il titolare di dimostrare, seppure con ogni mezzo, che il consenso sia stato effettivamente prestato, in virtù del principio di *accountability* (art. 5, par. 2, GDPR).

Una ulteriore novità del Regolamento riguarda la durata del trattamento, che, determinato o quantomeno determinabile, rientra ora tra gli obblighi informativi del titolare[71] e che concorre, dunque, a costituire il *set* informativo a disposizione dell'interessato per decidere se prestare o meno il proprio consenso.

Infine, ai sensi dell'art. 7, par. 3, GDPR, il consenso deve essere «*revocabile*» in qualsiasi momento, con la stessa facilità con cui è stato prestato, senza che ciò pregiudichi la liceità del trattamento anteriore alla revoca.

Non sembrano esservi particolari problemi interpretativi circa l'efficacia *ex nunc* della revoca (ossia senza effetti retroattivi), sulla sua esercitabilità *ad nutum* (ossia senza necessità di giustificati motivi o di giusta causa) e sulla sua ontologica autonomia rispetto al diritto di opposizione[72].

Nel vigore della precedente normativa – che non prevedeva espressamente l'istituto del diritto alla revoca – vi era stato chi aveva ipotizzato una delimitazione temporale per il suo esercizio in relazione al contrapposto affidamento ingenerato nel titolare del trattamento[73]. Il Regolamento, tuttavia, pare aver fugato ogni dubbio nella parte in cui, come visto, indica che la revoca del consenso possa avvenire «in qualsiasi momento» e, d'altro canto, ha attribuito rilevanza (*rectius*, prevalenza) al legittimo interesse del titolare in una distinta condizione di liceità[74].

---

[70] *Considerando* n. 32 del GDPR.

[71] Art. 13, par. 2, lett. *a)* ed art. 14, par. 2, lett. *a)*, GDPR.

[72] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 158.

[73] Cfr. S. Mazzamuto, *Il principio del consenso e il problema della revoca*, cit., p. 1041.

[74] «Sicché l'interesse del titolare, per avere un effetto paralizzante sul diritto di revoca (...) dovrebbe quantomeno superare la soglia di prevalenza indicata dalla disposizione *de qua* (...)» e il diritto di revoca, in tal caso, «non è più esercitabile perché verrebbe a mutare la condizione di liceità applicabile al caso di specie, la quale, accordando rilevanza all'interesse del titolare secondo la tipizzazione operata dal legislatore, farebbe venir meno il presupposto stesso di applicazione del diritto di revoca». Così F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 160.

2.2.1. *In particolare, il consenso dei minori*

Il tema del consenso dei minori ha comportato non poche difficoltà interpretative, soprattutto perché il legislatore europeo, con una scelta non esente da critiche e perplessità in ordine ad aspetti di carattere sistematico, all'art. 8 del GDPR ha dettato una norma speciale solo per i trattamenti basati sul consenso che abbiano ad oggetto dati comuni e riguardino un'offerta diretta di servizi della società dell'informazione ai minori, stabilendo che, in tali casi, il trattamento dei dati personali del minore è lecito ove il minore abbia almeno 16 anni (14 anni in Italia, in virtù dell'art. 2-*quinquies* del c. *privacy* post-riforma del 2018)[75].

Oltre a ciò, il legislatore ha ritenuto di precisare, sempre (solo) all'interno dell'art. 8 relativo al consenso dei minori nei servizi della società dell'informazione, che la norma ivi contenuta «non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore»[76].

La lettura combinata delle due disposizioni che precedono ha sollevato il dubbio che l'intenzione del legislatore potesse essere quella di attribuire, nell'ambito applicativo dell'art. 8 del GDPR, una «capacità di agire speciale» al minore di «stipulare validamente contratti di cessione dei dati personali», come ha sostenuto chi qualifica il consenso al trattamento dei dati come «consenso negoziale»[77].

In senso opposto, si è sostenuto che la citata clausola di salvezza delle norme nazionali in materia di validità e formazione del contratto implichi che il consenso prestato dal minore per il trattamento dei dati, nelle fattispecie in esame, «non faccia venir meno la necessità che il consenso contrattuale sia manifestato da chi eserciti la responsabilità genitoriale», con la conseguenza che, «ove (...) anche tale consenso [contrattuale] sia prestato dal minore, (...) il contratto dovrà ritenersi annullabile, in quanto concluso da soggetto incapace di agire»[78].

---

[75] Per una ampia disamina dell'argomento si rimanda a F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 164-181 e, anche per una panoramica dei diversi limiti di età individuati dagli Stati membri e per le problematiche relative alla verifica dell'età del minore ed alla corretta acquisizione del consenso, a G. BIANCHEDI, *Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico*, in *Ciberspazio e diritto*, 2019, 3, pp. 389-413.

[76] Art. 8, par. 3, GDPR.

[77] In tal senso cfr. V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., pp. 54-57. Questa interpretazione, a parere di chi scrive, evidenzia ancora di più la singolarità della scelta del legislatore europeo in direzione di un maggiore *empowerment* (e conseguente esposizione) della stessa categoria di soggetti (i minori) che il Regolamento afferma essere meritevoli di «specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali» (*considerando* n. 38). Si v., a tale ultimo proposito, anche GRUPPO DI LAVORO EX ART. 29, Linee Guida sul consenso, cit. e EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, cit.

[78] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 174, il quale attribuisce, per tali motivazioni, la particolare rilevanza della norma anche in relazione ai «trattamenti di dati relativi ai minori effettuati dai fornitori di servizi della società dell'informazione mediante l'utilizzo dei *cookies* acquisiti dagli utenti durante la mera attività di navigazione, a prescindere dalla conclusione (eventuale) del contratto di fornitura».

Anzi, tale orientamento trae una conferma della natura del consenso quale «autorizzazione integrativa» (invece che contrattuale / negoziale / dispositiva) proprio dalla richiesta del legislatore europeo, ritenuta di «grande rilievo sistematico», di «requisiti diversi per la capacità di agire ai fini del compimento dell'atto di consenso al trattamento dei dati personali e per la capacità di agire necessaria ai fini della manifestazione del consenso di natura contrattuale»[79].

2.3. Condizioni di liceità rimesse alla valutazione congiunta tra interessato e titolare: esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato

La condizione di liceità prevista dall'art. 6, par. 1, lett. *b)*, GDPR ha sollevato diversi problemi interpretativi per quanto riguarda il rapporto con il consenso al trattamento dei dati personali.

Come accennato, infatti, la revoca del consenso al trattamento dei dati ha comportato dubbi, sul piano ermeneutico, quando avviene nell'ambito di una cornice contrattuale[80], circostanza che risente dei diversi «modelli di lettura del consenso» esaminati poc'anzi.

A tale proposito, i sostenitori della natura negoziale del consenso al trattamento dei dati personali lo ritengono implicitamente (o presuntivamente) prestato con il consenso contrattuale quando il trattamento sia necessario per l'esecuzione di un contratto tra interessato e titolare.

Al contrario, chi propende per la natura autorizzatoria del consenso ritiene che in caso di operatività della condizione di liceità *ex* art. 6, par. 1, lett. *b)*, GDPR, in cui il trattamento dei dati sia necessario per l'esecuzione del contratto tra interessato e titolare, il consenso al trattamento dei dati debba intendersi radicalmente superato, proprio in virtù «del prevalente interesse alla circolazione dei dati personali in ragione dell'interesse stesso alla esecuzione del rapporto contrattuale»[81].

Di conseguenza, la questione relativa alla revoca viene risolta tenendo separata, da un lato, (i) l'ipotesi in cui non vi siano finalità e trattamenti ulteriori rispetto a quelli necessari per l'esecuzione del contratto, nella quale opera la condizione di liceità *ex* art. 6, par. 1, lett. *b)*, GDPR e, non essendo necessario il consenso al trattamento dei dati, non sussiste la possibilità di una sua revoca, e, dall'altro lato, (ii) l'ipotesi in cui le finalità di trattamento siano esorbitanti rispetto a quelle necessarie per l'esecuzione del contratto, ritenendo che, per esse, torni ad operare la necessità del consenso al trattamento *ex* art. 6, par. 1, lett. *a)*, GDPR, con conseguente revocabilità dello stesso[82].

---

[79] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 181.

[80] Cfr. S. Mazzamuto, *Il principio del consenso e il problema della revoca*, cit., p. 1042 e ss.; G. Resta, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in U. Breccia-L. Bruscuglia-F.D. Busnelli (a cura di), *Il diritto privato nel prisma dell'interesse legittimo*, Torino, 2001, pp. 52 ss.

[81] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 162.

[82] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 163.

Questa impostazione, si noti, presuppone l'assunto di partenza per cui una rigorosa lettura delle norme del GDPR[83] imponga la limitazione dei trattamenti riconducibili alla lett. *b)* perché necessari all'esecuzione del contratto solamente a quelli funzionali all'esecuzione della prestazione che il titolare pone in essere quale debitore dell'interessato, con la conseguente inapplicabilità della condizione di liceità *sub* lett. *b)* per i trattamenti posti in essere sui dati conferiti dall'interessato quali oggetto di una propria controprestazione debitoria, all'interno di operazioni indicate con il termine «scambio di dati»[84], frequenti nel campo dei servizi della società dell'informazione, ove il fornitore, titolare del trattamento, richiede al cliente-interessato il conferimento dei dati per la remuneratività del servizio, in ordine al quale non viene preteso alcun corrispettivo in denaro[85].

Per quanto riguarda, infine, le «misure precontrattuali adottate su richiesta dell'interessato» cui fa riferimento l'art. 6, par. 1, lett. *b)*, GDPR, in dottrina è stato osservato che trattasi delle attività di trattamento «funzionalmente collegate con la conclusione o l'esecuzione del contratto, poste in essere in una fase antecedente al suo perfezionamento», da distinguere rispetto alle attività di trattamento poste in essere in esecuzione di obblighi normativi, alle quali si applica la condizione di liceità relativa alla necessità di adempiere ad un obbligo legale *ex* art. 6, par. 1, lett. *c)*, GDPR[86].

2.3.1. *In particolare, la commercializzazione dei dati personali tra consenso e contratti di scambio*

Nello specifico, poi, maggiori criticità sono state evidenziate «qualora il contratto (i) abbia direttamente ad oggetto il trattamento dei dati personali dell'interessato ovvero (ii) implichi la facoltà per il titolare del trattamento di utilizzare economicamente i dati personali dell'interessato (ad esempio al fine di ricavare un'utilità economica nei rapporti contrattuali con soggetti terzi e garantire così al titolare del trattamento quel ritorno economico che gli consente di evitare richieste di compensi in denaro nella fornitura di servizi della società dell'informazione agli utenti-interessati)»[87].

Si è detto, in particolare, che il fatto che il trattamento sia basato sul consenso dell'interessato [*ex* art. 6, par. 1, lett. *a)*, GDPR e art. 9, par. 2, lett. *a)*, GDPR], non priva quest'ultimo della facoltà di «contrattualizzare la rimozione del limite» all'esercizio del diritto del titolare, «mediante la previsione di una controprestazione a

---

[83] E, in particolare, del citato art. 7, par. 4, GDPR che richiede espressamente «che vi sia il consenso al trattamento dei dati personali, distinto da quello contrattuale, qualora l'esecuzione del contratto da parte del titolare del trattamento sia subordinata alla manifestazione del consenso, da parte dell'interessato, al trattamento di dati personali non necessario alla predetta esecuzione»; cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 163.

[84] Cfr. F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, cit., 34 ss.

[85] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 192.

[86] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 190.

[87] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 191.

suo vantaggio a fronte del beneficio che il titolare del trattamento ricava dall'atto di autorizzazione»[88].

In tal modo, le due nature del consenso, tradizionalmente viste come antitetiche, finiscono per coesistere ed interagire, prospettandosi due consensi «tra loro funzionalmente collegati»: i) uno di natura «autorizzatoria integrativa» ed ii) uno «di natura contrattuale, con il quale l'interessato – dopo aver rimosso il limite previsto dall'ordinamento al potere del titolare di svolgere l'attività di trattamento (...) – concorda con il titolare del trattamento le modalità di utilizzo dei dati, anche in una logica di natura patrimoniale», senza mai spogliarsi del controllo su di essi, «potendo sempre far venire meno il consenso autorizzatorio reso in materia di protezione dei dati personali, mediante l'esercizio del diritto di revoca»[89].

Il collegamento funzionale tra i due consensi sopra citati comporta, come corollario fondato sull'art. 7, par. 3, GDPR, che consente all'interessato di revocare il proprio consenso «in qualsiasi momento», anche quando inserito in una cornice contrattuale, che la revoca del consenso al trattamento dei dati personali, di natura autorizzatoria, comporterebbe la caducazione anche degli effetti dell'accordo sull'utilizzo, a titolo oneroso o gratuito, dei dati[90].

Il tema, così delineato da un punto di vista teorico, è complesso e merita di essere approfondito anche dal punto di vista dell'interpretazione fornita dalla giurisprudenza di legittimità, come si vedrà, *infra*, nel successivo par. 3.

2.4. Condizioni di liceità rimesse alla valutazione del legislatore: adempimento di un obbligo legale, salvaguardia di interessi vitali dell'interessato o di un'altra persona, esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri

Le condizioni di liceità «rimesse alla valutazione del legislatore» (adempimento di un obbligo legale, salvaguardia di interessi vitali dell'interessato o di altra persona, esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) appartengono ad una tipologia di condizioni di liceità che riflette previsioni sostanzialmente già contenute nella disciplina anteriore al Regolamento, seppure con alcune differenze lessicali e, soprattutto, con la citata perdita del ruolo di eccezioni, rispetto alla regola generale del consenso, che avevano assunto nella normativa italiana di attuazione della Direttiva 95/46/CE.

Esse rappresentano, inoltre, un esempio degli ampi margini di autonomia lasciati agli Stati membri, ai quali ordinamenti interni (al pari del diritto UE), nello

[88] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 145.

[89] *Ibidem*.

[90] Con eventuali ulteriori effetti giuridici, che esulano dallo scopo di questo lavoro ed ai quali si fa, dunque, mero riferimento. Ci si è chiesti, ad esempio, se «nel caso di cessione dei dati personali per finalità di profilazione e *marketing* in cambio di sconti, tramite *fidelity card*, in occasione dell'acquisto di beni e servizi, la revoca dell'autorizzazione al trattamento dei dati personali» comporti «sul piano contrattuale (...) il recupero delle somme corrispondenti agli sconti praticati dal venditore di beni o dal fornitore di servizi». Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 150.

specifico, l'art. 6, par. 3, GDPR rimette l'individuazione della base giuridica su cui si fondano i trattamenti necessari per adempiere un obbligo legale [art. 6, par. 1, lett. *c)*] e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri [art. 6, par. 1, lett. *e)*].

Con riguardo a tali condizioni di liceità, nelle more dell'adozione di una normativa interna di adeguamento del Codice privacy al GDPR, il Garante per la protezione dei dati personali era intervenuto per confermare la vigenza, almeno in via temporanea, delle previgenti autorizzazioni generali, adottate in data 15 dicembre 2016[91], facendo tuttavia temere, per certi versi, che il potere integrativo lasciato agli Stati membri potesse, in tal modo, finire per essere usato per reintrodurre alcuni dei meccanismi formali e procedimentali configurarti sotto la vigenza delle norme domestiche, tra cui – appunto – l'autorizzazione al trattamento dei dati sensibili, che il Regolamento puntava invece ad eliminare[92].

Successivamente, il citato d.lgs. 101/2018 ha aggiunto al c. *privacy* l'art. 2-*ter*, con previsione della necessità che il trattamento necessario per l'esecuzione di un interesse pubblico sia fondato sulla previsione di una norma di legge o, nei casi previsti dalla legge, di un regolamento.

Parallelamente, l'art. 21 del predetto decreto legislativo demandava al Garante l'individuazione delle prescrizioni compatibili con la nuova normativa tra quelle contenute nelle autorizzazioni generali già adottate in relazione alle situazioni di trattamento di cui all'art. 6, par. 1, lett. *c)* ed *e)*, e di cui all'art. 9, par. 2, lett. *b)*, e par. 4[93].

Rispetto alla previgente normativa domestica, rappresenta una novità del Regolamento l'abbandono di un criterio formale ed automatico legato alla natura soggettiva pubblica (non economica) del soggetto titolare del trattamento, dalla quale discendeva una diversa disciplina applicabile rispetto ai soggetti privati.

Coerentemente, il citato art. 2-*ter* del c. *privacy* non specifica alcunché in merito alla natura pubblica del soggetto, richiamando solo la necessità di una previsione normativa esplicita di rango primario o secondario[94].

---

[91] GPDP, Provv. n. 424 del 19 luglio 2018, doc. *web*. n. 9026901, *Provvedimento in tema di Autorizzazioni generali del Garante per la protezione dei dati personali*, documento disponibile su Internet all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9026901 (consultato da ultimo in data 03 aprile 2021).

[92] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 121.

[93] Ciò è avvenuto con il provvedimento n. 497 del 13 dicembre 2018, con cui il Garante ha confermato la compatibilità delle seguenti autorizzazioni generali: (i) aut. gen. n. 1/2016 (*Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro*); (ii) aut. gen. n. 3/2016 (*Prescrizioni relative al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose*); (iii) aut. gen. n. 6/2016 (*Prescrizioni relative al trattamento di categorie particolari di dati da parte degli investigatori privati*); (iv) aut. gen. n. 8/2016 (*Prescrizioni relative al trattamento dei dati genetici*); (v) aut. gen. n. 9/2016 (*Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica*).

[94] L'art. 2-*sexies* del c. *privacy* contiene poi l'elenco delle materie nelle quali il trattamento si ritiene necessario per motivi di interesse pubblico «rilevante» e, dunque, basato su un fondamento legittimo anche quando abbia ad oggetto categorie particolari di dati personali; v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 124.

Con riferimento alla necessità di adempiere un obbligo legale, *ex* art. 6, par. 1, lett. *c)*, GDPR, si è posto, in seguito all'abrogazione dell'art. 24 del c. *privacy*, che espressamente equiparava a tali fini la legge, il regolamento e la normativa comunitaria, il problema dell'idoneità della normativa di secondo grado, generalmente risolto in senso affermativo, a condizione che l'atto regolamentare sia esecutivo, attuativo o integrativo di una norma primaria[95].

A proposito della condizione di liceità in esame, il *considerando* n. 45 precisa che è richiesto un atto normativo specifico per ogni singolo trattamento.

Per quanto riguarda, poi, i trattamenti necessari per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, *ex* art. 6, par. 1, lett. *d)*, GDPR, si è già evidenziato come essa rappresenti l'unica condizione di liceità configurata dal legislatore eurounitario come deroga alla loro generale equipollenza. Infatti, come anticipato, secondo il *considerando* n. 46, il trattamento dei dati fondato sulla necessità di salvaguardia di interessi vitali dell'interessato o di terzi dovrebbe avere luogo in linea di principio in via residuale, ossia «unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica».

Lo stesso *considerando* n. 46 evidenzia che alcuni trattamenti sono tali da poter essere fondati contemporaneamente su un interesse pubblico e sull'esigenza di salvaguardia dell'interesse vitale del soggetto cui i dati si riferiscono o di un terzo, come, ad esempio, i trattamenti necessari «per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in caso di emergenze umanitarie, in particolare in caso di catastrofi di origine naturale e umana».

Sempre riguardo alla salvaguardia degli interessi vitali dell'interessato o di un terzo, è doveroso ricordare che analoga previsione è contenuta nell'art. 9, par. 2, lett. *c)*, GDPR per il trattamento di dati appartenenti a categorie particolari, con l'annotazione, tuttavia, della diversa formulazione di tale ultima disposizione, stante il richiamo ulteriore ai casi in cui l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso[96].

Con riferimento, infine, alla condizione di liceità relativa al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento [art. 6, par. 1, lett. *e)*, GDPR], si coglie in maniera spiccata la nuova prospettiva del GDPR, esaminata in apertura di paragrafo, nella quale si affianca al carattere assoluto del diritto alla protezione dei dati (riconosciuto a chiunque e vantabile nei confronti di tutti) un carattere relativo, in quanto condizionato da vincoli esterni, compresa la «funzione sociale» a cui fa riferimento il citato *considerando* n. 4[97].

---

[95] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 183.

[96] Sull'argomento si rimanda a A. Cataleta, *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 204-228.

[97] Cfr. G. Mulazzani, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 198. Sulla «funzione sociale» di cui al cit. *considerando* n. 4 v., *amplius*, il contributo di A. Ricci,

Oltre a quanto già evidenziato con riferimento alla necessità di una norma di legge o, nei casi previsti da quest'ultima, di regolamento per l'individuazione della base giuridica, ai sensi dell'art. 2-*ter* del novellato c. *privacy*, si ritiene doveroso ricordare, seppure sinteticamente, che il co. 2 del medesimo articolo introduce alcune specifiche condizioni di legittimità ai fini della comunicazione o diffusione dei dati personali da parte di soggetti che svolgono i compiti di interesse pubblico o connessi all'esercizio di pubblici poteri[98].

2.4.1. *In particolare, il trattamento effettuato dalla pubblica amministrazione*

Come accennato poc'anzi, merita di essere ribadita la novità rispetto alla previgente l. 675/1996 ed al previgente testo del d.lgs. 196/2003 ante-riforma del 2018, nei quali la natura soggettiva del titolare del trattamento, pubblica o privata, tracciava una linea di demarcazione quanto a disciplina applicabile[99].

Infatti, nell'impianto normativo *ante* riforma del 2018, il trattamento dei dati comuni poteva avvenire, da parte di soggetti pubblici (non economici), anche senza il consenso dell'interessato, purché nei limiti delle finalità istituzionali dell'ente, previsti dalla norma istitutiva, mentre il trattamento dei dati sensibili poteva avvenire solo se previsto da una specifica norma di legge, anche in questo caso senza necessità del consenso dell'interessato né di specifica autorizzazione del Garante, salvo quanto previsto per il esercenti le professioni sanitarie e gli organismi sanitari pubblici[100].

Assoluta centralità rivestiva, pertanto, l'individuazione delle finalità istituzionali connesse alle funzioni svolte dagli enti[101].

2.4.2. *In particolare, i trattamenti nel contesto dell'epidemia*

Il mondo ha fronteggiato con difficoltà l'epidemia da SARS-CoV-2 (Covid-19) che, a partire dai primi mesi del 2020, ha travolto le vite delle persone e, per quanto qui di interesse, ha messo a dura prova molti istituti giuridici tradizionali, compresi quelli in materia di protezione dei dati personali.

Sulla «funzione sociale» del diritto alla protezione dei dati personali, in *Contratto e impresa*, 2017, 2, pp. 586 ss.

[98] Per i quali si rimanda diffusamente a G. MULAZZANI, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, cit., p. 203.

[99] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 128.

[100] Circostanza che, considerata insieme all'ampiezza delle eccezioni al consenso operanti per i titolari aventi natura privata, aveva indotto la dottrina a sottolineare come la portata del consenso risultasse già ridimensionata anche prima della riforma del 2018; v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 128. In particolare, sull'eccezione concernente i dati relativi allo svolgimento di attività economiche *ex* art. 24, co. 1, lett. *d)* del c. *privacy* (ora abrogato), v. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., pp. 999 ss.

[101] Per un'analisi più approfondita si rimanda a G. MULAZZANI, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, cit., p. 201.

Un problema comunemente avvertito, fonte anche di tensioni sociali, è derivato dalla difficoltà di definire il limite fino al quale fosse ritenuto accettabile derogare, nel nome di esigenze certamente condivisibili di contenimento dell'emergenza sanitaria e di salvaguardia di vite umane, alle norme ordinarie poste a tutela di altri diritti e libertà fondamentali, tanto più per quelle che non si presentavano già sufficientemente elastiche per far fronte a situazioni eccezionali.

Senza pretesa di completezza, la presente occasione di indagine consente comunque una riflessione per verificare la tenuta dell'impianto normativo alla prova dei fatti, come si vedrà più in dettaglio nel par. 3, ove verrà approfondita la tematica specifica del tracciamento dei contatti.

Nell'ordinamento italiano, almeno in una fase iniziale, si è assistito alla tendenza, non del tutto condivisibile, all'uso di fonti normative secondarie (come le ordinanze del Ministero della salute o del Dipartimento della protezione civile) per precostituire un'autonoma base giuridica per il trattamento legittimo dei dati particolari e per prevedere modalità affievolite di tutela, nel diritto dell'emergenza, con la conseguenza di «apportare limitazioni anche profonde a libertà fondamentali in nome del supremo interesse della tutela della salute»[102].

La tendenza iniziale è stata poi quantomeno contenuta tramite il ricorso allo strumento del decreto-legge, che ha permesso così di elevare la fonte, mantenendo fermo il carattere dichiaratamente temporaneo delle norme emergenziali.

L'introduzione di limitazioni alla portata degli obblighi e dei diritti previsti dagli artt. da 12 a 22 GDPR, nonché dei principi contemplati nell'art. 5, era già opportunamente concessa dal Regolamento, il cui art. 23 condiziona tale possibilità al rispetto dell'essenza dei diritti e delle libertà fondamentali e prescrive che «sia una misura necessaria e proporzionata in una società democratica per salvaguardare (...) importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse di (...) sanità pubblica e sicurezza sociale».

Il citato *considerando* n. 46, poi, prevede espressamente, come si è visto, che tra i trattamenti legittimi sia per motivi di interesse pubblico che per la salvaguardia degli interessi vitali dell'interessato rientrino in particolare quelli «a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione».

In conclusione di questo breve *excursus*, si ritiene importante ricordare la rapida presa di posizione dell'*European Data Protection Board* (EDPB), secondo cui le misure adottate dai governi per aumentare la rapidità e l'efficacia delle strategie di contrasto all'epidemia dovevano ritenersi in linea di principio legittime, in quanto preordinate alla tutela di un interesse pubblico rilevante, a condizione che rispettassero i canoni della proporzionalità e della temporaneità, rilevando altresì che le esigenze di contrasto all'epidemia e tutela della salute pubblica rilevassero di per sé quali possibili basi giuridiche del trattamento alternative al consenso dell'inte-

[102] Per una approfondita analisi dei provvedimenti succedutisi nel tempo si rimanda a G. Resta, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, in *giustiziacivile.com,* editoriale del 5 maggio 2020.

ressato, sia in relazione ai dati comuni [art. 6, par. 1, lett. *d)-e)*, GDPR] che ai dati particolari [art. 9, par. 2, lett. *c)-g)-h)-i)*, GDPR][103].

2.5. Condizioni di liceità rimesse alla valutazione del titolare: il legittimo interesse del titolare o di un terzo

Come si è visto nel primo paragrafo, l'art. 6, par. 1, lett. *f)*, GDPR, contempla la liceità dei trattamenti necessari per perseguire un interesse legittimo del titolare del trattamento o di un terzo, «a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

Lo stesso art. 6, par. 1 precisa che tale condizione di liceità è inapplicabile ai trattamenti effettuati da autorità pubbliche, nell'esecuzione dei loro compiti.

L'aspetto più rilevante del nuovo impianto normativo è indubbiamente rappresentato dalla rimessione della valutazione al solo titolare del trattamento, senza alcun preventivo coinvolgimento dell'autorità di controllo[104], espressione evidente del principio di *accountability*[105], salvo ovviamente «l'eventuale successivo intervento dell'interessato e/o del Garante, chiamati ad effettuare un vaglio solo a trattamento già avviato»[106].

Un parziale ritorno al passato, a dire il vero, si era temporaneamente verificato, per quanto riguarda la normativa italiana, per effetto della legge per il bilancio del 2018[107], poi modificata in parte *qua* dal d.lgs. 108/2018[108], che richiedeva la trasmissione al Garante di una «informativa» per comunicare preventivamente l'intenzione di avvalersi del legittimo interesse con riferimento a trattamenti connotati dal ricorso ad una nuova tecnologia o strumenti automatizzati.

Il GDPR, ai *considerando* da n. 47 a n. 50, fornisce al titolare diversi criteri guida nell'operazione di bilanciamento degli interessi, prevedendo che debbano essere considerate le ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare[109] ed enucleando una serie di finalità espressamente idonee ad

---

[103] EDPB, *Statement on the processing of personal data in the context of the COVID-19 outbreak*, del 19 marzo 2020, reperibile all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (consultato da ultimo in data 25 gennaio 2022).

[104] Come invece prevedeva l'art. 24, co. 1, lett. *g)*, del c. *privacy*, abrogato dal d.lgs. 101/2018.

[105] Particolarmente esplicativo, a questo proposito, risulta il provvedimento del 22 febbraio 2018 del Garante, ove si afferma che il titolare deve verificare se non sia più appropriato applicare, nel caso concreto, una diversa condizione di liceità del trattamento; GPDP, Provv. n.121 del 22 febbraio 2018, doc. *web* n. 8080493, reperibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8080493 (consultato da ultimo in data 02 aprile 2023).

[106] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 185.

[107] Art. 1, co. 1020-1025, della l. 27 dicembre 2017, n. 205.

[108] Il cui art. 22, co. 5, ha limitato l'applicazione di tali disposizioni esclusivamente ai trattamenti dei dati personali funzionali all'autorizzazione del cambiamento del nome o del cognome dei minorenni.

[109] Come avviene, ad esempio, nel caso in cui vi sia una «relazione pertinente e appropriata» tra interessato e titolare del trattamento, ad es. quando l'interessato è cliente o dipendente del titolare del trattamento. Sotto questo profilo, si è sostenuto che possano così legittimarsi «trattamenti di dati

essere fondate sul legittimo interesse, tra le quali spicca, indubbiamente, il *marketing* diretto, ossia nei confronti dei clienti[110].

Altre fonti cui fare riferimento nell'individuazione delle ipotesi di legittimo interesse sono la relazione al d.lgs. 101/2018[111], i casi precedentemente individuati dal Garante[112] ed infine l'elenco contenuto nell'Opinion 6/2014[113] del Gruppo di lavoro *ex* art. 29[114].

In ulteriore supporto dell'attività di valutazione del titolare può farsi riferimento alla descrizione analitica fornita dal citato Parere 6/2014 del Gruppo di lavoro *ex* art. 29 del «test di comparazione», così articolato: (a) la valutazione dell'interesse legittimo del titolare del trattamento, eventualmente corredata dalla valutazione di impatto *ex* art. 35, GDPR, (b) l'impatto sugli interessati, (c) il bilanciamento provvisorio e (d) le garanzie supplementari applicate dal titolare del trattamento per evitare qualsiasi indebita conseguenza sugli interessati[115].

Sempre riguardo al legittimo interesse, infine, si è sostenuto, richiamando le definizioni contenute nell'art. 4, par. 1, n. 10, GDPR, che il terzo, portatore dell'interesse rilevante oltre al titolare del trattamento, non possa essere l'interessato stesso[116].

---

ulteriori nel corso del contratto (come il nuovo indirizzo di un cliente) o trattamenti post-contrattuali, quali la comunicazione di dati a terzi per recupero del credito, il monitoraggio di un *account social* per verificare il rispetto della clausola di non concorrenza sottoscritta da un *ex* dipendente o per soddisfare esigenze di sicurezza aziendale, fatto sempre salvo il test comparativo». Così D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, cit., pp. 2783 ss.

[110] Altre ipotesi sono: (i) il trattamento dei dati strettamente necessario alla prevenzione delle frodi; (ii) la trasmissione all'interno del gruppo imprenditoriale, a fini amministrativi interni; (iii) l'analisi del traffico dei dati all'interno di una rete o di un sistema informatico, al fine di garantire la sicurezza delle reti e dell'informazione; (iv) esigenze di sicurezza, anche qualora il trattamento implichi la trasmissione dei dati alle autorità competenti alla repressione dei reati.

[111] Che indica come sorretto da legittimo interesse il trattamento di dati relativi all'esercizio del diritto di difesa o a quelli risultanti da registri pubblici.

[112] Il Garante ha individuato il legittimo interesse del titolare quale valido fondamento di liceità del trattamento nel caso della videosorveglianza da parte di soggetti privati (GPDP, Provv. 8 aprile 2010, doc. *web* n. 1712680), dell'utilizzo di sistemi antifrode (GPDP, Provv. n. 14 del 19 gennaio 2017, doc. *web* n. 6068256) e dei sistemi di localizzazione geografica su flotte aziendali (GPDP, Provv. n. 370 del 4 ottobre 2011, doc. *web* n. 1850581).

[113] L'elenco contenuto in Gruppo di lavoro *ex* art. 29, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'art. 7 della direttiva 95/46/CE, del 9 aprile 2014 annovera: l'esercizio del diritto alla libertà di espressione e d'informazione, anche nei mezzi di comunicazione e di espressione artistica, la commercializzazione diretta tradizionale e altre forme di commercializzazione o pubblicità, i messaggi indesiderati non commerciali, anche a fini di campagne politiche o di raccolta fondi per scopi benefici, l'esercizio di un diritto in via giudiziale, compreso il recupero del credito tramite procedure extragiudiziali, la prevenzione di frodi, uso improprio dei servizi o riciclaggio di denaro, il controllo del personale a fini di sicurezza o gestione, le procedure per la denuncia delle irregolarità, la sicurezza fisica, sicurezza informatica e sicurezza della rete, il trattamento di dati a scopi statistici o di ricerca storica o scientifica, il trattamento a scopi di ricerca (compresa la ricerca a fini commerciali).

[114] Cfr. D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, cit., pp. 2783 ss.

[115] Si v. diffusamente la disamina compiuta da D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, cit., pp. 2783 ss.

[116] *Ibidem*.

2.5.1. *In particolare, il* marketing *diretto e i* cookies

In chiusura del presente paragrafo, sia consentita una riflessione sul crescente ricorso all'istituto del legittimo interesse, parallelamente e in alternativa al consenso, per quanto riguarda il tracciamento *on-line* mediante *cookies*. L'argomento è ampio e richiederebbe l'analisi anche della c.d. direttiva e-*Privacy* 2002/58/CE e dell'art. 122 del c. *privacy*, che esulano dal presente lavoro, ma pare comunque importante sottolineare come non risulti affatto convincente l'interpretazione, diffusa nella prassi, volta ad estendere acriticamente ai *cookies* la condizione di liceità del legittimo interesse, quale ipotesi di *marketing* diretto, che – come visto – è espressamente ritenuto sussumibile sotto tale condizione di liceità proprio dal *considerando* n. 47[117]. In materia è intervenuto il Garante con l'emanazione delle «*Linee guida cookie e altri strumenti di tracciamento*» del 10 giugno 2021[118], ove ha ribadito la necessità del consenso preventivo per il trattamento dei dati personali che si avvalga di *cookies* per il tracciamento *online* dell'interessato, con eccezione per i soli *cookies* tecnici, in ordine ai quali il consenso non è richiesto, fermo restando in ogni caso l'obbligo di adeguata informativa.

3. Applicazione del principio nella casistica

3.1. Il principio di liceità nella casistica nazionale

3.1.1. *La liceità del consenso nella commercializzazione di dati personali e nelle pratiche di* marketing*. Il caso «Ad Spray» innanzi al Garante per la protezione dei dati personali e alla Corte di Cassazione*

Tra i principali provvedimenti del Garante in materia di liceità del trattamento, merita di essere approfondita, in tema di *marketing*[119], la pronuncia relativa, in particolare, alla liceità delle operazioni di *tying*, intendendo con tale termine quelle pratiche commerciali con cui, in occasione della vendita di un bene o servizio, si propone anche l'acquisto di un bene o servizio secondario, connesso al principale, qui rilevante con riguardo all'ipotesi contemplata all'art. 7, par. 4, GDPR, ove si disciplina il caso in cui si subordina la fornitura del servizio alla prestazione del consenso al trattamento dei dati personali non necessario per l'erogazione del servizio medesimo.

---

[117] Si v., inoltre, EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, cit.

[118] GPDP, Provv. n. 231 del 10 giugno 2021, doc. *web* n. 9677876, Linee guida cookie e altri strumenti di tracciamento, documento disponibile su Internet all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876 (consultato da ultimo in data 11 ottobre 2022).

[119] GPDP, Provv. 15 gennaio 2020, doc. *web* n. 9256486, in cui il Collegio ribadisce che ogni altra finalità di trattamento (es. profilazione, *marketing*, ecc.) necessita del consenso libero, specifico, informato per ciascuna di esse *ex* art. 6 par. 1 lett. *a)*, GDPR.

Il Garante, interpretando in senso restrittivo la norma poc'anzi citata, ha affermato che in tali operazioni di *tying*, la captazione del consenso al trattamento dei dati personali insieme a quello espresso per l'adesione al servizio principale, richiesto dall'utente/interessato, costituisce una coazione della volontà del medesimo, con violazione dei principi di correttezza e della libera manifestazione del consenso.

Si veda, a tal riguardo, il provvedimento inibitorio e prescrittivo reso dal Garante nei confronti della società Ad Spray[120]. Nel caso di specie, la società forniva un servizio di *newsletter* su temi giuridici, di finanza e fisco, richiedendo agli utenti di apporre un *flag* prestando il consenso al trattamento dei dati personali per la fruizione del servizio offerto, che implicava l'uso dell'indirizzo *e-mail* del destinatario del servizio anche per l'invio di comunicazioni commerciali[121].

Il Garante, in tale occasione, ha dichiarato illecito il trattamento dei dati effettuato dalla società titolare del trattamento in merito alla pratica di *tying*, in quanto il consenso richiesto (non necessario per l'invio di comunicazioni pubblicitarie) non rispetterebbe i requisiti posti prima dall'art. 23 del c. *privacy* e, successivamente, dall'art. 7, par. 4 del GDPR. L'Autorità ha ritenuto, nello specifico, che non potesse definirsi libero il consenso a ulteriori trattamenti di dati personali che all'interessato viene chiesto di prestare quale condizione necessaria per conseguire una prestazione richiesta o per fruire di un determinato servizio. La decisione veniva adottata conformandosi al contenuto delle Linee guida in materia di attività promozionale e contrasto allo *spam* del 4 luglio 2013[122]. Il Garante muoveva anche altri rilievi, incluso quello concernente l'assenza di specificità e di adeguata granularità del consenso, che rendeva ugualmente illecito, ma sotto altro profilo, il trattamento dei dati personali effettuato dalla società Ad Spray per finalità di *marketing*. La disciplina in esame richiede infatti che il consenso al trattamento, ove richiesto, debba essere riferito a un trattamento chiaramente e non solo genericamente individuato ed accordato in relazione a finalità specificamente indicate: tali elementi non sono stati rilevati dal Garante nella fattispecie sottoposta alla sua attenzione, concludendo per l'illeceità del trattamento, per via del consenso non libero né specifico, né prestato separatamente per ciascuna delle multiple finalità del trattamento e, dunque, nullo[123].

La società titolare del trattamento decise di impugnare il provvedimento del Garante innanzi all'autorità giudiziaria.

Nel 2016 il giudice di merito[124] aveva accolto l'opposizione di Ad Spray al provvedimento del Garante, incentrando la pronuncia sull'interpretazione del requi-

[120] GPDP, Provv. n. 427 del 24 settembre 2014, doc. *web* n. 3457687, Provvedimento inibitorio e prescrittivo nei confronti di AdSpray S.r.l.

[121] Per un'analisi di tale caso, sottoposto inizialmente all'attenzione del Garante e successivamente alla Corte di Cassazione, si rinvia, *amplius*, a F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, cit., pp. 34-58.

[122] GPDP, Provv. n. 330 del 4 luglio 2013, doc. *web* n. 2542348.

[123] F. Bravo, *op. ult. cit*., nota 3. In tal senso si era espresso anche il Gruppo di lavoro ex art. 29, *Opinion 15/2011 on the definition of consent* del 13 luglio 2017 e *Opinion 03/2013 on purpose limitation* del 2 aprile 2013, impostazioni confermate nel Regolamento all'art. 6, par. 1, lett. *a)*, nel quale si prescrive che il consenso debba essere «espresso per una o più specifiche finalità».

[124] Trib. Arezzo, sent. 29 aprile 2016.

sito della libertà del consenso in relazione all'autonomia delle parti ed affermando, contrariamente alla posizione assunta dall'Autorità di vigilanza, la liceità dei contratti con cui si prevede, a fronte dell'erogazione del servizio, una controprestazione costituita dal conferimento dei dati personali del cliente, in quanto espressione del principio di autonomia contrattuale[125]. Veniva dunque affermata la liceità dei contratti basati sul *business model* con cui si subordina l'accesso ad un servizio, erogato senza richiesta di corrispettivo in denaro, al consenso al trattamento dei dati personali del cliente, utilizzati per ottenere remunerativitá in altro modo, ad esempio nell'ambito di campagne di *marketing* contrattualizzate con soggetti terzi[126].

L'Autorità Garante proponeva tuttavia ricorso per Cassazione, chiedendo, a conferma della propria interpretazione ed in riforma della sentenza resa dal giudice di merito, che il trattamento dei dati personali fosse dichiarato contrario al principio di liceità per nullità del consenso al trattamento, non potendosi considerare libera la manifestazione della volontà qualora condizionata all'erogazione del servizio e concernente dati personali non necessari all'erogazione del servizio stesso.

Si noti che, in seguito all'entrata in vigore del GDPR, l'art. 23 del c. *privacy*, sulla cui interpretazione si basava l'orientamento del Garante, risulta ora sostituito dalle corrispondenti norme del Regolamento, che all'art. 4, par. 1, n. 11, definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato» e all'art. 7, par. 4, specifica che «nel valutare se il consenso sia stato liberamente prestato si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario alla esecuzione di tale contratto».

La Corte di Cassazione, pronunciatasi sulla questione con sentenza del 2 luglio 2018, n. 17278, pur basando la propria decisione sull'interpretazione dell'art. 23 c. *privacy*, ha avuto modo di tener conto anche dei nuovi riferimenti normativi, chiarendo innanzitutto la differenza strutturale tra consenso al trattamento dei dati personali e consenso contrattuale. Mentre per il consenso contrattuale rilevano, quali vizi della volontà, il dolo, la violenza morale e l'errore, secondo la rigida e tassativa previsione codicistica, a cui si ricollega il rimedio dell'annullabilità (e non della nullità) del contratto, che deve essere pronunciata con sentenza su richiesta della parte legittimata, per il consenso al trattamento dei dati personali la disciplina è profondamente diversa, risultando viziato ogni qual volta tale consenso non sia libero, specifico, informato e inequivocabile, con conseguente previsione del rimedio della nullità, che travolge *de iure* l'intero trattamento, comportandone l'automatica illiceità[127].

Quanto al requisito della libertà del consenso al trattamento dei dati personali, nei casi in cui si subordini ad esso l'erogazione del servizio all'interessato, la Corte di Cassazione, seppure con una pronuncia di accoglimento del ricorso del Garante, ha smentito l'automatica applicazione del divieto ipotizzato ed ha affermato, inve-

[125] F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, cit., pp. 34-58.
[126] *Ibidem.*
[127] *Ibidem.*

ce, in linea generale, la liceità dei contratti c.d. «di scambio di dati», ove si correli la prestazione del servizio al consenso al trattamento, per finalità commerciali, dei dati dell'interessato non necessari all'erogazione del servizio medesimo, al fine di ottenere in altro modo la remuneratività, purché il servizio non sia da considerare infungibile e la revoca del consenso non comporti un gravoso pregiudizio per l'interessato: in presenza di tali elementi, infatti, il consenso al trattamento non potrebbe considerarsi libero e il trattamento sarebbe da considerarsi illecito[128].

Segnatamente, la Cassazione ha affermato, nella richiamata sentenza, che «con riguardo all'aspetto della libertà, occorre esaminare, in relazione al caso in esame, la questione se il condizionamento di cui si è detto, tale da far sì che il consenso non sia conforme al dettato normativo, possa essere ravvisato nell'ipotesi in cui l'offerta di un determinato servizio da parte del gestore di un sito Internet sia – per l'appunto – condizionato al rilascio del consenso all'utilizzo dei dati personali per il successivo invio, da parte di terzi, di messaggi pubblicitari: quesito al quale si riferisce, oggi, il comma 4 dell'articolo 7 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (…). Ritiene la Corte, nel quadro di applicazione del citato articolo 23, che la risposta al quesito non possa essere univoca e, cioè, che il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso, giacché all'evidenza si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio»[129].

Sulla scorta di tali considerazioni, la Cassazione ha precisato, dunque, che «Non può allora essere condiviso l'argomento svolto dal giudice di merito secondo cui, dando credito alla tesi sostenuta dal Garante, si finirebbe per "delineare una sorta di obbligo *tout court*, per il gestore del portale, di offrire comunque le proprie prestazioni, a prescindere dalla prestazione del consenso al trattamento dei dati personali da parte dell'utente": e, in buona sostanza, per obbligare così il gestore del portale a rinunciare al tornaconto economico dell'operazione che egli compie, proveniente dall'attività pubblicitaria realizzata tramite l'impiego dei dati personali acquisiti. Nulla, infatti, impedisce al gestore del sito – beninteso, si ripete, in un caso come quello in questione, concernente un servizio né infungibile, né irrinunciabile –, di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali, mentre ciò che gli è interdetto è utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia effettivamente manifestato la volontà di riceverli. Insomma, l'ordinamento non vieta lo scambio di dati personali, me esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato»[130].

[128] *Ibidem.*
[129] Cass., sez. I, 2 luglio 2018, n. 17278.
[130] Cass., sez. I, 2 luglio 2018, n. 17278.

Spostando l'attenzione dal diritto dei contratti al diritto al trattamento dei dati personali, dunque, l'art. 7, par. 4 del GDPR non afferma il divieto di subordinare all'erogazione di un servizio richiesto dall'interessato il consenso al trattamento di dati personali non necessari all'erogazione del servizio, ma richiede che si tenga in massima considerazione tale circostanza, al fine di valutare se, nella fattispecie, il consenso al trattamento possa considerarsi libero o coartato: l'orientamento della Cassazione nel caso Ad Spray è quello di considerare libero il consenso – e dunque, sotto tale profilo, lecitamente prestato – se il servizio è fungibile e rinunciabile (e, dunque, se possa essere esercitata la revoca del consenso da parte dell'interessato senza subire un gravoso pregiudizio).

La Corte di Cassazione ha assunto un orientamento meno restrittivo di quello dell'Autorità Garante, valutando la libertà del consenso prestato rispetto alla fungibilità sul mercato del servizio offerto.

Proprio sui caratteri di fungibilità o infungibilità del servizio e del non gravoso sacrificio, la Cassazione, nel caso Ad Spray, ha ritenuto di considerare liberamente prestato il consenso dell'interessato e, dunque, di non censurare la liceità del trattamento sotto tale specifico rilievo. La Corte, tuttavia, come detto, è giunta comunque all'accoglimento del ricorso del Garante sulla base della ritenuta mancanza di un consenso adeguatamente informato e specifico dell'interessato.

La Cassazione, infatti, ha affermato, sotto il profilo della manifestazione del consenso, che lo stesso non può intendersi valido qualora nelle vicinanze della casella da spuntare per prestarlo non siano indicati anche quali siano i trattamenti effettivamente autorizzati, oppure – come nel caso in esame – se, in presenza di un *link* che riporti ad un'altra pagina contenente tale informazione, non sia contestualmente possibile accertare che l'interessato abbia effettivamente consultato e preso visione di tale ulteriore pagina e, in ogni caso, che non può considerarsi «specifico» un consenso prestato per «non meglio identificati messaggi pubblicitari», essendo necessario almeno indicare i settori merceologici o i servizi cui i messaggi pubblicitari futuri potevano essere riferiti[131].

Sotto tale diverso profilo, legato al difetto di granularità del consenso, la Corte è così giunta a ravvisare comunque il trattamento oggetto del caso di specie.

3.1.2. *L'illiceità del trattamento avente ad oggetto operazioni di recupero del consenso alle campagne di* marketing*. Il caso «Wind Tre» innanzi al Garante per la protezione dei dati personali e alla Corte di Cassazione*

Il caso della compagnia telefonica Wind Tre risulta affine al caso Ad Spray appena esaminato per il tenore delle conclusioni a cui è giunta la Corte di Cassazione con la recente ordinanza del 28 marzo 2022 n. 9920: qualora, al momento della conclusione del contratto, il consenso alle campagne di *marketing* non sia stato specificamente prestato dall'interessato, allora deve ritenersi che esso sia stato

[131] Anche su tali aspetti si rinvia a F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, cit., pp. 34-58, con particolare riguardo al tema della c.d. «granularità» del consenso.

implicitamente negato, con conseguente illiceità di ogni successiva attività volta a recuperare tale consenso, integrata da comunicazioni automatizzate.

Nel caso di specie la Wind Tre aveva inviato SMS con finalità di *marketing* a clienti di nuova e vecchia acquisizione. Il testo degli SMS per i nuovi acquisiti era del seguente tenore: «grazie per averci scelto. Vorremmo darLe il benvenuto nel mondo delle esclusive promozionali di Wind Tre ma ad oggi non si risulta il suo consenso ai contatti commerciali. Non perda l'occasione o chiami gratuitamente il (…)», seguito dall'indicazione del numero telefonico. Per i clienti già acquisiti, che non avevano prestato il consenso alle pratiche pubblicitarie, il testo recitava invece: «Gentile cliente, la informiamo che ad oggi non ci risulta il suo consenso ai contatti commerciali e promozionali di Wind Tre, rilasci il consenso ai contatti commerciali chiamando gratuitamente il (…)», seguito all'indicazione del numero telefonico.

A seguito di diverse segnalazioni ricevute dagli interessati, che contestavano l'illiceità di tale pratica, il Garante vietava a Wind Tre l'ulteriore trattamento per finalità promozionali dei dati personali dei propri utenti, volto ad acquisire il consenso per finalità di *marketing*, in quanto ritenuto contrastante con il principio di liceità[132].

La società titolare del trattamento impugnava il provvedimento innanzi all'autorità giudiziaria. Il Tribunale adito accoglieva il gravame, specificando che l'art. 130, co. 1, c. *privacy* non potesse ritenersi di ostacolo a pratiche consistenti nell'invio di messaggi volti ad acquisire la manifestazione consapevole da parte degli utenti del consenso ad invio di comunicazioni pubblicitarie[133]. Il Garante, tuttavia, proponeva vittoriosamente ricorso per Cassazione avverso la pronuncia di merito.

La Suprema Corte ha ribadito, così, il principio[134] per cui «una comunicazione telefonica finalizzata a ottenere il consenso per fini di marketing da chi l'abbia precedentemente negato [espressamente o semplicemente non prestandolo al momento della conclusione del contratto, *n.d.a.*], deve considerarsi essa stessa comunicazione commerciale poiché la finalità alla quale è imprescindibilmente collegato il consenso richiesto per il trattamento concorre a qualificare il trattamento stesso»[135]. Sicché anche a tale tipo di comunicazioni va considerato illecito, per difetto del consenso, dato che «l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita

[132] GPDP, Provv. n. 437 del 27 ottobre 2016, doc. *web* n. 5727908. Con tale provvedimento il Collegio assume la violazione dell'art. 2 Cost., dell'art. 8 CEDU, dell'art. 8 della Carta dei diritti fondamentali UE, del Reg. UE n. 679/2016 e dell'art. 130 c. *privacy*. Tale art. 130, com'è noto, disciplina le comunicazioni indesiderate prevedendo che «l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente», richiedendo, dunque, il consenso sia per l'invio di materiale o per la vendita diretta, sia per l'invio di comunicazioni commerciali. Qualora il consenso sia richiesto per attività promozionali da eseguirsi successivamente, si è già in presenza di comunicazioni commerciali «indesiderate». Il co. 2 dell'art. 130 c. *privacy*, specifica, inoltre, che «la disposizione (…) si applica anche alle comunicazioni elettroniche effettuate per finalità ivi indicate, mediante posta elettronica, telefax, messaggi di tipo MMS o SMS o altro tipo».

[133] Trib. Roma, sent. n. 10789/2019.

[134] Già affermato nella citata ordinanza n. 11019 del 26 aprile 2021.

[135] Cass. civ., sez. I, ord. 28 marzo 2022, n. 9920.

diretta per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente»[136].

Alla base, dunque, della pronuncia vi è l'assunto per il quale il consenso debba intendersi quale base giuridica necessaria anche per il semplice invio di generiche comunicazioni pubblicitarie e commerciali, a cui sono assimilate quelle volte al successivo recupero del consenso, non fornito dall'interessato alla società telefonica titolare del trattamento[137].

Parimenti, la Cassazione ha ritenuto rilevante il *considerando* n. 40 della Direttiva *e-privacy*[138], il quale sollecita «misure per tutelare gli abbonati da interferenze nella loro vita privata mediante comunicazioni indesiderate a scopo di commercializzazione diretta, in particolare mediante dispositivi automatici di chiamata (…) SMS» e prevede che «per tali forme di comunicazioni indesiderate a scopo di commercializzazione diretta è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi».

Alla luce delle suddette indicazioni, la mancanza della espressione del consenso deve essere letta quale sua negazione: qualora non prestato, il consenso al trattamento dei dati personali per finalità di *marketing* è da ritenersi negato al momento della conclusione del contratto e, dunque, successive attività volte a fare mutare il diniego costituiscono interferenze illegittime e integrano una violazione del principio di liceità del trattamento[139].

3.1.3. *Ancora sulla liceità del consenso al trattamento dei dati personali quale controprestazione della fornitura di servizi erogati senza richiesta di compenso. Il caso «Facebook» innanzi all'AGCM e al giudice amministrativo (TAR e Consiglio di Stato)*

Altre problematiche, già ripercorse nel caso Ad Spray, possono rinvenirsi, *mutatis mutandis*, in relazione all'uso dei *social network* i cui utenti, spesso, ignorano il reale valore, anche economico, dei dati e delle informazioni condivise a fronte della fruizione apparentemente gratuita del servizio, sottovalutando le conseguenze che potrebbero derivare dalla sovraesposizione dei propri dati personali sulle piattaforme *social*.

---

[136] *Ibidem*.

[137] La norma, inoltre, vieta l'invio di comunicazioni commerciali e promozionali effettuate camuffando l'identità del mittente o in violazione dell'art. 8 d.lgs. 9 aprile 2003, n. 70 o senza fornire contatti presso cui l'interessato possa far valere i diritti riconosciuti *ex* artt. 15-22 del GDPR.

[138] Direttiva 2002/58/CE, volta a evitare l'utilizzo celato di azioni rivolte ad attività di *marketing* nonostante la mancanza del consenso espresso specificatamente e anteriormente all'esecuzione dell'attività stessa.

[139] La *ratio* del provvedimento della Suprema Corte è da ravvisarsi nella protezione degli abbonati dalle interferenze nella loro vita privata, vietando al titolare del trattamento di porre in essere e poter lecitamente richiedere, in un secondo momento dalla conclusione del contratto, un successivo consenso a pratiche di marketing che possano ritenersi invece già rifiutate al momento medesimo della conclusione del contratto.

Risulta interessante citare, a tal riguardo, la vicenda relativa alla cessione dei dati personali degli utenti a fronte dell'utilizzo della piattaforma social *Facebook*[140].

Nonostante la vertenza fosse finita sotto la lente dell'Autorità Garante della Concorrenza e del Mercato (AGCM)[141] per gli aspetti relativi alle pratiche commerciali ingannevoli[142], dal caso emergono spunti interessanti anche in tema di protezione dei dati personali, in quanto le contestazioni mosse al *provider*, confermate anche dalle successive pronunce del giudice amministrativo[143], erano attinenti all'aspetto della disinformazione dell'utente, che è sia «consumatore» sia «interessato» al trattamento, circa l'uso dei dati personali da questi conferiti alla società fornitrice del servizio, che li sfrutta a fini commerciali senza che l'utente venga adeguatamente messo al corrente di ciò ed essendo, al contrario, indotto a credere nella gratuità del servizio con cui gli viene messo a disposizione l'uso della piattaforma di *social network*, senza potersi accorgere, in tutta la sua effettiva portata, della profilazione ad uso commerciale che ne consegue.

Tale condotta, secondo l'AGCM, configura gli estremi di una pratica commerciale ingannevole laddove «Facebook non informa l'utente con chiarezza e immediatezza in merito alla raccolta e all'utilizzo, a fini remunerativi, dei dati dell'utente da parte del Professionista e, conseguentemente, dell'intento commerciale perseguito, volto alla monetizzazione dei medesimi»[144].

---

[140] Cfr., al riguardo, F. Bravo, *La «compravendita» di dati personali?*, in *Diritto di Internet*, 2020, 3, pp. 521-540.

[141] AGCM, Provv. n. 27432 adottato in data 29 novembre 2018, disponibile all'indirizzo Internet http://www.agcm.it/dotcmsCustom/tc/2023/12/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/5A1EFA963A109B64C125835F00542FE2/%24File/p27432.pdf (da ultimo consultato in data 15 aprile 2021).

[142] L'Autorità ha interpretato come rientrante all'interno della disciplina consumeristica l'ipotesi in cui, in seguito alla profilazione degli utenti, il fornitore della piattaforma utilizzi i dati raccolti anche per finalità commerciali.

[143] Cfr. T.A.R. Lazio, sede di Roma, sez. I, sent. 10 gennaio 2020 n. 260 e n. 261 e Cons. Stato, sez. VI, sent. 29 marzo 2021, n. 2631.

[144] Nel provv. cit. l'AGCM chiarisce, altresì, che «Le informazioni fornite risultano generiche ed incomplete senza adeguatamente distinguere tra, da un lato, l'utilizzo dei dati funzionale alla personalizzazione del servizio con l'obiettivo di facilitare la socializzazione con altri utenti "consumatori", dall'altro, l'utilizzo dei dati per realizzare campagne pubblicitarie mirate. L'ingannevolezza risulta, peraltro, aggravata dalla circostanza che, nell'uso di FB, le finalità commerciali si prestano ad essere confuse con le finalità sociali e culturali, tipiche di un social network. Nella pagina di registrazione a FB, a fronte del claim "Facebook ti aiuta a connetterti e rimanere in contatto con le persone della tua vita", rileva, dunque, l'assenza di un adeguato *alert* che informi gli utenti, con immediatezza ed efficacia, in merito alla centralità del valore commerciale dei propri dati rispetto al servizio di social network offerto, limitandosi FB a sottolineare come l'iscrizione sia gratuita per sempre. L'incompletezza dell'informazione fornita nella pagina di accesso a Facebook non viene meno neanche per la recente introduzione, da aprile 2018, del "banner cookie" in quanto la sua visualizzazione è solo eventuale e non necessariamente collegata alla registrazione nella Piattaforma FB. Infatti, il banner non compare in fase di creazione dell'account qualora l'utente abbia già "cliccato e navigato" sul sito. Inoltre, esso è, comunque, generico e collocato in posizione non adiacente all'indicazione della gratuità del servizio. Giova, infine, osservare che l'utilizzo di tale banner è imposto dalla normativa sulla Privacy e risponde, quindi, ad esigenze regolate da principi diversi da quelli contenuti nel Codice del Consumo».

Il caso è stato poi esaminato dall'Autorità giudiziaria amministrativa, che ha confermato l'illiceità della condotta del *provider* in relazione alla disciplina in tema di pratiche commerciali scorrette, seppur con riferimento ad una soltanto delle condotte censurate. Si è pronunciato, dapprima, il TAR Lazio, sede di Roma[145], affermando, tra l'altro, che «Il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un "*social network*"»[146].

Tali principi venivano confermati anche dal Consiglio di Stato[147], all'esito di un giudizio instaurato a seguito di distinte impugnazioni proposte sia dal *provider* che dall'AGCM, successivamente riunite nel medesimo procedimento.

Limitatamente a quanto più interessa in questa sede, la richiamata sentenza del Consiglio di Stato ha statuito, in maniera significativa, che «A fronte dunque della promessa gratuità del servizio l'utente era indotto ad accedere per ottenere i vantaggi "immateriali" costituiti dalla adesione e coinvolgimento in un *social network* in seguito all'iscrizione nella piattaforma mettendo a disposizione i propri dati personali, che venivano dunque coinvolti nella profilazione a fini commerciali senza che l'utente fosse stato reso edotto in modo efficace dell'esatta portata di tale utilizzo, che poteva essere interrotto, con revoca del consenso, solo in epoca successiva (difatti, pur potendo successivamente disattivare l'utilizzo dei dati, al momento della iscrizione in piattaforma l'utente non poteva esimersi dal cedere al professionista la mole di dati personali inseriti nel portale all'atto della registrazione e dall'autorizzarlo al loro trattamento) e a fronte di una capillare indicazione degli svantaggi che ne sarebbero conseguiti»[148].

Peraltro, rileva ancora il giudice amministrativo, nella sentenza da ultimo citata, «contrariamente a quanto sostenuto dalle società in sede istruttoria, i dati conferiti

[145] Cfr. T.A.R. Lazio, sede di Roma, sent. n. 260/2020 e n. 261/2020, cit.

[146] Su tali sentenze si veda *amplius*, ancora una volta, F. BRAVO, *La «compravendita» di dati personali?*, cit., pp. 521 ss.

[147] Cfr. Cons. Stato, sent. n. 2631/2021, cit.

[148] *Ibidem*.

permettevano la profilazione dell'utente, arricchendo in questo modo la base dati dei clienti per finalità strettamente commerciali»[149].

Sul piano giuridico si registra un'applicazione concorrente della disciplina in materia di protezione dei dati personali con quella consumeristica.

Pur non emergendo esplicitamente dalle richiamate pronunce dell'AGCM e dell'autorità giudiziaria amministrativa, in quanto vertenti su questioni afferenti ad altro settore dell'ordinamento giuridico, si può ugualmente desumere che i profili di illiceità concernenti la pratica commerciale in questione, censurata sotto il profilo del diritto dei consumi, si riverberino anche sulla liceità del consenso al trattamento dei dati personali di cui all'art. 7 del GDPR, inficiandone la validità proprio con riguardo alla mancata chiara consapevolezza, in capo agli utenti, interessati al trattamento, delle finalità determinate per le quali i dati personali vengono raccolti dal *provider*, titolare del trattamento. L'assenza di granularità del consenso, oltre alle più specifiche verifiche in ordine alla fungibilità del servizio e dell'assenza di un gravoso pregiudizio per l'utente in caso di successiva revoca del consenso al trattamento dei dati, porterebbero a desumere l'illiceità del consenso medesimo, ai sensi degli artt. 6, par. 1, lett. *a)* del GDPR e 9, par. 2, lett. *a)* del GDPR in relazione all'art. 7 del GDPR[150].

3.1.4. *Liceità del trattamento e consenso dei minori nella società digitale. Il caso «Tik Tok» nei diversi provvedimenti del Garante*

Le criticità relative all'utilizzo dei *social network* diventano ancor più delicate quando ad accedere alla rete siano minori, soprattutto, alla luce della perdurante assenza di reali controlli circa la validità del consenso da questi fornito, anche con riguardo alla veridicità dell'età dichiarata dai minori per poter esprimere autonomamente la dichiarazione di autorizzazione al trattamento dei dati, ove la legge lo consenta, e all'effettiva legittimazione dei genitori a fornire il consenso nelle restanti ipotesi[151].

Considerata, quindi, la peculiarità della categoria di interessati, la natura dei dati trattati e i maggiori rischi ad essi connessi, il trattamento di dati personali ascrivibili a tale categoria di interessati è circondato, come visto nei paragrafi che precedono, da una serie di maggiori tutele.

Sotto questo profilo, meritano di essere citati i provvedimenti dell'Autorità Garante in risposta alle preoccupazioni sollevate dalla notevole diffusione della piattaforma Tik Tok tra i giovani ed i giovanissimi[152].

---

[149] *Ibidem*.

[150] Cfr., segnatamente, F. Bravo, *La «compravendita» di dati personali?*, in *Diritto di Internet*, 2020, 3, pp. 538 ss., nella parte dedicata ai cumuli della tutele consumeristica e relativa alla protezione di dati personali.

[151] In materia di consenso dei minori al trattamento dei dati personali si veda F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 164 ss.; nonché G. Bianchedi, *Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico*, cit., pp. 389-413.

[152] G. Bianchedi, *op. cit.*, p. 389. L'A. fa riferimento alla sanzione inflitta dalla US Federal Trade Commission (FTC) al *social network* Musical.ly – Tik Tok a cui ha fatto seguito una indagine della

Il *social* "Tik Tok", infatti, è stato, nei primi mesi del 2021, oggetto di cronaca per la drammatica vicenda, che ha scosso l'opinione pubblica, di una bambina di dieci anni, morta dopo aver tentato di emulare una *challenge* vista sulla piattaforma alla quale era iscritta. Considerata la gravità dell'accaduto, il Garante disponeva, con il Provvedimento datato 22 gennaio 2021[153], il blocco istantaneo del trattamento, ravvisando «i presupposti di necessità ed urgenza previsti dall'art. 66 del Regolamento» e «vietando l'ulteriore trattamento dei dati degli utenti che si trovano sul territorio italiano per i quali non vi sia assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico»[154].

Il *provider* gestore della piattaforma ha, da parte sua, risposto di voler provvedere, a partire dal 9 febbraio 2021, al blocco degli utenti italiani, chiedendo una seconda indicazione della data di nascita prima di poter utilizzare l'*app*, nonché di voler provvedere alla rimozione dell'*account* degli utenti che dovessero risultare al di sotto dei tredici anni di età[155.] Al fine di valutare l'effettività dell'età indicata, il *social network* ha annunciato di volersi servire di strumenti di *age verification* basati su tecnologie di intelligenza artificiale, impegnandosi con l'autorità di controllo irlandese ad attuare le valutazioni in merito al loro utilizzo a tali fini. Inoltre, ha previsto l'aggiunta di un pulsante in *app* che permetta agli utenti di segnalare la presenza di utilizzatori che si sospettino avere una età inferiore ai 13 anni e ad impegnare il doppio del numero dei moderatori parlanti lingua italiana. Ancora, il *provider* si è impegnato a modificare la propria campagna informativa pubblicitaria, prevedendo di inviare notifiche *push* agli utenti prima di bloccarne i profili, oltre alla utilizzazione di *banner* per fornire i *link* a specifiche informazioni sulla sicurezza implementata e alla possibilità di optare per un profilo pubblico o privato. Sia sul *web* sia sulla carta stampata, il *provider* ha inoltre promesso di rivolgersi ai genitori degli utenti, ribadendo il limite di anni 13 per l'utilizzazione della piattaforma *online* e, infine, in

ICO britannica (Information Commissioner's Office). V. *US Federal trade Commission's press release of February 27, 2019* (https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc) e *Information Commissioner's Office*, "*The Information Commissioner's response to the Department for Digital, Culture, media & Sport consultation on the Online Harms White Paper*", 1 July 2019 (https://ico.org.uk/about-the-ico/consultations/department-for-digital-culture-media-sport-consultation-online-harms-white-paper/).

153 GPDP, Provv. n. 20 del 22 gennaio 2021, doc *web* n. 9524194.

154 Il provvedimento veniva reso considerando, in particolare: (i) «l'art. 24, par. 2, della Carta dei diritti fondamentali dell'Unione europea, ai sensi del quale "in tutti gli atti relativi ai minori, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del minore deve essere considerato preminente"»; (ii) «il considerando 38 del Regolamento, in base al quale i minori meritano una specifica protezione relativamente ai loro dati personali in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia, nonché dei loro diritti, soprattutto quando, come nel caso di specie, la raccolta dei dati personali dei minori avviene all'atto dell'utilizzo di servizi forniti direttamente a questi ultimi»; (iii) «l'art. 25, paragrafo 1, del Regolamento, che impone al titolare del trattamento di implementare adeguate misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati al fine di soddisfare i requisiti del Regolamento e per proteggere i diritti degli interessati».

155 GPDP, *Tik Tok si adeguerà alle richieste del Garante privacy. Ma l'Autorità vigilerà sull'effettiva efficacia delle misure che verranno adottate*, comunicato stampa del 3 febbraio 2021, doc. *web* n. 9533424.

riferimento agli utenti, ha rinnovato la promessa di utilizzare un linguaggio accessibile e comprensibile per enucleare i profili del trattamento dei dati raccolti.

Si tratta di provvedimenti e di misure che non paiono esenti da critiche. A tacer d'altro, non si comprende il riferimento al limite d'età di tredici anni, giacché, come si è visto, l'art. 2-*quinquies* del c. *privacy*, così come modificato dal d.lgs. 101/2018, in tema di «*Consenso del minore in relazione ai servizi della società dell'informazione*», determina in 14 anni la soglia per l'autodeterminazione del minore.

Solo successivamente il Garante, nel provvedimento di prescrizione del 25 marzo 2021[156], a seguito di una ulteriore analisi, ha ingiunto alla società che gestisce la piattaforma Tik Tok «l'immediata implementazione di misure idonee di sbarramento all'ingresso della piattaforma volte ad evitare l'accesso ad essa da parte di minori di anni 13 e 14 privi della necessaria manifestazione di volontà resa dal titolare della responsabilità genitoriale, corredate da un chiaro ed inequivoco avviso automaticamente attivabile ad ogni apertura dell'app in questione che ne evidenzi l'utilizzo riservato esclusivamente ai maggiori di anni 13, debitamente autorizzati dagli esercenti la responsabilità genitoriale fino all'età di anni 14», continuando ad imporre «la limitazione provvisoria del trattamento, vietando l'ulteriore trattamento dei dati personali degli utenti dei quali non risulti in grado di verificare l'età anagrafica o, almeno, l'appartenenza a una fascia di età compatibile con la fruizione di servizi destinati a un pubblico di ultra-tredicenni debitamente autorizzati dagli esercenti la responsabilità genitoriale fino all'età di anni 14».

Il Garante ha ritenuto che, nel caso di specie, vi fossero inadeguate basi giuridiche legittimanti il trattamento e misure non idonee a garantire che il trattamento posto in essere fosse conforme alle prescrizioni indicate nel GDPR, rilevando la violazione, da parte del titolare, dei principi di *accountability*, di *privacy by design* e *by default*, nonché quello di *liceità* del trattamento in oggetto, con particolare riguardo alla violazione delle modalità di rilascio dell'informativa e del consenso al trattamento, a cui si aggiungono i rilievi concernenti la violazione del trasferimento dei dati all'estero e della conservazione dei dati trattati.

Appare poi utile citare il contenuto del comunicato stampa del 12 maggio 2021, con il quale il Garante ha aggiornato gli interessati circa i fatti accaduti[157]: dalla emanazione dei provvedimenti inibitori d'urgenza resi a partire da febbraio 2021, la società ha provveduto al blocco o alla rimozione di più di cinquecentomila *account* di infratredicenni italiani, adottando misure per impedire l'accesso dei più piccoli alla piattaforma. Dal provvedimento del mese di febbraio Tik Tok ha richiesto a più di dodici milioni e mezzo di utenti italiani di confermare di avere una età maggiore di tredici anni e centoquarantamila utenti sono stati bloccati tramite strumenti di moderazione e segnalazione dell'*app*. A seguito delle suddette implementazioni, il Garante ha chiesto di intervenire ulteriormente al fine di evitare che minori di anni "tredici" possano accedere alla piattaforma, ottenendo un nuovo impegno

[156] GPDP, Provv. n. 126 del 25 marzo 2021, doc. *web* n. 9574709.

[157] GPDP, *Da Tik Tok nuove misure per tenere i più giovani fuori dalla piattaforma. Intanto oltre 500 mila gli account di infratredicenni italiani già rimossi*, comunicato stampa del 12 maggio 2021, doc. *web* n. 9584923.

del *provider* a porre in essere misure fortemente incidenti sul principio di liceità del trattamento, sulle quali il Garante ha dichiarato di voler vigilare, proseguendo con l'attività di indagine a tutela dei minori utilizzatori del predetto *social network*.

Più recentemente, a fronte delle rilevate criticità concernenti la raccolta del consenso, la società fornitrice della nota piattaforma di *social network* ha ritenuto di percorrere altra strada, invocando quale base giuridica del trattamento il *legittimo interesse* di cui all'art. 6, par. 1, lett. *f)*, GDPR, ottenendo un nuovo provvedimento del Garante, reso in via d'urgenza in data 7 luglio 2022[158], con cui veniva affermata l'illiceità del trattamento, per violazione della normativa in materia di protezione dei dati personali, qualora venisse effettivamente fatto ricorso alla predetta condizione di liceità in luogo del consenso.

Per di più, annota ancora il Garante, «non può non evidenziarsi un approccio della piattaforma al tema della base giuridica piuttosto ondivago e piegato alle varie esigenze di volta in volta emergenti. Ad esempio, nella lunga vicenda relativa al trattamento dei dati dei minori di anni 13 che ha portato il Garante ad ordinare il blocco d'urgenza dei trattamenti in Italia da parte della piattaforma, quest'ultima ha sempre sostenuto l'applicabilità per i minori della base giuridica del contratto, rinviando invece al consenso per la somministrazione di pubblicità mirata ai maggiori di anni 16. Ora si intende modificare detta base giuridica, per i trattamenti originati presso la piattaforma, invocando il riferimento al legittimo interesse, come se la scelta del fondamento giuridico non fosse un presupposto consustanziale del trattamento dei dati, ma rappresentasse solo un disinvolto utilizzo della migliore opzione di volta in volta selezionabile da parte del titolare»[159].

3.2. La casistica internazionale sulla «*lawfulness of processing*»

3.2.1. *Liceità del trattamento, approvazione dei* cookies *e validità del consenso. Il caso della SA spagnola sul vettore «Vueling Airlines»*

Ampliando l'orizzonte dell'esame sin qui condotto dei principali provvedimenti ad una prospettiva sovranazionale, un primo caso rilevante riguarda l'utilizzo dei *cookies* di cui si è occupata l'Autorità di controllo spagnola nel caso della compagnia aerea Vueling.

In quel caso, la violazione delle previsioni sul consenso realmente informato e validamente espresso sull'uso dei cookie è costata al vettore Vueling Airlines S.L. la sanzione amministrativa di euro 30.000 comminata dall'Agencia Española de Protectión de Datos perché il vettore non aveva ottenuto dai propri utenti un valido consenso sull'uso dei *cookies* e non aveva fornito la possibilità di rifiutarli e accettarli[160].

[158] GPDP, Provv. n. 248 del 7 luglio 2022, doc. *web* n. 9788429.

[159] *Ibidem.*

[160] AGENCIA ESPAÑOLA DE PROTECTIÓN DE DATOS, *Resolution* disponibile all'indirizzo Internet https://www.aepd.es/es/documento/ps-00300-2019.pdf (da ultimo consultato in data 5 maggio 2021).

Il Garante spagnolo, accertata l'effettiva violazione delle modalità di acquisizione del consenso da parte del titolare del trattamento e accertato, altresì, il trasferimento dei dati raccolti tramite l'ausilio dei *cookies* di terze parti, appurava che il consenso dell'utente era implicitamente accordato tramite la prosecuzione dello scorrimento della pagina *web* senza, tuttavia, che egli avesse la possibilità di opporsi alla installazione di quei *cookies* non necessari al funzionamento della pagina e del servizio richiesto e ciò rendeva illecito il trattamento ai sensi dell'art. 22, co. 2, della *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*[161].

3.2.2. (segue)*: e la pronuncia della CGUE sul caso «Planet49»*

Sulla questione della valida espressione del consenso e sull'uso dei *cookies* si è autorevolmente pronunciata, con sentenza del 1 ottobre 2019, anche la Grande Sezione della Corte di Giustizia dell'Unione europea (CGUE), nella Causa C-673/17, dirimendo una controversia sorta tra due Federazioni di consumatori tedesche e la Planet49 GmbH, società fornitrice di giochi *on-line* che aveva bandito un concorso a premi.

Le Federazioni si erano rivolte alla Corte lamentando il fatto che gli utenti che volessero giocare al *game* fornito dalla Planet49 fossero reindirizzati ad una *web page* dove comparivano due didascalie accompagnate dalla casella di spunta da selezionare o deselezionare. Una prima casella, se selezionata, dava l'opportunità di acconsentire ad essere contattati da aziende per ricevere informazioni commerciali e promozionali; la seconda, che risultava già preselezionata, richiedeva di acconsentire alla installazione di *cookies* anche per finalità di profilazione e commerciali.

Le Federazioni lamentavano la violazione della normativa tedesca in materia e adivano il Tribunale di Francoforte sia per il risarcimento del danno sia per richiedere a Planet49 una modifica dell'uso dei *cookies*. Il tribunale accoglieva parzialmente il ricorso in primo grado e Planet49 ricorreva in appello presso il Tribunale superiore che, cassando come infondate le domande delle Federazioni, asseriva che l'utente

[161] Il testo della legge n. 34 del 11 luglio 2002 (*Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*) è disponibile all'indirizzo Internet https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758. Il comportamento del titolare risultava non conforme all'art. 22, co. 2, della Ley n. 34/2022, citato nel testo, di cui si propone di seguito una traduzione informale: «I fornitori di servizi possono utilizzare dispositivi di archiviazione e recupero dei dati sulle apparecchiature terminali dei destinatari, a condizione che questi ultimi abbiano dato il loro consenso dopo aver ricevuto informazioni chiare e complete sul loro utilizzo, in particolare sulle finalità del trattamento dei dati, in conformità con le disposizioni della Legge Organica 15/1999 del 13 dicembre sulla protezione dei dati personali.
Laddove tecnicamente possibile ed efficace, il consenso del destinatario ad accettare il trattamento dei dati può essere fornito attraverso l'uso di appropriate impostazioni del browser o altre applicazioni.
Ciò non impedisce l'eventuale memorizzazione o accesso di natura tecnica al solo scopo di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica o, nella misura strettamente necessaria, per la fornitura di un servizio della società dell'informazione espressamente richiesto dal destinatario».

avrebbe potuto provvedere autonomamente alla deselezione della spunta della casella e che tale opzione fosse chiaramente segnalata dal corredo chiaro e preciso dell'informazione sul funzionamento dei *cookies*.

La Corte Federale di giustizia, investita del ricorso, si interrogava sulla validità del consenso ottenuto mediante una casella di spunta in origine già preselezionata rispetto alle previsioni della normativa europea e procedeva sospendendo il procedimento con rinvio pregiudiziale *ex* art. 267 TFUE alla Corte di Giustizia dell'Unione europea, la quale si pronunciava ritenendo applicabili sia la Direttiva 95/46/CE sia il Reg. UE n. 679/2016 la cui disciplina, nonostante il Regolamento fosse entrato in vigore il 25 maggio 2018 e quindi successivamente sia alla data dell'ultima udienza davanti al Giudice del rinvio sia a quella pregiudiziale, era ritenuta comunque applicabile *ratione temporis* anche nell'ambito del procedimento principale poiché l'azione fatta valere dalle Federazioni intendeva censurare la condotta di Planet49 sia rispetto ai fatti pregressi, sia per il futuro.

La Corte di Giustizia ha ritenuto che il silenzio dell'utente dinnanzi allo scorrimento di una pagina *web* fornita di caselle preselezionate non possa configurare un consenso validamente espresso, orientamento ulteriormente avvalorato dalle disposizioni contenute nella Direttiva 2002/58/CE ("*e-Privacy*").

La Corte di Lussemburgo ha affermato, quindi, l'impossibilità di configurare quale consenso validamente espresso la mera possibilità di un'azione di *opt-out* tramite la quale negare il proprio consenso, affermando che sia «praticamente impossibile determinare in modo oggettivo se, non deselezionando una casella preselezionata, l'utente di un sito Internet abbia effettivamente manifestato il proprio consenso al trattamento dei suoi dati personali, nonché, in ogni caso, se tale consenso sia stato manifestato in modo informato».

È utile considerare che, in merito ai dati archiviati sul *device* dell'utente ai sensi del *considerando* n. 24 della citata Direttiva *e-Privacy*[162], a tali informazioni si debba riconoscere ampia tutela *ex* art. 8 CEDU quali dati della sfera privata dell'utente che debbano essere protetti alla luce delle disposizioni della normativa in materia. I *cookies* installati nel terminale dell'utente certamente permettono di avere accesso a molteplici dati e informazioni personali, nei cui confronti opera la tutela prevista ai sensi dell'art. 5, par. 3, della citata Direttiva 2002/58/CE[163]. Tale disposi-

[162] Nel *considerando* n. 24 della Dir. 2002/58/CE si afferma che «Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della Convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. I cosiddetti software spia, bachi invisibili ("web bugs"), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza».

[163] Ai sensi dell'art. 5 della Dir. 2002/58/CE (rubricato «*Riservatezza delle comunicazioni*»), «1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare, essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazio-

zione richiama l'art. 10 della Direttiva 95/46/CE, abrogata dal GDPR, in merito alle informazioni da rendere ai fini di un corretto e lecito trattamento dei dati personali.

Alla luce delle disposizioni in materia, la Corte di Giustizia ha considerato vietato l'utilizzo delle caselle preselezionate ai fini della valida espressione del consenso, la cui possibilità di deselezione non può in alcun modo essere intesa quale esplicazione di consenso attivo da parte dell'utente, non potendosi considerare il mancato esercizio della facoltà di *opt-out* come comportamento attivo e volitivo dell'interessato idoneo a integrare l'esistenza della condizione di liceità richiesta dalla disciplina in esame.

3.3. Le *app* di *contact tracing* nella pandemia da Covid-19 in Europa e in Italia

Un tema che merita di essere approfondito separatamente, per l'eccezionalità dei problemi da affrontare, che hanno richiesto in diversi casi di rivedere l'ordinario bilanciamento di interessi, riguarda il trattamento dei dati personali nell'ambito della pandemia causata da Covid-19.

Infatti, nell'ambito di una situazione di emergenza sanitaria[164] senza precedenti per dimensioni, gravità e persino imprevedibilità degli esiti[165], gli interventi (il più delle volte urgenti) di governi e dei soggetti privati si sono orientati verso l'uso di soluzioni basate sui dati per il contenimento della diffusione del virus al fine di tutelare la salute pubblica, suscitando, tuttavia, numerose preoccupazioni in materia di tutela della vita privata dei cittadini[166].

Un *virus* ignoto ha percorso e paralizzato il globo, mettendo in mostra le vulnerabilità del mondo e dell'uomo, costringendo i cittadini a stringenti misure di di-

ni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

2. Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale.

3. Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente».

[164] Vista la dichiarazione dell'Organizzazione Mondiale della Sanità dell'11 marzo 2020, con la quale l'epidemia da COVID-19 è stata valutata come «pandemia» in considerazione dei livelli di diffusività e gravità raggiunti a livello globale; si v. anche il d.l. 22 aprile 2021, n. 52, conv. con mod. dalla l. 17 giugno 2021, n. 87 (in G.U. del 21 giugno 2021, n. 146).

[165] GPDP, Intervista al Presidente Soro del 29 marzo 2020, doc. *web* n. 9301470.

[166] EDPB, *Linee Guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, 21 aprile 2020.

stanziamento sociale volte al rallentamento della diffusione dei contagi e rivoluzionando nel profondo i comportamenti e le abitudini delle persone[167].

Gli attori chiamati in causa nel più grande evento pandemico verificatosi dal secondo dopoguerra hanno delineato un nuovo sistema di controllo e di tutela della salute «ideando risposte efficaci per limitare la pandemia e proteggere i diritti umani e le libertà fondamentali»[168].

Per quanto il trattamento dei dati personali si sia rivelato efficace e necessario per la gestione della pandemia, è stato indispensabile mantenere un alto livello di protezione dei dati processati al fine di costituire un clima di fiducia tra i cittadini e creare condizioni di accettabilità delle misure adottate, fortemente limitative delle libertà personali nell'ottica – appunto – di tutela della salute globale.

Sin dall'approdo del *virus* in Europa – il primo Paese ad essere stato colpito è stato proprio l'Italia con il primo caso accertato nel febbraio 2020 –, si è assistito ad una rapida diffusione dei contagi, che in breve tempo hanno superato i confini geografici dei Paesi. A seguito di un primo comprensibile momento di difficoltà, per via della straordinarietà e gravità dell'evento, si è preferito maturare un comune approccio europeo al fine di dare una risposta concreta alla crisi.

3.4. (*segue*): Le Linee Guida dell'*European Data Protection Board* (EDPB)

Il primo intervento rilevante del Comitato europeo nel contesto dell'epidemia da Covid-19 è rappresentato dalla *Dichiarazione sul trattamento dei dati personali*[169], adottata in considerazione del fatto che i governi e gli organismi pubblici e privati stavano adottando misure volte al contenimento dell'impatto della diffusione da coronavirus e che tali misure stavano comportando il trattamento di diverse tipologie di dati personali.

In tale Dichiarazione, l'EDPB, dopo aver precisato che le norme di protezione contenute nel GDPR non fossero da intendersi in modo alcuno in contrasto con le misure volte al contenimento della pandemia, sottolineava la necessità di «garantire la liceità del trattamento dei dati personali e, in ogni caso, ricordare che qualsiasi misura adottata in questo contesto debba rispettare i principi generali del diritto e non possa essere irrevocabile. L'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza»[170].

In merito, in particolare, al principio di liceità del trattamento, la Dichiarazione dell'EDPB specificava che «il Regolamento generale sulla protezione dei dati (RGPD) è una normativa di ampia portata e contiene disposizioni che si applicano

[167] GPDP, Intervista al Presidente Soro del 29 marzo 2020, cit.

[168] EDPB, *Linee Guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, cit.

[169] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19*, adottata il 19 marzo 2020, disponibile all'indirizzo Internet https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_it_1.pdf (da ultimo consultato in data 2 aprile 2023).

[170] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19*, cit.

anche al trattamento dei dati personali in un contesto come quello relativo al Covid-19. Il RGPD consente alle competenti autorità sanitarie pubbliche e ai datori di lavoro di trattare dati personali nel contesto di un'epidemia, conformemente al diritto nazionale e alle condizioni ivi stabilite. Ad esempio, se il trattamento è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica. In tali circostanze, non è necessario ottenere il consenso degli interessati».

Per quanto «riguarda il trattamento dei dati personali, comprese le categorie particolari di dati, da parte di autorità pubbliche competenti (ad es. autorità sanitarie pubbliche), il Comitato ritiene che gli articoli 6 e 9 del RGPD consentano tale trattamento, in particolare quando esso ricada nell'ambito delle competenze che il diritto nazionale attribuisce a tale autorità pubblica e nel rispetto delle condizioni sancite dal RGPD», specificando ulteriormente che, «per quanto riguarda il trattamento dei dati delle telecomunicazioni, come i dati relativi all'ubicazione, devono essere rispettate anche le disposizioni nazionali di attuazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva e-privacy)»[171].

Poco prima della pubblicazione delle Linee guida dell'EDPB del 21 aprile 2020[172], la Presidente del Comitato trasmetteva alla Commissione europea una visione d'insieme di quello che sarebbe stato il contenuto delle Linee guida, indicando, quali utili strumenti di contrasto alla diffusone del *virus*, l'utilizzo di *app* di *contact tracing*[173]. L'adesione a tali *app* veniva da subito identificata come volontaria, indicando l'uso del *bluetooth* quale sistema di prossimità da utilizzare poiché maggiormente selettivo e di minor impatto sulla *privacy* dei cittadini. Nel testo della Lettera, la Presidente Jelinek ribadiva la centrale importanza dei criteri di *accountability* e dello svolgimento di una DPIA, del principio di *privacy by design* e *by default*, quali, tra gli altri, principi cardine in materia di trattamento dei dati personali ai sensi della normativa comunitaria. La Presidente suggeriva di subordinare l'uso di tali strumenti a stringenti controlli e verifiche di funzionamento affinché questi fossero perfettamente conformi alle regole della protezione dei dati personali e della libertà e della tutela dei diritti degli interessati al fine di ridurre al minimo le ingerenze sulla vita privata dei cittadini e, al contempo, fosse possibile tutelare la salute pubblica in una sfida tanto impegnativa.

Il concetto dell'adesione volontaria è stato promosso sin da subito dal Comitato e poi seguito dal Garante italiano, nonché dalle altre autorità di controllo, eretto a tutela della liberà di scelta del cittadino.

---

[171] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia da COVID-19,* cit., punto, 1.3.

[172] EDPB, *Linee Guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, cit.

[173] Lettera del 14 aprile 2020 della Presidente del Comitato Europeo per la Protezione dei dati personali consultabile sul sito del GPDP all'indirizzo Internet https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316030 (da ultimo consultato in data 2 aprile 2023). In materia di segnalano gli scritti di D. Poletti, *Il trattamento dei dati inerenti alla salute all'epoca della pandemia: cronaca dell'emergenza*, in *Persona e mercato*, 2020, 2, pp. 65 ss.; D. Poletti, *Contact tracing e App Immuni: atto secondo*, in *Persona e mercato*, 2021, 1, pp. 92 ss.; G. Resta, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, cit.; V. Cuffaro-R. D'orazio, *La protezione dei dati personali ai tempi dell'epidemia*, in *Corriere giuridico*, 2020, 6, pp. 729 ss.

Nelle Linee guida e nella ipotesi del Garante italiano si è addivenuti poi alla soluzione dell'obbligo di legge o dell'interesse pubblico quale base legittima del trattamento, fermo restando il consenso dell'utente, senza che possa essere cagionato pregiudizio a chi non faccia uso dell'*app* indicata, lasciando la libertà di scelta all'interessato e promuovendo una adeguata e trasparente campagna di sensibilizzazione a livello nazionale tesa a incoraggiare l'uso dello strumento di tracciamento, chiarendone la trasparenza, la funzionalità e la necessità[174].

Il Comitato Europeo per la Protezione dei dati ha auspicato sin dagli albori dello scoppio della pandemia che si instaurasse un clima di collaborazione tra i Paesi dell'Unione al fine di tutelare i diritti degli interessati, mantenere un clima di fiducia e identificare reali misure di contrasto alla pandemia. Considerate le *app* di *contact tracing* quali valido strumento per il contrasto della diffusione del *virus*, le citate Linee guida hanno chiarito le condizioni ed i principi per l'uso dei dati di localizzazione acquisiti degli strumenti di tracciamento. Tali dati vengono usati a supporto della risposta governativa all'evento pandemico al fine di creare modelli di diffusione del virus e per valutare l'efficacia delle stringenti misure di isolamento e quarantena da subito adottate. Le *app* di tracciamento installate nei *devices* degli utenti sono state, inoltre, utilizzate come strumento di avviso, tramite un sistema di *alert*, al fine di notificare alle «persone che sono probabilmente entrate in contatto con soggetti confermati positivi», e per «interrompere tempestivamente la trasmissione del contagio»[175].

L'approvazione di tali strumenti ha sollevato dibattiti circa l'efficacia degli strumenti di tracciamento e dell'impatto di questi sulla *privacy* dei cittadini: il Comitato ha sottolineato l'esigenza di procedere alla lettura del GDPR in combinato disposto con la Direttiva 2002/58/CE sulla vita privata e sulle comunicazioni elettroniche, la quale contiene norme specifiche che consentono l'uso di dati anonimi o personali per sostenere le autorità pubbliche e altri soggetti a livello nazionale e dell'UE, nel monitoraggio e nel contenimento della diffusione da *virus*. Il Comitato ha poi aggiunto che il ricorso alle *app* di tracciamento si debba ritenere volontario e che i dati raccolti si basino su informazioni di prossimità relative agli utenti, proseguendo l'analisi con un approfondimento circa l'utilizzo dei dati relativi all'ubicazione[176] dei *devices*, ricordando che tali informazioni possano essere trattate solo nei limiti degli artt. 6 e 9 della Direttiva citata; possano, cioè, essere trasmesse a terzi o autorità solo se resi anonimi dal fornitore oppure con il previo consenso dell'utente.

Per quanto concerne le informazioni archiviate sull'apparecchiatura, si prevedeva di poter accedere a tali dati solo se l'interessato avesse preventivamente prestato il consenso e/o l'accesso fosse necessario al servizio della società dell'informazione

[174] Si rimanda alla lettura della Lettera del 14 aprile 2020 della Presidente del Comitato Europeo per la Protezione dei dati personali, cit., e agli ulteriori approfondimenti sul funzionamento degli algoritmi utilizzati, sul codice sorgente, sul divieto di geolocalizzazione degli utenti e sul futuro dei dati raccolti al termine della emergenza sanitaria.

[175] *Ibidem*, p. 4.

[176] *Ibidem*, p. 5: «dati relativi all'ubicazione raccolti da fornitori di servizi di comunicazione elettronica (come gli operatori di telecomunicazioni mobili) nel corso della prestazione del loro servizio; e dati relativi all'ubicazione raccolti da fornitori di servizi della società dell'informazione, la cui funzionalità richiede l'uso di tali dati (ad esempio, navigazione, servizi di trasporto, ecc.)».

richiesto dall'utente. In riferimento ai dati, il Comitato sottolineava la necessità di privilegiare il trattamento di quelli anonimi, eliminando, cioè, la possibilità di collegare i dati raccolti con una persona fisica identificata o identificabile ponendo in essere uno sforzo «ragionevole». Qualora i dati raccolti non potessero essere anonimizzati, avrebbero dovuto essere intesi nel campo di applicazione del GDPR e non della Direttiva citata[177].

In merito al principio di liceità, si è osservato che, qualora le *app* di tracciamento comportassero la memorizzazione o l'accesso a informazioni precedentemente archiviate sul *device* dell'utente e qualora tali informazioni fossero necessarie per consentire al fornitore di rendere il servizio richiesto dall'utente, allora il trattamento dei dati non richiederebbe la prestazione del consenso da parte dell'interessato[178]; per le operazioni non necessarie, invece, si riteneva indispensabile chiederne il consenso.

Il Comitato ha poi precisato che la base giuridica del trattamento non dovesse necessariamente essere l'espressione della volontà dell'utente: qualora le autorità pubbliche fornissero un servizio sulla base di un mandato conferito dalla legge, la base giuridica maggiormente pertinente doveva essere identificata nello svolgimento di un compito di interesse pubblico ai sensi dell'art. 6, par. 1, lett. *e)* del GDPR. In questo senso si precisava che «la base giuridica o la misura legislativa che costituisce il fondamento di liceità per l'uso dell'*app* di tracciamento dei contatti dovrebbero prevedere garanzie significative, compreso un riferimento alla natura volontaria dell'*app*. Dovrebbe essere inclusa una chiara specificazione delle finalità e delle limitazioni riguardanti l'ulteriore utilizzo dei dati personali, nonché una chiara identificazione del titolare o dei titolari coinvolti. Occorre inoltre individuare le categorie di dati e i soggetti ai quali i dati personali possono essere comunicati, e per quali scopi. A seconda del grado di interferenza, occorre integrare salvaguardie ulteriori tenendo conto della natura, della portata e delle finalità del trattamento. Infine, il Comitato raccomanda di prevedere, non appena possibile, i criteri per stabilire quando l'*app* dovrà essere disinstallata e a chi spetti assumere tale determinazione»[179].

Il Comitato suggeriva che i processi di tracciamento fossero supervisionati da personale sanitario qualificato al fine di evitare che gli algoritmi di funzionamento identificassero falsi positivi e negativi e, in particolare, che i passi successivi alla ricezione di *alert* non si basassero unicamente su trattamenti automatizzati. Suggeriva, ancora, che tali algoritmi, al fine di garantire la correttezza del trattamento, il rispetto del principio di *accountability* e la conformità alla legge, fossero riesaminati e testati periodicamente da esperti e, ai fini della più ampia trasparenza possibile, ne fosse reso pubblico il codice sorgente. Prima della implementazione delle *app*, aggiungeva la raccomandazione di effettuare valutazioni di impatto, raffigurando il trattamento di tali dati una possibilità di rischio elevato per i diritti e le libertà delle

[177] Si rimanda l'approfondimento del tema sulla anonimizzazione ed in particolare alla p. 6 delle citate Linee guida.

[178] EDPB, *Linee Guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*, cit., punto 28, p. 7.

[179] *Ibidem*.

persone, configurandosi le ipotesi di trattamento su larga scala di dati relativi alla salute, monitoraggio sistematico e uso di nuove tecnologie.

3.5. (*segue*): Le *app* di *contact tracing* nei provvedimenti del Garante

Nel giugno 2020, sulla scorta delle citate Linee guida del Comitato Europeo per la protezione dei dati, il Garante italiano ha emanato il Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema[180] di allerta Covid 19 – App Immuni, autorizzando il Ministero della Salute ad avviare il servizio di trattamento.

La società fornitrice (Bending Spoons S.p.A.), come previsto dalle Linee guida europee, aveva provveduto all'invio al Ministero della relazione della valutazione di impatto sul sistema elaborato[181]. Da tale valutazione, benché il flusso di dati trattato fosse in ipotesi molto ampio, era emersa l'esistenza di misure volte a garantire il rispetto dei dritti e delle libertà degli interessati e la previsione di attività per attenuare i rischi da questa eventualmente derivanti.

Il Garante, considerata la complessità del sistema e il numero ampissimo di soggetti potenzialmente coinvolti, ha accolto la DPIA proposta prescrivendo una serie ulteriore di misure volte a rafforzare la sicurezza dei dati raccolti, chiedendo, nello specifico, particolare attenzione al rilascio di adeguata informativa agli utenti in riferimento anche al funzionamento dell'algoritmo di calcolo del sistema e delle ipotesi di errore di notificazione di esposizione al rischio, che venisse garantita la trasparenza dei dati raccolti ed il loro uso, nonché il trattamento delle informazioni per fini statistici-epidemiologici, evitando che tali dati potessero essere riassociati a soggetti identificabili adottando idonee misure di sicurezza e tecniche di anonimizzazione[182].

---

[180] GPDP, Provv. n. 95 del 1° giugno 2020, doc. *web* n. 9356568.

[181] Per la quale si rimanda a GPDP, Nota sugli aspetti tecnologici del 3 giugno 2020, doc *web* n. 9357972.

[182] GPDP, Provv. n. 65 del 25 febbraio 2021, doc. *web* n. 9555987, con cui il Garante ha ribadito che «Il trattamento di dati personali effettuato da parte del Ministero della salute nell'ambito del Sistema di allerta Covid-19 mediante l'App "Immuni" presenta una valutazione d'impatto, modificata secondo le indicazioni del Garante, contenente la previsione di misure adeguate a garantire il rispetto dei diritti e delle libertà degli interessati, che attenuano i rischi che potrebbero derivare dal trattamento, e un nuovo meccanismo per consentire in autonomia, a un soggetto risultato positivo, di caricare le TEK (*Temporary Exposure Key*) nel *backend* di Immuni e dunque di interagire direttamente con il sistema di allerta Covid-19 per comunicare l'esito positivo del referto, consentendo una maggior efficienza complessiva del sistema medesimo» e che «Il trattamento dei dati personali operato dal Ministero della salute in relazione al Sistema di allerta Covid-19 (App "Immuni") – che ha la propria base giuridica in specifiche previsioni normative (tra cui l'art. 6, d.l. n. 28/2020, conv. con mod. dalla l. 27/2020) per il perseguimento di un interesse pubblico rilevante, ai sensi degli artt. 6, par. 1, lett. *e)*, e 9, par. 2, lett. *i)*, GDPR ed è caratterizzato dall'adesione volontaria dell'utente che scarica l'App sul proprio smartphone previa adeguata informativa – è autorizzato dal Garante per la protezione dei dati personali». Cfr., *amplius*, E. GUERRI, *Autorizzazione al trattamento dei dati personali effettuato attraverso l'App Immuni (sistema di allerta Covid-19) da parte del Ministero della Salute*, in *Data protection e privacy officer (Osservatorio Privacy dell'Università di Bologna),* Commento al Provvedimento del Garante del 25 febbraio 2021, doc. *web* n. 9555987, disponibile *online* in *open access* all'indirizzo https://www.dataprotection-privacy.it/autorizzazione-al-trattamento-dei-dati-

Dal momento dell'inizio della pandemia il Garante ha svolto numerose attività in materia, pubblicando documenti e approfondimenti[183] al fine di orientare l'opinione pubblica e di tutelare i cittadini contro il dilagare di *app* di tracciamento, raccogliendo poi i principali orientamenti nelle FAQ di *contact tracing* e *app* regionali per Covid-19[184], ove si ribadiva che l'utilizzo di tali strumenti fosse disciplinato dall'art. 6 del d.l. n. 28/2020, che ha istituito il Sistema nazionale di allerta Covid ed ha uniformato a livello nazionale il quadro di garanzie poste a tutela degli interessati[185].

Considerate le varie ipotesi opzionate dagli enti locali, il Garante ha ribadito in tale occasione che le regioni non potessero limitare l'accesso nei propri territori solo a coloro che avessero installato l'*app* Immuni, configurando tale previsione una conseguenza pregiudizievole per gli interessati in quanto incidente sulla libertà di circolazione, diritto fondamentale costituzionalmente garantito[186].

Sulla base dei presupposti citati, del contenuto delle Linee guida dell'EDPB ed in particolare della necessità di prevedere norme dell'ordinamento come base giuridica per la liceità del tracciamento mediante *app*, il Garante in un comunicato stampa dell'estate 2020, in merito al proliferare di simili soluzioni per il *contact tracing*, si è espresso ribadendo come i trattamenti non coperti dalla normativa nazionale siano illeciti e violino le norme in materia di *privacy*[187]. L'Autorità ha ritenuto necessario chiarire che l'emergenza Covid-19 non funge in automatico da base giuridica sufficiente a legittimare il trattamento di dati personali e categorie particolari di tali dati per consentire il tracciamento dei contatti da parte di titolari pubblici e privati. Gli unici trattamenti leciti previsti sono quelli fondati su e giustificati da adeguata base giuridica che poggi su una norma di legge nazionale. Ogni altro trattamento privo di adeguata fonte giuridica era da intendersi, dunque, in violazione della normativa europea e nazionale.

Ciò ha trovato successiva conferma nel provvedimento[188] del Garante con cui, dopo un precedente provvedimento di limitazione provvisoria[189], è stata dichiarata l'illiceità del trattamento posto in essere mediante l'*app* «Mitiga Italia»[190], non sussistendo una valida base giuridica.

---

personali-effettuato-attraverso-lapp-immuni-sistema-di-allerta-covid-19-da-parte-del-ministero-della-salute/ (consultato da ultimo in data 5 ottobre 2022).

183 GDPD, Coronavirus e protezione dei dati, documenti e approfondimenti, doc. *web* n. 9293264.

184 GDPD, FAQ – App nazionale di *contact tracing* e *app* regionali per Covid-19, documenti e approfondimenti, consultabili all'indirizzo Internet https://www.garanteprivacy.it/temi/coronavirus/faq#contact-tracing (da ultimo consultato in data 21 aprile 2021).

185 D.l. 30 aprile 2020, n. 28 (pubbl. in G.U. del 30 aprile 2020, n. 111), conv. con mod. dalla l. 25 giugno 2020, n. 162 (pubbl. in G.U. del 29 giugno 2020, n.162). La norma (art. 6) funge da presupposto giuridico per introdurre il sistema di tracciamento come misura di sanità pubblica e soddisfa i requisiti del GDPR come enucleati agli artt. 6, par. 1, lett. *e)*, par. 2, lett. *g)* e lett. *i)* e del nuovo c. *privacy* agli artt. 2-*ter* e 2-*sexies*.

186 GPDP, FAQ – App nazionale di *contact tracing* e *app* regionali per Covid-19, documenti e approfondimenti, cit.

187 GPDP, comunicato del 10 agosto 2020, doc. *web* n. 9447462.

188 GPDP, Provv. n. 102 del 24 marzo 2022, doc. *web* n. 9762855.

189 GPDP, Provv. n. 224 del 3 giugno 2021, doc. *web* n. 9592298.

190 L'*app* in questione risulta essere stata utilizzata per la prima volta nel maggio 2021 per consentire l'ingresso alla finale di una competizione sportiva degli spettatori in possesso di certificazione atte-

In tale occasione, il Garante ha ribadito che «la previsione di subordinare l'accesso a luoghi al possesso di una certificazione attestante l'avvenuta vaccinazione, la guarigione o lo stato di negatività dal Covid-19, costituisce una misura volta a comportare una limitazione delle libertà personali»[191] e, come tale, «può essere considerata ammissibile solo se prevista da una norma di legge statale» ai sensi dell'art. 6, par. 2 e 3, GDPR e dell'art. 9, GDPR, nonché degli artt. 2-*ter* e 2-*sexies* del c. *privacy*, «adottata in conformità a quanto previsto dal Regolamento, ovvero definendo un complesso articolato di misure volte a consentire il conseguimento del rilevante obiettivo di interesse pubblico, nel contesto emergenziale, nel rispetto dei diritti e delle libertà degli interessati, secondo un criterio di proporzionalità».

Al contrario, il Garante ha confermato che «un trattamento di dati finalizzato a verificare il possesso delle condizioni per autorizzare l'accesso a locali ed eventi, che emuli, di fatto, le funzionalità del sistema pubblico di certificazione verde Covid-19, non può trovare fondamento nel consenso dell'interessato, quale base giuridica del trattamento (art. 6, par. 1, lett. *a)* del Regolamento) e quale condizione per il trattamento delle categorie particolari di dati degli utenti (art. 9, par. 2, lett. *a)* del Regolamento)»[192].

stante l'avvenuta vaccinazione, la guarigione o lo stato di negatività da Covid-19.

[191] GPDP, Provv. n. 224 del 3 giugno 2021, cit.

[192] *Ibidem*.

Capitolo III
Il principio di correttezza

Giovanni Di Ciollo

SOMMARIO: 1. Inquadramento normativo. – 1.1. Le disposizioni rilevanti in ambito nazionale e sovranazionale. – 1.2. La correttezza tra clausola generale e principio. – 2. Portata del principio. – 2.1. La determinazione contenutistica del principio di correttezza. L'inevitabile confronto con il canone civilistico di correttezza e buona fede. – 2.2. Il principio di correttezza come criterio di bilanciamento di interessi. – 2.3. Rilevanza dell'abuso del diritto in ambito *privacy*. Il problema della revoca del consenso – 2.4. Correttezza e modalità operative. – 2.5. Regole deontologiche e codici di condotta. – 2.6. Finalità del trattamento, ragionevoli aspettative. – 3. Applicazione del principio nella casistica. – 3.1. Estensione e limiti del principio di correttezza. – 3.2. Uno sguardo concreto alla correttezza "procedurale". – 4. Riflessioni conclusive.

1. Inquadramento normativo

1.1. Le disposizioni rilevanti in ambito nazionale e sovranazionale

Il principio di correttezza in ambito *privacy*[1] è sancito all'art. 5, par. 1, lett. *a)*, Reg. (UE) 679/2016 sulla protezione dei dati personali, il quale recita: «I dati personali sono: *a)* trattati in modo lecito, corretto e trasparente nei confronti dell'interessato».

[1] La dottrina più rilevante sul punto, in ordine cronologico: A. Barba, *Le modalità del trattamento*, in V. Cuffaro-V. Ricciuto, *La disciplina del trattamento dei dati personali*, Torino, 1997, pp. 162-167; E. Navarretta, Commento *sub* art. 9, in C.M. Bianca-F.D. Busnelli (a cura di), *Commentario alla L. 31 dicembre 1996, n. 675*, in *Le Nuove leggi civile commentate*, Padova, 1999, 2-3, p. 318 ss.; P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, p. 419 ss.; F. Piraino, *La liceità e la correttezza*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, p. 745 ss.; E. Navarretta, Commento *sub* art. 11, in C.M. Bianca-F.D. Busnelli (a cura di), *Commentario al d.lgs. 30 giugno 2003, n. 196 ("Codice della* privacy*")*, in *I libri de Le nuove leggi civili commentate*, Padova, 2007, p. 241 ss.; F. Resta, Commento *sub* art. 5, in G.M. Riccio-G. Scorza-E. Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018, pp. 52-54; G. Malgieri, Commento *sub* art. 5, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta, *Codice della privacy e data protection*, Milano, 2021, pp. 180-182; a livello europeo, cfr. D. Clifford-J. Ausloos, *Data protection and the Role of Fairness*, in *Yearbook of European Law*, 2018, 1, p. 130 ss; G. Malgieri, *The concept of Fairness in the GDPR: A linguistic and contextual interpretation*, in *FAT '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, ACM, 2020, p. 154 ss. Per i riferimenti dottrinali in tema di correttezza come clausola generale e come principio, con particolare riguardo al codice civile, si rinvia, *infra*, al par. 1.2.

Il principio non è una novità apportata dal GDPR – questo già era previsto dalla l. 31 dicembre 1996, n. 675, all'art. 9, co. 1, lett. *a)*, il quale recitava: «I dati personali oggetto di trattamento devono essere: *a)* trattati in modo lecito e secondo correttezza»; trasposizione dell'art. 6, par. 1, lett. *a*), Dir. 95/46/CE, secondo cui: «Gli Stati membri dispongono che i dati personali devono essere: *a)* trattati lealmente e lecitamente»[2]. Il dettato è confluito, sostanzialmente inalterato, nell'ormai abrogato art. 11, co. 1, lett. *a)*, d.lgs. 30 giugno 2003, n. 196 (Codice per la protezione dei dati personali). Il principio ricorre altresì nella Convenzione di Strasburgo n. 108[3] all'art. 5, par. 1, lett. *a)*: «I dati a carattere personale oggetto di elaborazione automatica devono essere: *a)* ottenuti ed elaborati lealmente e legalmente»; l'inciso è confluito, a seguito dell'introduzione del protocollo emendativo alla Convenzione in oggetto del 18 maggio 2018, alla lett. *d)* dell'art. 5, par. 1 del testo consolidato della Convenzione (c.d. Convenzione n. 108+)[4].

Il principio di correttezza, insieme con gli altri, è richiamato all'art. 5 del Regolamento, a tal fine rubricato «Principi applicabili al trattamento di dati personali», dunque mutando la precedente "etichetta" apposta dal legislatore unionale; difatti, il precedente art. 6 della direttiva 95/46/UE era contenuto nella Sezione I del Capo II, rubricata «Principi relativi alla qualità dei dati»[5].

I principi, a seguito della riforma del 2016, costituiscono la chiave di volta che sorregge il complesso di norme dettate nella nuova normativa *privacy*, caratterizzati da valenza tanto programmatica quanto precettiva, come del resto si intende dalla conformazione dell'apparato sanzionatorio *ex* art. 83, par. 5, lett. *a)*, GDPR, ed *ex* art. 166, co. 5, d.lgs. 196/2003, anche in considerazione della previsione di inutiliz-

---

[2] Occorre specificare, dal punto di vista etimologico, che *lealtà* e *correttezza* sono ambo traduzioni del termine inglese "*fairness*"; di conseguenza l'interprete italiano deve distinguere la correttezza dall'*esattezza*, in inglese "*accuracy*", consacrata, in forma di principio, alla lett. *d)* dell'art. *de quo*. La sostanziale equivalenza delle espressioni *fairness*, *correttezza*, nonché *buona fede in senso oggettivo*, appare pacifica in dottrina: «Nella cultura italiana la "buona fede" è sinonimo di lealtà, correttezza, e quindi ha un significato molto vicino alla nozione inglese di *fairness*», così G. ALPA, *I principi generali*, in G. IUDICA-P. ZATTI (a cura di), *Trattato di diritto privato*, 2ª ed., Milano, 2006, pp. 250-251.

[3] Trattato del consiglio d'Europa 29 gennaio 1981, n. 1985, «*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*», firmato dall'Italia il 2 febbraio 1983, ratificato il 29 marzo 1997.

[4] Trattato del Consiglio d'Europa 10 ottobre 2019, n. 223, «*Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*», firmato dall'Italia il 5 marzo 2019. A seguito dell'introduzione di tale protocollo emendativo, la versione consolidata della Convenzione è stata ridenominata «108+». Il protocollo emendativo introduce un rafforzamento delle tutele già approntate agli interessati alla luce dell'emanazione del GDPR. La correttezza viene menzionata altresì all'art. 8, par. 1, ult. periodo del testo consolidato della convenzione: «*Each Party shall provide that the controller informs the data subjects of* (...) *as well as any necessary additional information in order to ensure fair and transparent processing of the personal data*».

[5] Altresì, l'abrogato art. 11 d.lgs. 196/2003, così come modificato da d.lgs. 101/2018, era rubricato «*Modalità del trattamento e requisiti dei dati*», contenuto nel Capo I del Titolo III, denominato «*Regole generali per il trattamento dei dati*».

zabilità dei dati raccolti in violazione della disciplina rilevante[6] *ex* art. 2-*decies* d.lgs. 196/2003.

L'estrema somiglianza degli enunciati dei diversi atti normativi nei quali è contenuta la clausola generale di correttezza suggerisce che vi sia, in linea di principio, continuità contenutistica tra il principio di correttezza previsto dalla direttiva 95/46/CE e quello previsto dal nel Regolamento (UE) 679/2016.

Il concetto di correttezza, altresì, è richiamato in plurimi *considerando* del GDPR (nn. 39, 45, 60, 71, 129) e articoli (5, 6, 13, 14, 40) del Regolamento, seppure mai autonomamente, ma solo congiuntamente o al principio di liceità o a quello di trasparenza; altresì, il Regolamento non ne fornisce una definizione espressa e non ne chiarisce la portata, non essendone mai espressamente esemplificati i precipitati diretti[7]: alla disamina di tali aspetti, nella teoria e nella prassi, si riservano rispettivamente i par. 2 e 3 del presente scritto.

1.2. La correttezza tra clausola generale e principio

Il principio di correttezza contemplato dalla normativa di settore costituisce altresì clausola generale[8]: occorre distinguere i due concetti. Chi scrive ritiene di accedere alla ricostruzione di Velluzzi, il quale, conducendo il proprio studio nel solco già inciso da Mengoni e Belvedere[9], definisce la "clausola generale" quale «termine o sintagma[10] di natura valutativa (in quanto necessitante di un processo di *integra-*

---

[6] M. Ratti, *La responsabilità da illecito trattamento dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, pp. 783-784. La disposizione in commento ricalca, peraltro, il secondo comma dell'abrogato art. 11 d.lgs. 196/2003, il quale, collocato immediatamente dopo l'enunciazione dei principi della materia, implicitamente rimarcava, in ottica interpretativa sistematica, la rilevanza, ai fini dell'operatività del rimedio inibitorio, della violazione dei principi stessi, *ivi* compreso quello di correttezza. Sul punto cfr. E. Navarretta, Commento *sub* art. 11, cit., pp. 244-245.

[7] Al contrario del principio di trasparenza, la cui portata è ben delineata e descritta nel *considerando* n. 39.

[8] Cfr. V. Velluzzi, *Le clausole generali: semantica e politica del diritto*, Milano, 2010, cap. I. Sul tema, diffusamente, cfr. M. Libertini, *Clausole generali, norme di principio, norme a contenuto indeterminato. Una proposta di distinzione*, in *Riv. crit. dir. priv.*, 2011, 3, p. 345 ss.; A. Belvedere, *Le clausole generali tra interpretazione e produzione di norme*, in *Politica del diritto*, 1988, p. 311 ss.; A. Falzea, *Gli* standards *valutativi e la loro applicazione*, in *Riv. dir. civ.*, 1987, p. 1 ss.; Id., Standards *valutativi e controllo di legittimità*, in Id., *Ricerche di teoria generale del diritto e di dogmatica giuridica*, *III*, *Scritti d'occasione*, Milano, 2010, p. 645 ss.; S. Rodotà, *Il tempo delle clausole generali*, in *Riv. crit. dir. priv.*, 1987, p. 709 ss., anche in Id., *Critica del diritto privato*, Napoli, 2017, p. 131 ss.; L. Mengoni, *Spunti per una teoria delle clausole generali*, in *Riv. crit. dir. priv.*, 1986, p. 9 ss.; C. Castronovo, *L'avventura delle clausole generali*, in *Riv. crit. dir. priv.*, 1986, p. 21 ss.; A. di Majo, *Clausole generali e diritto delle obbligazioni*, in *Riv. crit. dir. priv.*, 1984, p. 539 ss.; F. Roselli, *Il controllo della cassazione civile sull'uso delle clausole generali*, Napoli, 1983; K. Engisch, *Introduzione al pensiero giuridico*, trad. di A. Baratta, Milano, 1970.

[9] Cfr. V. Belvedere, *Le clausole generali tra interpretazione e produzione di norme*, cit., *passim*; L. Mengoni, *Spunti per una teoria delle clausole generali*, cit., *passim*.

[10] Ordunque il «frammento di norma», così come definita da Luigi Mengoni in Id., *Spunti per una teoria delle clausole generali*, cit., p. 11. *Contra*, M. Libertini, *Clausole generali*, cit., pp. 348-349, nota n. 5, il quale rileva che negli usi linguistici correnti ci si riferisce alle clausole generali quali norme *complete*, seppur connotate da un coefficiente di indeterminatezza.

zione valutativa; *n.d.a.*)[11] caratterizzato da indeterminatezza, per cui il significato di tali termini o sintagmi non è determinabile (...) se non facendo ricorso a criteri, parametri di giudizio (definiti altresì come *standard*; *n.d.a.*)[12], interni e/o esterni al diritto tra loro potenzialmente concorrenti»[13]; ordunque, i "principi"[14], espressi o inespressi, sono «norme, affatto peculiari, ma norme, mentre le clausole generali sono termini o sintagmi, vale a dire elementi, componenti di norme»[15]. Principi e clausole generali, dunque, percorrono binari differenti, i quali possono incontrarsi, financo sovrapporsi, nel caso in cui un principio contenga termini valutativi (dunque clausole generali), o essere distinti, qualora la clausola generale non faccia parte di un principio, espresso o inespresso[16].

L'art. 5, par. 1, lett. *a)*, GDPR, posta la sua collocazione gerarchicamente sovraordinata nella disciplina oggetto di disamina, atteso il carattere di indeterminatezza che la connota, integra senz'altro un principio[17]. Allo stesso tempo, tuttavia, la

[11] Cfr. V. VELLUZZI, *Le clausole generali*, cit., p. 63 ss.

[12] V. VELLUZZI, *Le clausole generali*, cit., p. 64: «(...) lo *standard* è il criterio di giudizio per mezzo del quale si determina il significato della clausola generale risolvendo l'indeterminatezza. L'integrazione valutativa è, dunque, la scelta dello standard operata dall'interprete tra criteri concorrenti» Sul punto altresì L. MENGONI, *Spunti per una teoria delle clausole generali*, cit., pp. 14-15: «(...) oggetto del rinvio disposto dalle clausole generali non sono gli *standards* per sé considerati, ma in quanto riconoscibili come forme esemplari dell'esperienza sociale dei valori. Essi non sono norme senz'altro applicabili, ma piuttosto esprimono punti di vista, criteri direttivi per la ricerca di valori che il giudice deve poi tradurre, con un proprio giudizio valutativo, in una norma di decisione». Sulla consistenza di tale rinvio, a specificazione degli elementi costitutivi della clausola generale, Pedrini rimarca, sulla scorta di Velluzzi: «(...) non basta un termine valutativo per avere una clausola generale, essendo necessario che il primo sia quantomeno interpretabile come un rinvio a *standard* meta-giuridici», cfr. F. PEDRINI, *Clausole generali e principi costituzionali*, in *Forum di quaderni costituzionali. Rassegna*, 2015, p. 26, nota a piè di pagina n. 118.

[13] Cfr. V. VELLUZZI, *Le clausole generali*, cit., p. 34 ss.

[14] Più approfonditamente, sui principi, cfr. N. LIPARI, *Intorno ai «principi generali del diritto»*, in *Riv. dir. civ.*, 2016, 1, p. 28 ss.; U. BRECCIA, *Principi: luci e ombre nel diritto contemporaneo*, in *Riv. it. scienze giur.*, 2014, p. 122 ss.; G. ALPA, *I principi generali*, cit., *passim*; ID., *Il dialogo sui principi generali tra legislazione, dottrina e giurisprudenza*, in *Riv. it. sc. giur.*, 2013, 4, p. 85 ss.; G. PINO, *Principi e argomentazione giuridica*, in *Ars interpretandi*, 2009, p. 131 ss.; G. ZAGREBELSKY, *Diritto per: valori, principi o regole? (a proposito della dottrina dei principi di Ronald Dworkin)*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, 2002, II, p. 865 ss.; R. DWORKIN, *I diritti presi sul serio*, trad. it. di F. ORIANA, Bologna, 1982.

[15] Cfr. V. VELLUZZI, *Le clausole generali*, cit., p. 78.

[16] Cfr. V. VELLUZZI, *Le clausole generali*, cit., pp. 79-80.

[17] Cfr. G. PINO, *principi e argomentazione giuridica*, cit, p. 134 ss. A livello sistematico, si evidenzia che l'art. *de quo* è rubricato «*Principi applicabili al trattamento di dati personali*», ed è contenuto nel Capo II del Regolamento stesso, titolato «*Principi*». Similmente, seppure in riferimento alla clausola generale di buona fede, F. PIRAINO, *La buona fede in senso oggettivo*, Torino, 2015, p. 76: «mentre il "principio" è qualificazione della norma, la "clausola generale" è qualificazione dell'enunciato normativo o meglio di una sua porzione, quella coincidente con i termini valutativi». L'A. precisa che il canone di buona fede non è qualificabile come "principio fondamentale" in quanto non partecipa del carattere idealistico e assiologico proprio di tale categoria, pur nella sua indubbia connotazione valoriale, essendo, al contrario, più appropriato definirlo come "principio generale", in quanto votato ad assolvere una funzione squisitamente strumentale (come la tutela dell'autodeterminazione contrattuale, la preservazione degli assetti di interessi convenuti nel regolamento contrattuale in caso di sopravvenienze, etc.), posto il suo carattere sovraordinato rispetto alla pluralità di

correttezza *ivi* richiamata costituisce clausola generale[18]: l'atteggiarsi del principio, dunque, dipende dalla determinazione dello spettro di significati attribuibili al termine "correttezza", la quale avverrà mediante l'individuazione degli *standard* che si riterranno più adeguati[19].

2. Portata del principio

2.1. La determinazione contenutistica del principio di correttezza. L'inevitabile confronto con il canone civilistico di correttezza e buona fede

Lo studio del principio di correttezza non può che prendere le mosse dall'analisi delle clausole di correttezza[20] *ex* art. 1175 c.c. e buona fede oggettiva[21] *ex* art. 1375 c.c., endiadi ad oggi intesa in senso unitario[22]. Tali clausole rinviano a un *corpus* di valori metagiuridici e morali compendiati[23] nella relazione del Ministro Guardasigilli al Codice civile: «La correttezza è uno stile morale della persona che indica spirito di lealtà, abito virile di fermezza, di chiarezza e di coerenza, fedeltà e rispetto a quei doveri che, secondo la coscienza generale, devono essere osservati nei rapporti tra consociati»[24]. Invero, tale tentativo di illustrare la clausola di buona fede e correttezza è stato tacciato di dogmatismo[25] e demagogismo[26]. A seguito di

norme che regolano la materia delle obbligazioni e dei contratti. Precedentemente, cfr. A. di Majo, *Delle obbligazioni in generale. Art. 1173-1176*, Commento *sub* art. 1175, in F. Galgano (a cura di), *Commentario del Codice civile Scialoja-Branca*, Bologna-Roma, 1988 p. 305 ss. Similmente pure G.M. Uda, *La buona fede nell'esecuzione del contratto*, Torino, 2005, p. 76 ss., il quale sostiene la compresenza, nell'ordinamento, della clausola generale di buona fede e di un principio generale di buona fede, desunto dalla iterazione di una molteplicità di norme aventi ad oggetto la buona fede in senso oggettivo.

[18] In tal senso, cfr. P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., p. 400; la stessa Navarretta, nel riferirsi alla correttezza nell'ambito della l. 675/1996, adopera la locuzione "clausola generale", cfr. E. Navarretta, Commento *sub* art. 9, cit., p. 326.

[19] Cfr. S. Patti, *L'interpretazione delle clausole generali*, in *Riv. dir. civ.*, 2013, 2, p. 263 ss.

[20] Cfr. A. di Majo, *Delle obbligazioni in generale*, cit., p. 287 ss.; L. Rovelli, «*Correttezza*», in *Digesto civ.*, IV, Torino, 1989, p. 423 ss.; V. Carbone, Commento *sub* art. 1175 – *Comportamento secondo correttezza*, in V. Cuffaro (a cura di), *Delle obbligazioni. I. Artt. 1173-1217 c.c.*, in E. Gabrielli, *Comm. cod. civ.*, Torino, 2012, p. 77 ss.

[21] Cfr. L. Bigliazzi Geri, *Buona fede nel diritto civile*, in *Digesto civ.*, II, Torino, 1988, p. 169 ss.; sul tema, ampiamente e approfonditamente, cfr. F. Piraino, *La buona fede in senso oggettivo*, cit., *passim*.

[22] Una risalente dottrina soleva operare un *discrimen* contenutistico tra le due clausole, essendo una dettata in materia di obbligazioni, l'altra in materia contrattuale; sul tema, diffusamente cfr. F. Piraino, *La buona fede in senso oggettivo*, cit., p. 12 ss; G. Finazzi, *Correttezza e buona fede*, in L. Garofalo (a cura di), *Trattato delle obbligazioni*, I.4, Milano, 2018, p. 5 ss.; A. di Majo, *Delle obbligazioni in generale*, cit., p. 287 ss.; S. Rodotà, *Le fonti di integrazione del contratto*, Milano, 1969 (ristampa 2004), p. 132 ss.; E. Betti, *Teoria generale delle obbligazioni*, Torino, 1953.

[23] Per una rassegna dei tentativi definitori della clausola di buona fede si veda F. Piraino, *La buona fede in senso oggettivo*, cit., p. 27 ss.

[24] Cfr. Relazione del Ministro Guardasigilli al testo definitivo del Codice civile, n. 558.

[25] Cfr. F. Piraino, *La buona fede in senso oggettivo*, cit., p. 27 ss.

[26] Cfr. A. di Majo, *Delle obbligazioni in generale*, cit., p. 285 ss.

un intervento normativo, poco dopo l'emanazione del Codice[27], l'inciso che faceva riferimento ai principi della solidarietà corporativa venne espunto, data l'inattualità del richiamo di matrice ideologica fascista[28]. Privato di tale guida, parte della dottrina ha sostenuto l'implicita abrogazione della norma[29]; tuttavia, la stessa ha ritrovato la perduta ragione d'essere grazie agli sforzi d'interpretazione costituzionalmente orientata[30], soprattutto in relazione al principio di solidarietà[31] sancito dall'art. 2 Cost. La clausola di buona fede altresì ricorre nell'art. 2598 c.c., co. 1, n. 3), nella veste di «*correttezza professionale*», la quale è caratterizzata dal dovere di astenersi

[27] Art. 3, co. 2, d.lgs.lgt. 14 settembre 1944, n. 287.

[28] Cfr. F. PIRAINO, *La buona fede in senso oggettivo*, cit., p. 9, nota a piè di pagina n. 40.

[29] In dottrina è stato mordacemente rimarcato come tale articolo, in ragione della sua collocazione, costituisse un «festone di poco gusto collocato all'inizio del libro per dare al lettore profano la sensazione che vi avrebbe respirato aria fascista», cfr. G. PUGLIESE, *Relazione sul libro delle obbligazioni*, in *Annuario di diritto comparato e di studi legislativi*, Roma, 1950, p. 176. Altresì, cfr. G. FERRI, *Diritto agli utili e diritto al dividendo*, in *Riv. dir. comm.*, 1963, 1, p. 412; V. GRECO, *Ancora sulla concorrenza sleale per violazione delle esclusive di vendita*, in *Riv. dir. comm.*, 1955, 2, p. 461 ss.

[30] Cfr. G. FINAZZI, *Correttezza e buona fede*, *cit.,* p. 4 ss.; S. RODOTÀ, *Il principio di correttezza e la vigenza dell'art. 1175 cod. civ.*, in *Banca borsa tit. cred.*, 1965, 1, p. 149 ss.

[31] Cfr. L. MENGONI, *Obbligazioni «di risultato» e obbligazioni «di mezzi» (studio critico)*, in C. CASTRONOVO-A. ALBANESE-A. NICOLUSSI (a cura di), *Scritti. II. Obbligazioni e negozio*, Milano, 2011, pp. 261-262, in particolare nota n. 35: «Il d.leg. 14 settembre 1944, n. 287 non ha avuto la mano felice quando ha soppresso l'inciso finale dell'art. 1175 («in relazione ai principi della solidarietà corporativa»). Sarebbe stato assai più opportuno conservare l'inciso, limitandosi a sostituire all'aggettivo «corporativa» l'aggettivo «sociale». Tuttavia, la mutilazione dell'articolo operata dal frettoloso legislatore del 1944 può oggi essere riparata coordinando l'art. 1175 c.c. con l'art. 2 Cost. È certo, comunque, che gli obblighi di correttezza, la cui osservanza è imposta vicendevolmente al debitore e al creditore dal criterio della buona fede, si desumono dai principi di solidarietà che ispirano la moderna comunità statale». Altresì, cfr. S. RODOTÀ, *Le fonti di integrazione del contratto*, cit., p. 115 ss.; C.M. BIANCA, *La nozione di buona fede quale regola di comportamento contrattuale*, in *Riv. dir. civ.*, 1983, 1, pp. 209-210. Al riguardo si rammenta, altresì, la risalente sentenza 5 novembre 1970 del Trib. di Bologna, in *Foro it.*, 1971, IV, p. 1030 ss.; il giudice, nel ricercare le regole di correttezza (modernamente, uno degli *standard* concorrenti) da applicare al caso concreto, ritiene necessario il riferimento, oltre che alle disposizione del Codice civile e altre leggi, ai principi fondamentali della Costituzione, in particolare quello di solidarietà sociale: «Tali criteri, insieme al principio, vigente nel diritto civile, della reciproca buona fede nei rapporti negoziali, delineano un quadro che ha per fulcro il principio del rispetto della personalità e della dignità altrui, nella consapevolezza di appartenere ad una identica collettività, nella quale è d'obbligo lo spirito di solidarietà, che può ingiungere talvolta perfino ad imporre una certa attenuazione dell'uso dei propri diritti». Altresì, cfr. Cass. civ., sent. 10 marzo 1998, n. 2639, Cass. civ., sent. 5 maggio 2000, n. 5671, entrambe pronunciate in tema di responsabilità extracontrattuale per danno derivante da circolazione di veicoli, nelle quali è esplicitato come l'oggetto del principio di solidarietà sociale si desuma, «oltre che dalla Costituzione (art. 2), anche da alcune norme del c.c. (art. 1175 c.c.)». Non si può far a meno di evincere una relazione circolare tra clausola di buona fede e principio di solidarietà: la prima attinge al secondo, e quest'ultimo, in relazione alle fattispecie contrattuali, si concretizza, nei suoi significati, rifacendosi al primo; sul punto, approfonditamente, G.M. UDA, *La buona fede nell'esecuzione del contratto*, cit., p. 64 ss. Sul rapporto tra principio di correttezza, principio di solidarietà e dati personali si veda, in particolare, F. BRAVO *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, pp. 405-441 (nonché, *amplius*, il Cap. XIV del presente volume).

dal porre in essere comportamenti che siano idonei a recare pregiudizio all'esercizio dell'altrui attività professionale[32].

La clausola generale di correttezza e buona fede non impone esclusivamente un generale obbligo di astensione dal ledere l'altrui diritto: è stato evidenziato come, intesa in tal senso, la clausola andrebbe sostanzialmente a coincidere con il principio di *neminem laedere ex* art. 2043 c.c. Difatti, non si armonizzerebbero con tale posizione sia la previsione di quegli obblighi di informazione nella fase precontrattuale[33], nonché la presenza di norme quali l'art. 1227, co. 2, c.c., il quale prevede l'irrisarcibilità del danno derivante dall'inadempimento del debitore, ove questo fosse evitabile dal creditore con l'uso dell'ordinaria diligenza[34]. Deve dunque ritenersi che l'adempimento del dovere di correttezza si sostanzi *anche* in comportamenti attivi ed operosi.

Alla clausola di correttezza e buona fede si ricollegano tradizionalmente diverse funzioni: questa è funge da *canone valutativo* delle condotte delle parti nella fase di attuazione del rapporto obbligatorio[35], ovvero assurge a fonte di integrazione del contratto[36], sulla base del concorso di fonti eteronome alla determinazione del

---

[32] Quale il metro di paragone per saggiare la correttezza di tali comportamenti, tuttavia, è stato a lungo dibattuto in dottrina e giurisprudenza. Le diverse proposte ricostruttive hanno fatto variamente riferimento a: principi di natura etica, prassi professionale, norme deontologiche, principi di natura prettamente economica, ovvero all'interpretazione più strettamente aderente ai principi generali dell'ordinamento di rango costituzionale, nonché una combinazione tra i precedenti; cfr., sul punto, M. Libertini, *I principi della correttezza professionale nella disciplina della concorrenza sleale*, in *Eur. dir. priv.*, 1999, p. 509 ss.; vedi, altresì, G. Ghidini, *La correttezza professionale (art. 2598, n. 3. c.c.) tra due ordinamenti costituzionali*, in Aa.Vv., *Studi in ricordo di Pier Giusto Jaeger*, Milano, 2011, p. 753 ss., p. 757 ss.; V. Di Cataldo-A. Vanzetti, *Manuale di diritto industriale*, 8a ed., Milano, 2018, p. 25 ss.; G. Floridia, *Le clausole generali. La clausola generale della correttezza professionale di cui al n. 3 dell'art. 2598 c.c.*, in Aa.Vv., *Diritto industriale. Proprietà intellettuale e concorrenza*, 6a ed., Torino, 2020, p. 386 ss.

[33] C.M. Bianca, *Le obbligazioni*, in *Diritto civile*, III, 3a ed., Milano, 2019, p. 140 ss. Rilevante, sul punto, Cass. civ., sent. 29 settembre 2005, n. 19024, in *Danno e resp.*, 2006, p. 25 ss., nota di V. Roppo-G. Afferni, D*ai contratti finanziari al contratto in genere: punti fermi della Cassazione su nullità virtuale e responsabilità precontrattuale*; altresì, cfr. G. Meruzzi, *La responsabilità precontrattuale tra regola di validità e regola di condotta*, in *Contratto e impresa*, 2006, p. 944 ss.

[34] *Ex multis* cfr. Cass. civ., sent. 20 novembre 1991, n. 12439, in *Foro it.*, 1993, 4, p. 1223 ss. Cfr. G. Finazzi, *Correttezza e buona fede*, cit., p. 9.

[35] Cfr. C.M. Bianca, *La nozione di buona fede quale regola di comportamento contrattuale*, in *Riv. dir. civ.*, 1983, 1, p. 205. Occorre specificare che Bianca sembra operare una sintesi tra i pregressi orientamenti dottrinali: un primo orientamento (cfr. U. Natoli, *L'attuazione del rapporto obbligatorio. I. Il comportamento del creditore*, in A. Cicu-F. Messineo (diretto da), *Trattato di diritto civile e commerciale*, XVI, Milano, 1974, p. 6 ss.) riteneva che il canone di buona fede fosse un criterio di valutazione *elastico* ed *ex post* del contegno delle parti, il quale doveva compiersi rinunciando a far riferimento a modelli comportamentali prefigurati, limitando l'attività valutativa alle circostanze del caso concreto; un secondo orientamento, al contrario, sottolineava la portata conformativa *rigida* della clausola, idonea ad orientare la condotta delle parti fin dal principio del rapporto, sulla base di regole di condotta necessariamente preesistenti (cfr. M.L. Loi-F. Tessitore, *Buona fede e responsabilità precontrattuale*, Milano, 1975, p. 19 ss.).

[36] *Ex multis*, cfr. S. Rodotà, *Le fonti di integrazione del contratto*, ristampa integrata, Milano, 2004, p. 175 ss.; V. Roppo, *Il contratto*, Milano, 2011, 2a ed., p. 465 ss.; A. D'Angelo, *La buona fede*, in *Il contratto in generale*, IV, in M. Bessone (diretto da), *Tratt. dir. priv*., XIII, Torino, 2004, p. 43 ss.

regolamento contrattuale *ex* art. 1374 c.c., prevedendo in capo ai paciscenti nuovi obblighi, non solo con funzione suppletiva delle lacune eventualmente riscontrabili nelle pattuizioni[37], bensì anche giungendo al riconoscimento di autonomi obblighi di protezione[38]. La disgiunzione tra le due funzioni illustrate è dovuta alla *querelle*,

Rilevante, in giurisprudenza, la sentenza Cass. civ., 20 aprile 1994, n. 3774: «il dovere di correttezza (art. 1175 c.c.) (...) si porge nel sistema come limite interno di ogni situazione giuridica soggettiva, attiva o passiva, contrattualmente attribuita, concorrendo, quindi, alla relativa conformazione in senso ampliativo o restrittivo rispetto alla fisionomia apparente, per modo che l'ossequio alla legalità formale non si traduca in sacrificio della giustizia sostanziale e non risulti, quindi, disatteso quel dovere (inderogabile) di solidarietà, ormai costituzionalizzato (art. 2 Cost.), che, applicato ai contratti, ne determina integrativamente il contenuto o gli effetti (art. 1374 cod. civ.) e deve, ad un tempo, orientarne l'interpretazione (art. 1366 cod. civ.) e l'esecuzione (art. 1375 cod. civ.), nel rispetto del noto principio secondo cui ciascuno dei contraenti è tenuto a salvaguardare l'interesse dell'altro, se ciò non comporti un apprezzabile sacrificio dell'interesse proprio».

[37] In tal senso F. PIRAINO, *La buona fede in senso oggettivo*, cit., p. 276. In generale, sulla questione dell'incompletezza contrattuale e della portata integratrice della clausola di buona fede, anche in ottica comparatistica, v. V. BONGIOVANNI, *Integrazione del contratto e clausole implicite*, Milano, 2018, p. 106 ss.

[38] Sulla rilevanza degli obblighi di protezione in relazione alla buona fede in funzione integrativa, cfr. F. PIRAINO, *La buona fede in senso oggettivo*, cit., p. 245 ss. Degli obblighi di protezione si discorre ben più frequentemente in ambito precontrattuale, riconducendoli alla categoria delle «*obbligazioni senza prestazione*», cfr. C. CASTRONOVO, *L'obbligazione senza prestazione. Ai confini tra contratto e torto*, in *Le ragioni del diritto. Scritti in onore di Luigi Mengoni*, I, Milano, 1995, p. 147 ss.; ID., *Responsabilità civile*, Milano, 2018, 4ª ed., p. 521 ss.; L. MANNA, *Le obbligazioni senza prestazione*, in L. GAROFALO-M. TALAMANCA (diretto da), *Trattato delle obbligazioni. I. La struttura e l'adempimento*, t. III, L. GAROFALO (a cura di), *Obbligazioni senza prestazioni e obbligazioni naturali*, Padova, 2010, p. 3 ss.; Cfr. S. ROSSI, *Contatto sociale (fonte di obbligazione)*, in *Digesto civ.*, appendice di aggiornamento V, Torino, 2010, p. 346 ss.; A. ZACCARIA, *Der aufhaltsame Aufstieg des sozialen Kontakts – La resistibile ascesa del «contatto sociale»*, in *Riv. dir. civ.*, 2013, 1, p. 77 ss.; F. PIRAINO, *la buona fede in senso oggettivo*, cit., p. 230 ss.; A. DI MAJO, *L'obbligazione "protettiva"*, in *Eur. dir. priv.*, 2015, 1, p. 8 ss.; A. NICOLUSSI, *Obblighi di protezione*, in *Enc. dir.*, Ann. VIII, Milano, 2015, p. 659 ss.; A. M. GAROFALO, *Il problema del contatto sociale*, in *Teoria e storia del diritto privato*, 2018, XI, *passim*; D. PITTELLA, *Dall'obbligazione senza prestazione alla responsabilità extracontrattuale del medico: rigetto locale o totale del contatto sociale "qualificato"?*, in *Contratto e impresa*, 2020, 1, p. 418 ss. La dottrina a sostegno di tale figura valorizza l'art. 1337 c.c., fonte autonoma di obbligazioni "protettive" prive di una prestazione così come intesa ai sensi dell'art. 1174 c.c. (cfr. L. MENGONI, *Autonomia privata e costituzione*, in *Scritti*, I, Milano, 2011, p. 109), estendendone il campo di applicazione, per analogia, anche a fattispecie non afferenti alle trattative contrattuali (C. CASTRONOVO, *L'eclissi del diritto civile*, Milano, 2015, p. 146). L'addentellato normativo su cui tali obbligazioni si innestano è l'art. 1173 c.c., in particolare l'inciso «*ogni altro atto o fatto idoneo a produrle in conformità dell'ordinamento giuridico*», mentre la situazione di fatto dalla quale hanno scaturigine è l'affidamento obiettivo ingenerato in una parte dal contegno dell'altra (cfr. L. MENGONI, *Sulla natura della responsabilità precontrattuale*, in *Riv. dir. comm.*, 1956, 2, p. 370; per una ricostruzione in chiave storica dell'interpretazione dell'art. *de quo*, in relazione alla questione *ivi* affrontata, cfr. D. PITTELLA, *Dall'obbligazione senza prestazione alla responsabilità extracontrattuale del medico*, cit., p. 421 ss.): «L'affidamento, da misurarsi ovviamente su basi oggettive, che un soggetto ripone nelle specifiche conoscenze professionali, costituisce un fatto idoneo *ex* art. 1173 c.c. a far sorgere una relazione giuridicamente rilevante tra la persona che versa in uno stato soggettivo di fiducia e il danneggiante. È proprio, quindi, la configurabilità di questo particolare legame a permettere l'individuazione dei soggetti legittimati al risarcimento», (A. THIENE, *Inadempimento alle obbligazioni senza prestazione*, in G. VISINTINI (a cura di), *Trattato della responsabilità contrattuale,* I, *Inadempimento e rimedi*, Padova, 2009, p. 337); il contatto tra le diverse sfere

ancora perdurante, sulla inconciliabilità di tali modi di operare, alternativi e in sé

giuridiche, nello specifico, deve essere *qualificato* da uno scopo che esse intendano perseguire (Cass. civ., sent. 12 luglio 2016, n. 14188). Conseguenza di tale ricostruzione è l'attrazione di talune figure (C. Castronovo, *L'eclissi del diritto civile*, cit., p. 130), tradizionalmente riconducibili nell'alveo della responsabilità aquiliana, al paradigma di responsabilità da inadempimento di obbligazioni *ex* art. 1218 c.c., ben più favorevole per il danneggiato in relazione al regime prescrizionale, al riparto dei carichi probatori e alla determinazione dei danni risarcibili (cfr. D. Pittella, *Dall'obbligazione senza prestazione alla responsabilità extracontrattuale del medico*, cit., p. 437 ss.). In termini non troppo dissimili, Piraino identifica l'ambito elettivo delle obbligazioni senza prestazione in quelle vicende «che non si iscriv(ono) adeguatamente nello schema dell'illecito aquiliano, a causa di indiscutibili elementi di relazionalità (*rechtlich Sonderverbindung*), ma neppure si presenta(no) come un inadempimento di un'obbligazione in senso classico, in quanto il vincolo, che pur sussiste, non ha una funzione poietica, non essendo preordinato all'incremento della sfera giuridica dell'avente diritto», cfr. F. Piraino, *La responsabilità precontrattuale e la struttura del rapporto prenegoziale*, in *Persona e Mercato*, 2017, 2, pp. 127-128. Punto comune delle ricostruzioni *ivi* esposte è la conformazione, nella forma di obbligazioni senza prestazione, di fattispecie non dotate di una disciplina sufficientemente attagliata alle peculiarità che le connotano (C. Castronovo, *Responsabilità civile*, cit., pp. 523-524).

Orbene, chi scrive ritiene che l'ambito della tutela dei dati personali è estraneo a tale novero per due ordini di motivi. In primo luogo, finanche ritenendo integrati i requisiti oggettivi del contatto sociale qualificato – limitatamente al momento della predisposizione dell'informativa, nei trattamenti per i quali è richiesta – tra interessato e titolare del trattamento, in ragione dell'obbiettivo affidamento che connota un rapporto tanto squilibrato come quello in oggetto, in caso di violazione degli obblighi di protezione – normati e ipostatizzati in obblighi informativi e di trasparenza, da adempiere conformemente ai principi del GDPR e alla disciplina di cui agli artt. 12-14 GDPR – non vi è dubbio sul regime di responsabilità da applicare – quello di cui all'art. 82 GDPR –, in quanto l'apparato sanzionatorio delineato dalla normativa di settore attribuisce pieno rilievo alle violazioni della correttezza tanto nelle fasi precedenti al trattamento quanto in costanza dello stesso, non operando, a tal fine, alcuna distinzione, né temporale, né qualitativa: non hanno dunque rilievo le considerazioni di autonomia del piano degli obblighi di protezione rispetto al rapporto principale. In secondo luogo, si rileva che la figura dell'obbligazione senza prestazione risulta inadeguata, se confrontata con il modello di responsabilità introdotto dalla normativa *de quo*. A tal proposito, l'art. 82, par. 2, GDPR, delinea un duplice regime di regime di responsabilità per il titolare e il responsabile del trattamento (cfr. S. Sica, Commento *sub* art. 82, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta, *Codice della privacy e data protection*, cit., p. 892): in particolare, il responsabile del trattamento risponde a titolo di colpa presunta superabile provando di aver adempiuto agli obblighi del GDPR o alle legittime istruzioni del titolare del trattamento, mentre quest'ultimo risponde a titolo di responsabilità oggettiva (la dottrina citata ritiene che la nuova norma di riferimento vada interpretata in continuità con la disciplina di cui all'art. 15 d.lgs. 30 giugno 2003, n. 196, abrogato dal d.lgs. 10 agosto 2018, n. 101, il quale estendeva il regime di cui all'art. 2050 c.c. a tutte le ipotesi di danno conseguenti il trattamento di dati personali, cfr. S. Sica, *op. ult. cit.*, p. 893; similmente, M. Ratti, *La responsabilità da illecito trattamento dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, cit., p. 780). Il regime di responsabilità oggettiva, difatti, inasprisce l'onere di prova liberatoria a carico del danneggiante se confrontato con il regime di responsabilità *ex* art. 1218 c.c., il quale, al contrario, troverebbe applicazione in caso di inadempimento dell'obbligazione senza prestazione.

Tali rilievi inducono a ritenere che la figura dell'obbligazione senza prestazione non solo non si coniughi adeguatamente, a livello sistematico, con le norme che attribuiscono rilevanza ai normati obblighi di protezione della disciplina *privacy*, bensì finirebbe per approntare una tutela più debole nei confronti del danneggiato, contraddicendo l'intima ragion d'essere dell'elaborazione dottrinale esposta.

autosufficienti[39], del canone di buona fede. Le posizioni possono così sinteticamente riassumersi: in quest'ultima ricostruzione, la buona fede opera integrando il rapporto nella fase di esecuzione dello stesso, mediante la previsione di nuovi obblighi accessori, la cui violazione permette il ricorso alla tutela risarcitoria, inibitoria e in forma specifica[40]; nella seconda funzione, sulla base della valutazione dei comportamenti delle parti secondo buona fede, l'applicazione rigida del diritto è contemperata dall'esperibilità dell'*exceptio doli generalis*, volta a paralizzare le pretese formalmente legittime ma sostanzialmente abusive e contrarie a buona fede, e a valutare la correttezza dell'adempimento in sede di esecuzione del contratto o, più precisamente, la rilevanza dell'inadempimento sul piano rimediale[41]. Le due declinazioni operative corrispondono a differenti modalità di tutela sotto l'egida della buona fede, che poggiano l'una su un ragionamento più strettamente sillogistico, dal quale discende una forma di tutela volta alla rimozione del danno sofferto, l'altra su un ragionamento prettamente *morale* e non primamente orientato sul piano dei rimedi[42].

Sin dal recepimento della direttiva *privacy* nel '96, la correlazione tra principio di correttezza nella disciplina di settore e clausola generale di correttezza e buona fede è apparsa chiara allo stesso legislatore domestico; Navarretta rammenta che, in sede di recepimento, si sostituì «al precetto di un trattamento dei dati personali lecito e corretto (così il disegno di legge approvato alla Camera con il n. 1580), un'espressione che volutamente ricalca il modello codicistico: trattamento lecito e "secondo correttezza" (...) non per amore di simmetria linguistica, ma più probabilmente per eludere un'interpretazione moraleggiante o restrittiva della correttezza e per ereditare le mature riflessioni autoctone, dense di sviluppi interni a partire dall'abuso del diritto»[43].

---

[39] Piraino rimarca come tali entrambi orientamenti siano stati concepiti in modo da poter spiegare completamente e in modo autosufficiente gli effetti della buona fede, cfr. F. PIRAINO, *La buona fede in senso oggettivo*, cit., pp. 346-347; lo stesso A., peraltro, non esclude la possibilità di ibridazione delle due funzioni, seppur non in merito all'assetto rimediale di cui esse sono foriere, cfr. ID., *La buona fede in senso oggettivo*, cit., p. 351. Altri AA., nel segno della conciliazione tra tali due orientamenti, hanno peraltro sostenuto che la differenza tra gli stessi fosse più nominale che sostanziale: «i sostenitori della prima si mostr(a)no propensi a qualificare come obblighi "nuovi" (e, dunque, "integrativi") quelle che sono semplici modalità – individuate dal giudice come "corrette" (ossia conformi a buona fede, tanto ai sensi dell'art. 1366 c.c. quanto ai sensi dell'art. 1375 c.c.) – di adempimento di obblighi (o di esercizio di diritti) già scaturenti dal contratto», così G. D'AMICO, *Applicazione diretta dei principi costituzionali e integrazione del contratto*, in *Giust. civ.*, 2015, pp. 271-272.

[40] Cfr. A. DI MAJO, *Delle obbligazioni in generale*, cit., p. 322; F. PIRAINO, *La buona fede in senso oggettivo*, cit., p. 348.

[41] Cfr. F. PIRAINO, *La buona fede in senso oggettivo*, cit., p. 352 ss.; chiama tale funzione della buona fede «integrazione *in executivis*», sottolineandone la rilevanza nella fase di attuazione del rapporto obbligatorio, A. DI MAJO, *Delle obbligazioni in generale*, cit., p. 324 ss.

[42] Cfr. F. PIRAINO, *La buona fede in senso oggettivo*, cit., pp. 350-351.

[43] Cfr. E. NAVARRETTA, Commento *sub* art. 9, cit., p. 319. Sul punto anche V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, p. 106.

Tuttavia, sembra che né il parallelismo lessicale, oggi venuto meno con l'emanazione del Regolamento, né tantomeno la scelta del termine «correttezza», in luogo di «leale», siano stati elementi decisivi per l'attrazione del principio, inteso nei suoi significati più generali, nell'alveo della clausola generale di buona fede già nota all'ordinamento domestico. A tal proposito, difatti, si rileva che, raffrontando le diverse versioni linguistiche del testo del GDPR, le soluzioni adottate spaziano da termini più lessicalmente vicini al corrispettivo italiano «leale»[44], al termine «equo»[45], peraltro usato dal legislatore domestico nel *considerando* n. 129, seppure non in relazione all'attività di trattamento; meno frequenti le soluzioni che invece adoperano l'omologo estero del termine «corretto»[46]. Altresì, più platealmente, la soluzione tedesca, che ricorre all'espressione «*Treu und Glaube*», con la quale si traccia un chiaro riferimento alla buona fede codicistica di cui al § 242 BGB; parimenti, nell'ordinamento francese, è ormai pacifico il «*devoir de loyauté*»[47], avente funzione sostanzialmente analoga al dovere di correttezza nell'adempimento delle obbligazioni *ex* art. 1175 c.c.

Appare dunque chiaro che il principio di correttezza della normativa di settore *ivi* analizzato germini specificamente dalla *bona fides* della tradizione giuridica europea[48]. Le conclusioni della dottrina e giurisprudenza italiana raggiunte nel campo della buona fede sono dunque utile e pertinente guida per indirizzare lo studio che si procede ad esporre, tenendo bene a mente, tuttavia, che il corretto quadro di interpretazione del principio oggetto di esame deve tenere conto delle diverse sensibilità e tradizioni giuridiche delle plurime nazioni destinatarie dell'atto normativo unionale a massima armonizzazione, nonché delle differenze linguistiche tra i vari atti normativi, come altresì specificato dalla CGUE[49], la quale, in particolare, rimarca: «anche nel caso di piena concordanza delle versioni linguistiche, (...) il diritto comunitario impiega una terminologia che gli è propria. D'altronde, va sottolineato che le nozioni giuridiche non presentano necessariamente lo stesso contenuto nel diritto comunitario e nei vari diritti nazionali»[50].

---

[44] Nella specie, il testo del Regolamento in francese fa spesso uso del termine «*loyal*» come traduzione del termine inglese «*fair*» (cfr. *considerando* n. 39); similmente, il testo spagnolo fa uso del termine «*leal*».

[45] Il testo portoghese fa largo uso del termine «*equitativo*» per tradurre il termine «*fair*», come anche quello rumeno adopera il termine «*echitabile*».

[46] Il testo svedese all'art. 5, par. 1, lett. *a)*, adopera il termine «*korrekt*», seppure, per tutti gli altri casi, ricorre al termine «*rattvis*», traducibile come «equo». Per una disamina delle differenti peculiarità linguistiche delle soluzioni adottate dagli stati membri per tradurre il termine «*fair*», cfr. G. Malgieri, *The concept of Fairness in the GDPR*, cit., pp. 162-163.

[47] *Ex multis* cfr. Y. Picod, *Le devoir de loyauté dans l'exécution du contrat*, *Librairie générale de droit et de jurisprudence*, 1989, *passim*; Cass. com., sent. 6 novembre 2012, n. 11-20582.

[48] Cfr. G. Malgieri, *The concept of Fairness in the GDPR*, cit., p. 161.

[49] Cfr. Corte di giustizia, causa 283/81, Srl CILFIT e Lanificio di Gavardo SpA c. Ministero della sanità, § 18: «Va (...) considerato che le norme comunitarie sono redatte in diverse lingue e che le varie versioni linguistiche fanno fede nella stessa misura: l'interpretazione di una norma comunitaria comporta quindi il raffronto di tali versioni».

[50] Cfr. CGUE, sent. ult. cit., par. 19.

La forte indeterminatezza del concetto di "buona fede" ha indotto la dottrina, ormai da anni, a desistere da ogni approccio definitorio di tale la clausola generale, data l'impossibilità di enunciarne il contenuto in modo completo e assiomatico. A tal proposito, non convincono le molteplici formule adoperate in relazione alla stessa[51], le quali finiscono per ridursi a operazioni descrittive generiche o tautologiche[52], il cui valore non può essere che meramente esemplificativo. Dunque, invece che volgere lo studio in tale direzione, la ricerca dello spettro di significati e funzioni da attribuire al principio di correttezza nella materia della tutela dei dati personali, sulla scorta della metodologia già adottata da di Majo nella disamina della clausola generale di correttezza e buona fede[53], si soffermerà, rispettivamente, sulle differenti sfumature etimologiche, e, dunque, di significato, che, come già accennato nel presente paragrafo, tingono il principio di correttezza, nonché sugli ambiti operativi nei quali tale principio viene in rilievo.

2.2. Il principio di correttezza come criterio di bilanciamento di interessi

La prima menzione della correttezza, come già precisato *supra*, si rinviene all'art. 5, par. 1, lett. *a)*, accostato ai termini «liceità» e «trasparenza». Tale trittico, tuttavia, non si ripete nel testo dell'atto normativo, dacché il principio di correttezza è affiancato, di volta in volta, o da quello di liceità o da quello di trasparenza.

La dottrina in commento alla previgente normativa[54] ha ampiamente approfondito il rapporto tra liceità e correttezza. A tal proposito, è stata criticata da più parti[55] la tendenza, fin troppo prodiga in analiticità, del legislatore europeo, il quale, declamando il principio di liceità, non sembra aver aggiunto nulla che non fosse già chiaro tenuto conto dell'art. 288, par. 2, TFUE, il quale è sufficiente a sancire la vincolatività, per gli Stati membri dell'Unione Europea, del Regolamento in oggetto. A ciò si aggiunga che, come specificato nel par. 1, la violazione dei principi, *ivi* compresi quelli di liceità e correttezza, comporta l'illiceità del trattamento, rendendo esperibili meccanismi rimediali sanzionatori e inibitori.

A fronte di tale dato positivo, la dottrina ha sentito l'esigenza di elaborare criteri discretivi per adeguatamente delineare gli ambiti elettivi – con i rispettivi punti d'intersezione – dei principi di correttezza e liceità. Nella specie, si è sostenuto che entrambi i principi operano come tecniche di bilanciamento di interessi[56]: la liceità,

---

[51] Sull'ondivaghezza delle quali si rimanda, tra tutti, a F. PIRAINO, *La buona fede in senso oggettivo*, cit.

[52] Cfr. A. DI MAJO, *Delle obbligazioni in generale*, cit., p. 336.

[53] Cfr. A. DI MAJO, *Delle obbligazioni in generale*, cit., p. 305 ss. Altresì, F. PIRAINO, *La buona fede in senso oggettivo*, cit., pp. 8, nota n. 31.

[54] Cfr., in particolare, E. NAVARRETTA, Commento *sub* art. 9, cit.; EAD., Commento *sub* art. 11, cit.; F. PIRAINO, *Liceità e correttezza*, cit.

[55] Cfr. F. PIRAINO, *Liceità e correttezza*, cit., pp. 749-750; P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., p. 408 ss.

[56] Cfr. E. NAVARRETTA, Commento *sub* art. 9, cit., p. 321. Sulle condizioni di liceità del trattamento come meccanismi di selezione e bilanciamento di interessi meritevoli, cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, cit., p. 113 ss. Approfonditamente,

da intendersi *in senso stretto*, tendenzialmente opera *a priori*, stabilendo *ex ante* le condizioni *formali* di legittimità del trattamento; la correttezza tendenzialmente opera a posteriori, stabilendo *ex post* le condizioni *sostanziali* di legittimità dello stesso. La dialettica tra liceità e correttezza è stata paragonata[57] al doppio grado di valutazione della condotta delle parti nell'attuazione del rapporto obbligatorio, il primo di rigorosa conformità del fatto alla legge, il secondo di valutazione delle condotte ai sensi del canone di buona fede[58].

Il dialogo tra correttezza e liceità si è detto connotato da *complementarità esterna*[59]: più sono intensi i vincoli posti dallo *jus strictum*, tanto meno vi sarà spazio per il bilanciamento degli interessi secondo la regola di correttezza; viceversa, ove dovessero allentarsi le maglie del diritto positivo, si espanderà lo spettro di influenza di quest'ultima. Altresì, i due principi si trovano, tra loro, in un ulteriore rapporto, definito di *complementarità interna*: nella specie, è stata rimarcata l'operatività della regola di correttezza all'interno dello spettro applicativo della regola di liceità, tale da «evitare un uso distorto della libertà già a priori maggiormente limitata»[60], e dunque idonea ad orientare l'esercizio del diritto secondo correttezza.

La correttezza opera, *in primis*, in quelle fessure di discrezionalità attribuite dal legislatore al titolare del trattamento, in particolare ogni qual volta sia demandato allo stesso un giudizio valutativo sulla prevalenza o meno di interessi contrapposti, fra i quali, in particolare, quello al perseguimento del legittimo interesse del titolare del trattamento o di terzi, *ex* art. 6, par. 1, lett. *f)*, GDPR; nonché l'interesse al proseguimento dell'attività di trattamento qualora il titolare del trattamento ritenga che vi siano motivi legittimi cogenti e prevalenti *ex* art. 21, par. 1, GDPR; parimenti, la correttezza, pur non essendo espressamente richiamata, si erge a canone di valutazione sia del merito della sussistenza di rischi per i diritti e le libertà dell'interessato, in relazione agli artt. 35 e 36 GDPR, dovendosi ritenere senz'altro contrarie a correttezza le eventuali argomentazioni illogiche, oblique, omissive, fraudolente o mistificatorie volte a far apparire come scevro di rischi un trattamento che, al contrario, li presenta, anche relativamente all'appropriatezza ed efficacia delle misure poste in essere[61], sia, infine, di cosa debba essere considerato *un rischio* per i diritti e le libertà dell'interessato. Altre circostanze, per le quali il criterio di correttezza assurge a canone di bilanciamento sono le «specifiche situazioni di trattamento» di cui agli artt. 85-89, nelle quali il diritto dell'interessato deve essere bilanciato con interessi per lo più pubblici.

---

sulle tecniche di bilanciamento degli interessi nel previgente codice *privacy* e il ruolo, sotto tale aspetto, dei principi di tale materia, cfr. F. Piraino, *Codice della* privacy *e bilanciamento di interessi*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, cit., p. 695 ss.

57 Cfr. F. Piraino, *Codice della* privacy *e bilanciamento di interessi*, cit., p. 718.

58 Cfr. U. Natoli, *L'attuazione del rapporto obbligatorio*, cit., p. 27 ss.; L. Bigliazzi Geri, *Buona fede nel diritto civile*, cit., p. 172 ss.

59 Cfr. E. Navarretta, Commento *sub* art. 9, cit., p. 325; F. Piraino, *Liceità e correttezza*, cit., pp. 761-762.

60 Cfr. E. Navarretta, Commento *sub* art. 9, cit., p. 326.

61 Cfr. par. 2.4 del presente scritto.

Nel ruolo di canone di bilanciamento[62], il giudizio secondo correttezza attinge alla nozione di *equità*[63]: il *considerando* n. 129, a tal proposito, nel far riferimento ai poteri delle autorità di controllo dei singoli Stati membri, specifica che gli stessi debbano essere esercitati in modo *equo*. Il sintagma «in modo equo» è traduzione dell'avverbio originale inglese «*fairly*», il cui relativo sostantivo «*fairness*» è invece sempre tradotto come «correttezza» nel testo normativo. L'accezione particolare intesa si ricava dallo stesso *considerando*, il quale dispone che ogni misura adottata dalle autorità su citate deve essere «imparziale» e «proporzionale». Imparzialità e proporzionalità implicano la *non discriminazione*; tale accento si ritrova nel *considerando* n. 71 inerente alle decisioni automatizzate e l'attività di profilazione. Nello stesso, difatti, pur essendo ammessi meccanismi decisori automatizzati, sono posti limiti al ricorso a tale forma di trattamento: in particolare, il titolare del trattamento deve adottare misure tecniche e organizzative tali da impedire *effetti discriminatori* nei confronti degli interessati; a tal proposito, il Gruppo di lavoro *ex* art. 29, nelle linee guida sulla profilazione e sulle decisioni automatizzate[64], specifica che il trattamento automatizzato di dati idoneo a ingenerare discriminazioni sulla base del sesso, delle opinioni politiche, della religione, deve ritenersi contrario a correttezza.

Occore precisare che l'espressione «nei confronti dell'interessato» adoperata all'art. 5, par. 1, lett. *a*), Reg. UE n. 679/2016, sia da intendersi riferita all'ambito operativo del principio di trasparenza, il quale, per la sua fisionomia, non può avvincere l'attività dell'interessato: del resto, la differenza tra la precedente formulazione della norma e quella attuale sta proprio nell'addizione dell'inciso «trasparente nei confronti dell'interessato», che non si ritiene vada interpretato come volontà del legislatore unionale di limitare l'operatività dei principi di liceità e correttezza a vantaggio del solo interessato, restringendo il campo di applicazione degli stessi rispetto all'assetto previgente della normativa.

---

[62] Ribadito dalla Corte di giustizia europea, *Volker und Markus Schecke GbR* (C-92/09) e *Hartmut Eifert* (C-93/09) *c. Land Hessen*, sentenza del 9 novembre 2010, §49 ss. Piraino ridimensiona, correttamente, la portata della tecnica del bilanciamento di interessi nell'ambito della disciplina di settore *de quo* (F. PIRAINO, *Liceità e correttezza*, cit., p. 832 ss.) atteso che l'esistenza di un largo numero di norme preposte alla regolamentazione capillare delle fasi del rapporto giuridico interessato dalla normativa *privacy* non consente di discorrere, in accezione generale rivolgendosi al principio di correttezza, di operatività dello stesso quale criterio di bilanciamento in senso *tecnico*, il quale invece presuppone la tendenziale indipendenza dell'ambito elettivo dei diritti in conflitto, tal per cui questo sorge solo ove si verifichi una loro, finanche parziale, sovrapposizione.

[63] Accezione propria del principio, come si è visto nelle diverse versioni linguistiche del testo normativo. L'*aequitas*, storicamente collegata alla *bona fides*, in epoca romana assurgeva a criterio di valutazione della fattispecie in esame, dove l'applicazione più rigida del diritto cedeva il posto ad un'applicazione più flessibile e attagliata alle peculiarità del caso concreto, cfr. L. SOLIDORO MARUOTTI, *Aequitas e ius scriptum. Profili storici*, in *Annali della Facoltà Giuridica dell'Università di Camerino*, 2012, 1, p. 207 ss. Sull'equità, cfr. R. MARTINO, *Riflessioni preliminari sull'evoluzione storico-giuridica della nozione di equità come principio «in bianco»*, in F. RICCI (a cura di), *Princìpi, clausole generali, argomentazione e fonti del diritto*, Milano, 2018, p. 57 ss.; O. BUCCI, *Il principio di equità nella storia del diritto*, Napoli, 2000, *passim*.

[64] Cfr. GRUPPO DI LAVORO EX ART. 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, adottate il 3 ottobre 2017 e revisionate il 6 febbraio 2018, p. 10.

Altresì, non si ritiene che il principio in parola debba limitarsi all'attività *stricto sensu* di trattamento, al contrario di quanto potrebbe suggerire una lettura letterale della norma. Senza dubbio, la maggior parte dei principi raccolti nell'art. 5 GDPR ha una vocazione spiccatamente operativa e riferita a tale attività; tuttavia, è altrettanto pacifico che i principi di trasparenza e correttezza trovino applicazione anche nei riguardi di attività non strettamente rientranti nella definizione di trattamento data dall'art. 4, par. 1, n. 2, GDPR, in particolare la predisposizione dell'informativa, come del resto sottolineato dal Regolamento stesso al *considerando* n. 60. Appare più rispondente allo scopo della normativa, dunque, estendere l'ambito applicativo dei suddetti principi ad ogni attività posta in essere secondo le regole dettate dalla disciplina di settore e connessa al trattamento di dati personali; e non solo limitatamente a beneficio dell'interessato, bensì anche degli altri soggetti *privacy*, *ivi* inclusi il titolare e il rappresentante del trattamento.

2.3. Rilevanza dell'abuso del diritto in ambito privacy. Il problema della revoca del consenso

Nello scrutinare la clausola generale di correttezza quale termine di giudizio sostanziale *ex post* del rapporto che si instaura tra i soggetti coinvolti nell'operazione di trattamento, nonché come regola idonea a scandire *ex ante* i termini di esercizio dei diritti, non si può prescindere dall'esaminare l'estensibilità, *in subiecta materia*, della teorica del divieto di abuso del diritto[65], il quale implica un esercizio censura-

[65] Ricondotto alla buona fede in funzione valutativa. Sull'abuso del diritto, *ex multis*, cfr. M. Rotondi, *L'abuso del diritto*, in *Riv. dir. civ.*, 1923, p. 105 ss.; U. Natoli, *Note preliminari ad una teoria dell'abuso del diritto nell'ordinamento giuridico italiano*, in *Riv. trim. dir. proc. civ.*, 1958, 37 ss.; S. Romano, *Abuso del diritto*, in *Enc. dir.*, I, Milano, 1958, p. 168 ss.; D. Messinetti, *Abuso del diritto*, in *Enc. dir.*, *Aggiornamento*, II, Milano, 1998, p. 1 ss.; P. Rescigno, *L'abuso del diritto*, Bologna, 1998; S. Patti, *Abuso del diritto*, in *Dig. civ.*, I, Torino, 1987, p. 1 ss.; G. Pino, *Il diritto e il suo rovescio. Appunti sulla dottrina dell'abuso del diritto*, in *Riv. crit. dir. priv.*, 2004, 1, p. 25 ss.; Id., *L'abuso del diritto tra teoria e dogmatica (precauzioni all'uso)*, in G. Maniaci (a cura di), *Eguaglianza, Ragionevolezza e logica giuridica*, Milano, 2006, p. 115 ss.; M. Pompei, *L'abuso del diritto. Un approccio tra filosofia e teoria*, Torino, 2019; in V. Velluzzi (a cura di), *L'abuso del diritto. Teoria, storia e ambiti disciplinari*, Pisa, 2012, i seguenti saggi: M. Atienza-J. Ruiz Manero, *Abuso del diritto e diritti fondamentali*, p. 31 ss.; G. Cazzetta, *Responsabilità civile e abuso del diritto fra otto e novecento*, p. 51 ss. Sulla distinzione tra buona fede e abuso del diritto, cfr. F. Piraino, *La buona fede in senso oggettivo*, cit., p. 375 ss., e, più in generale, p. 354 ss. Autorevole dottrina, distinguendo tra le due figure, ha escluso la rilevanza del divieto di abuso del diritto in ambito contrattuale, all'interno del quale la buona fede svolge funzione prettamente integrativa, di contro individuandone il campo di elezione nell'ambito delle potestà e delle libertà, cfr. P. Rescigno, *L'abuso del diritto*, cit., p. 58, 86, 97 ss. Si rinviene la genesi di tale istituto nel canone di buona fede, pur distinguendone la natura e l'ambito applicativo: quest'ultima, difatti, costituisce il «precetto», il *prius* normativo, di cui il contrasto delle condotte connotate da violazione del divieto di abuso del diritto rappresenta solo una delle «funzioni», F. Piraino, *La buona fede in senso oggettivo*, cit., p. 381. Sull'abuso del processo, cfr. M. Taruffo, *L'abuso del processo: profili generali*, in *Riv. trim. dir. proc. civ.*, 2012, 1, p 117 ss.; M.F. Ghirga, *Abuso del processo e sanzioni*, Milano, 2012; A. Dondi, voce «*Abuso del processo (diritto processuale civile)*», in *Enc. dir.*, Ann. III, Milano, 2010, p. 1 ss.; V. Ansanelli, *Abuso del processo*, in *Dig. civ.*, Agg. III, I, Torino, 2007, p. 1 ss.

bile del diritto in un contesto di apparente rispetto della cornice formale nella quale lo stesso è di norma validamente azionabile.

Orbene, tale istituto è nato come rimedio *extra ordinem*, un "correttivo" di creazione dottrinale non esplicitamente previsto dall'ordinamento domestico, finalizzato a sopperire al vuoto di tutela derivante dall'esercizio improprio del diritto. Tuttavia, come già visto, a fronte della violazione del principio di correttezza nell'ambito di attività di trattamento dei dati personali, la normativa di settore appronta rimedi inibitori[66] e risarcitori[67], appropriandosi dell'ambito elettivo dell'abuso del diritto: difatti, da un lato, sebbene non ogni condotta contraria al principio di correttezza incarni un abuso del diritto, dall'altro è difficile immaginare un trattamento abusivo del diritto nei termini *supra* esposti che non integri una violazione del principio anzidetto. Tale assorbimento porta a ritenere che, quanto meno per tutte le attività

Rilevante, nella giurisprudenza di legittimità, Cass. civ, sez. un., sent. 18 settembre 2009, n. 20106; tra i vari commenti, si rimanda a A. GENTILI, *Abuso del diritto e argomentazione giuridica*, in *Resp. civ. prev.*, 2010, 2, p. 354 ss.; G. D'AMICO, *Recesso* ad nutum*, buona fede e abuso del diritto*, in *I contratti*, 2010, 1, p. 5 ss. In tale pronuncia, la Suprema Corte ha precisato gli elementi costitutivi dell'abuso del diritto, nella specie: «1) La titolarità di un diritto soggettivo in capo ad un soggetto; 2) la possibilità che il concreto esercizio di quel diritto possa essere effettuato secondo una pluralità di modalità non rigidamente predeterminate; 3) la circostanza che tale esercizio concreto, anche se formalmente rispettoso della cornice attributiva di quel diritto, sia svolto secondo modalità censurabili rispetto ad un criterio di valutazione, giuridico od extragiuridico; 4) la circostanza che, a causa di una tale modalità di esercizio, si verifichi una sproporzione ingiustificata tra il beneficio del titolare del diritto ed il sacrifico cui è soggetta la controparte»; cfr., sul punto, F. PIRAINO, *La buona fede in senso oggettivo*, cit., p. 372 ss. Dottrina successiva ha articolato una più analitica e precisa definizione di abuso del diritto: «L'azione A realizzata da un soggetto S nelle circostanze X è abusiva se e solo se: 1) Esiste una regola regolativa (con *regole regolative* gli AA. intendono quelle che ordinano, proibiscono o permettono una data condotta, cfr. *ivi*, p. 31; *n.d.a.*) che permette a S di realizzare A nelle circostanze X. Questa regola è un elemento del fascio di posizioni normative in cui si trova S come titolare di un certo diritto soggettivo. 2) Come conseguenza di A, un altro soggetto o altri soggetti soffrono un danno D, e non esiste una regola regolativa che proibisca di causare D. 3) D, tuttavia, appare come un danno ingiustificato perché si dà qualcuna delle seguenti circostanze: 3.1) Che, nel realizzare A, S non perseguiva altra finalità discernibile che causare D o che S realizzò A senza alcun fine serio e legittimo discernibile; 3.2) Che D è un danno eccesivo o anormale. 4) Il carattere ingiustificato del danno determina che l'azione A resti fuori dalla portata dei princìpi che giustificano la regola permissiva a cui si allude in 1) e che sorga una nuova regola che stabilisce che nelle circostanze X' (X più qualche circostanza che supponga una forma di realizzazione di 3.1) o di 3.2)) l'azione A è proibita», M. ATIENZA-J. RUIZ MANERO, *Abuso del diritto e diritti fondamentali*, cit., p. 33. Tale dottrina è germinata intorno alla categoria dell'"*illecito atipico*", sulla quale si rimanda a M. ATIENZA-J. RUIZ MANERO, *Illeciti atipici. L'abuso del diritto, la frode alla legge, lo sviamento di potere*, Bologna, 2004; F.D. BUSNELLI, *Illeciti atipici e il dibattito tra regole e principi*, in *Europa e diritto privato*, 2006, 3, p 1035 ss.; C. CASTRONOVO, *Abuso del diritto come illecito atipico?*, in *Europa e diritto privato*, 2006, 3, p. 1051 ss.; P. COMANDUCCI, *Abuso del diritto e interpretazione giuridica*, in V. VELLUZZI (a cura di), *L'abuso del diritto. Teoria, storia e ambiti disciplinari*, cit., p. 19 ss.; per una ricognizione delle posizioni critiche, cfr. M. POMPEI, *L'abuso del diritto. Un approccio tra filosofia e teoria*, cit., p. 121 ss.

[66] L'art. 2-*decies* d.lgs. 30 giugno 2003, n. 196, prevede l'inutilizzabilità dei dati personali raccolti in violazione della normativa di settore.

[67] L'art. 82, par. 1, GDPR, disciplina i profili risarcitori e il regime di responsabilità del titolare e del responsabile del trattamento nelle ipotesi di violazione, da parte di costoro alla violazione della normativa di settore

concernenti *sticto sensu* il trattamento di dati personali, l'espressa previsione di rimedi risarcitori e inibitori, in favore dell'interessato e nei confronti del titolare o del responsabile del trattamento, a fronte della violazione finanche dei principi *privacy*, sterilizzi il dibattito sull'ambito di applicazione dell'abuso del diritto ai trattamenti contrari a correttezza.

Tuttavia, tali strumenti di tutela sono posti esclusivamente a vantaggio dell'interessato. Occorre chiedersi, a tal punto della trattazione, se sia possibile, di converso, ipotizzare condotte abusive poste in essere dall'interessato stesso, esaminando, nello specifico, la configurabilità di un esercizio abusivo del diritto revoca del consenso al trattamento dei dati da parte dell'interessato. Occorre sottolineare che, nella normativa previgente, non essendovi espressa previsione del diritto di revoca, la dottrina, dopo averne ammesso l'esistenza, ne aveva contemperato l'esercizio apponendo limiti all'esercitabilità dello stesso, da rinvenirsi nella compromissione di interessi rilevanti di terzi in ragione della revoca[68], ammettendo l'esercizio valido del

[68] Cfr. F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 159; V. Cuffaro-V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, cit., p. 223; S. Patti, Commento *sub* art. 23, in *Commentario al d.lgs. 30 giugno 2003, n. 196*, cit., pp. 552-553. A tal proposito, si rammenta che autorevole dottrina, nel tentativo di giustificare i frequentissimi atti negoziali aventi come riferimento diritti della personalità, senza tuttavia infrangere il dogma dell'indisponibilità, ha parlato di «*parziale disponibilità*» degli stessi, consistente nella facoltà di acconsentire alla lesione, da parte dai beneficiari del consenso, del proprio diritto della personalità (cfr. A. De Cupis, *I diritti della personalità*, in A. Cicu, F. Messineo (diretto da), *Trattato dir. civ. comm.*, 2ª ed., Milano, 1982, p. 93); l'A., in tema di diritti sull'immagine personale, ha negato l'esercitabilità del potere di revoca nel caso in cui la pubblicazione di una raffigurazione si inserisca in un contratto, sulla scorta dell'incompatibilità di tale diritto con il regolamento contrattuale convenuto tra paciscenti (cfr. A. De Cupis, *I diritti della personalità*, cit., p. 299). Di contro, altra dottrina ritiene che il consenso all'utilizzazione commerciale della propria immagine sia sempre revocabile, fermo l'altrui diritti al risarcimento del danno quando il diritto sia esercitato secondo modalità abusive, utilizzando, a tal proposito, l'espressione «*abuso del diritto della personalità*», cfr. F. Galgano, *Trattato di diritto civile*, I, 3ª ed., Padova, 2014, p. 190; altresì, cfr. V. Di Nicola, *L'atto di disposizione del diritto all'immagine ha, dunque, natura non patrimoniale*, in *Contratto e impresa*, 2005, 2, p. 463 ss.; in giurisprudenza, cfr. Cass. civ., sent. 17 febbraio 2004, n. 3014, con nota di A. Albanese, *Immagine: lesione del diritto e consenso tacito allo sfruttamento commerciale*, in *Resp. civ.*, 2004, p. 112 ss.; Cass. civ., sent. 29 gennaio 2016, n. 1748. Più in generale, sulla circolazione dei diritti della personalità, G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 250 ss.
Tale questione si inserisce nell'ambito del perdurante e acceso dibattito dottrinale sulla natura giuridica del consenso al trattamento dei dati personali, individuandosi una prima tesi che ne rimarca la valenza "autorizzatoria" (cfr. F. Bravo, *Il commercio elettronico dei dati personali*, in *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 103 ss.; G. Votano, Commento *sub* art. 23, in Cirillo (a cura di), *Il codice sulla protezione dei dati personali*, Milano, 2004, p. 134; D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 351 ss.), sulla scorta dei caratteri di assolutezza, indisponibilità, intrasmissibilità e imprescrittibilità dei diritti della personalità (su tali caratteri, cfr. V. Zeno Zencovich, voce «*Personalità (diritti della)*», in *Digesto civ.*, XIII, Torino, 1995, p. 430 ss.) e una seconda che gli attribuisce valenza «negoziale» o dispositiva (cfr. V. Zeno Zencovich, voce «*Cosa*», in *Digesto civ.*, IV, Torino, 1989, par. 13; Id., *Sull'informazione come «bene» (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv.*, 1999, p. 485 ss.; G. Oppo, *Sul consenso dell'interessato*, in V. Cuffaro-V. Ricciuto-V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1999, p. 125; in ambito di diritti sull'immagine personale, A. De Cupis, *I diritti della personalità*, cit., p. 299. Nega espressamente il carattere indisponibile dei diritti della personalità A. Galasso,

diritto solo ove, in presenza di tali interessi concorrenti, fosse supportato da *giustificati motivi*[69], andando all'uopo anche a individuare, sulla scorta di tali premesse, limiti temporali all'esercizio di tale diritto[70].

A seguito dell'avvicendamento normativo, il consenso, quale presupposto legittimante il trattamento, ha perduto il ruolo di preminente centralità che rivestiva, talché deve ritenersi che il diritto di revoca dello stesso, ai sensi dell'art. 7, par. 3, GDPR, sia esercitabile *ad nutum*, nei casi in cui il trattamento trovi il suo fondamento giuridico nell'art. 6, comma 1, lett. *a*), GDPR[71], posto che, a differenza della normativa previgente, il legislatore, nell'art. 6, comma 1, GDPR, ha operato *ex ante* il bilanciamento di interessi a tutela dei quali erano stati suggeriti limiti al potere di revoca, prevendo espressamente quali trattamenti fossero suscettibili di essere caducati dall'esercizio del diritto di revoca «in qualsiasi momento»[72].

Ciò non di meno, l'assioma di libera revocabilità non esclude in radice la configurabilità di un esercizio abusivo del diritto di revoca. Tala questione acquisisce rilievo alla luce della nuova disciplina europea sui contratti di fornitura di contenuti e servizi digitali, direttiva 2019/770/UE, recepita con il d.lgs. 4 novembre 2021, n. 173[73], la quale ha previsto espressamente, all'art. 3, par. 1, confluito nell'art. 135-*octies*, co. 4, c.cons., l'ipotesi di somministrazione di servizi o contenuti digitali a fronte della "fornitura" di dati personali all'operatore economico, il quale è autorizzato a trattarli per fini diversi dalla mera prestazione del servizio; si rileva, per fugare ogni dubbio, che tali dati non sono trattati *ex* art. 6, par. 1, lett. *b*), GDPR[74], dacché, in tal caso, l'esercizio del diritto di revoca non sarebbe consentito[75]. Intorno a tale novità normativa si è riacceso il dibattito sulla natura del consenso e, in particolare, sulla

Diritto civile e relazioni personali, in *Dem. dir.*, 1996, 1, p. 253). Per una approfondita ricognizione delle differenti posizioni, cfr. F. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 15 ss., in particolare note a piè di pagina nn. 19-20; F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 135 ss., note note a piè di pagina nn. 55-57. Il dibattito si ripresenta in termini simili nell'ambito del diritto sull'immagine personale, per il quale si rimanda a M. PROTO, *Il diritto e l'immagine*, Milano, 2012, p. 171 ss.

69 Subordinava l'esercizio del diritto revoca alla sussistenza della «giusta causa», nei casi in cui fosse insorto un legittimo interesse al trattamento in capo al titolare, G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in U. BRECCIA-L. BRUSCUGLIA-F.D. BUSNELLI (a cura di), *Il diritto privato nel prisma dell'interesse legittimo*, Torino, 2001, p. 42 ss.; similmente, cfr. S. PATTI, Commento *sub* art. 11, in *Commentario alla L. 31 dicembre 1996, n. 675*, cit., p. 364.

70 Cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., p. 1041 ss.

71 Così F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 159.

72 Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 160.

73 Per un estensivo commento del recepimento, cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135* octies-*135* vicies ter *c.cons. La nuova disciplina dei contratti b-to-c per la fornitura di contenuti e servizi digitali*, in *Le nuove leggi civili commentate*, 2022, 6, p. 1499 ss.; v. pure V. VERSACI, *Il valore negoziale dei dati personali del consumatore: spigolature sul recepimento della direttiva 2019/770/UE in una prospettiva comparata*, in E. CREMONA-F. LAVIOLA-V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022, p. 155 ss.

74 Cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1511 ss.

75 Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 160-161.

patrimonializzazione dei dati personali[76]. Secondo un primo orientamento, il dato personale non può essere direttamente oggetto di atti dispositivi negoziali, appartenendo questi alla sfera dei diritti della personalità: ciò che viene "patrimonializzato", al contrario, è l'*atto autorizzatorio al trattamento*. Tale tesi trova conforto, nel caso di specie, anche nel *considerando* n. 24 della direttiva in questione, che recita: «la protezione dei dati personali è un diritto fondamentale e (i) dati non possono dunque essere considerati una merce». La tesi opposta, invece, parte dal dato empirico dell'oggettivo valore economico attribuibile ai dati personali, quotidianamente oggetto di "scambio" e trattamenti a fini commerciali, e che il trattamento di questi costituisca precipuamente la controprestazione, nella fattispecie in esame.

Tanto premesso, è ragionevole chiedersi se in siffatti contratti, a fronte della prestazione erogata dalla società fornitrice del servizio o contenuto digitale e all'impegno di fornire i propri dati personali, l'esercizio del diritto di revoca del consenso si distorca nel mezzo con cui una parte – il consumatore – possa *arbitrariamente* nullificare la propria controprestazione, andando a squilibrare il sinallagma contrattuale[77]. Invero, l'antinomia si rinviene a livello normativo: da un lato l'art. 135-*octies*, co. 4, c. cons, esplicitamente consente la somministrazione di contenuti e servizi digitali a fronte di un trattamento ulteriore di dati personali, non necessario per l'erogazione della prestazione; dall'altro l'art. 7 GDPR, nonché il *considerando* n. 43, impongono il più ampio grado di libertà nella prestazione del consenso e nella revoca dello stesso, tenendo *nella massima considerazione* l'eventualità che la prestazione di un servizio sia subordinata alla prestazione al consenso al trattamento di dati non necessario all'esecuzione del contratto[78]. La contraddittorietà delle norme è evidente, in quanto l'ultima si preoccupa di cautelare l'interessato da trattamenti di dati *superflui* ai fini dell'erogazione di un servizio, l'altra esplicitamente li prevede, dunque, se non incoraggiando, quanto meno agevolando l'utilizzo del dato personale come posta contrattuale suscettibile di valutazione economica[79]. Spetta all'interprete l'ingrato compito di armonizzare le dissonanze del legislatore europeo.

---

[76] Rilevanti, sul tema, le posizioni di F. Bravo, *Il commercio elettronico dei dati personali*, in *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 113 ss.; Id., *La «compravendita» di dati personali?*, in *Diritto di internet*, 2020, 3, p. 531 ss. Id., *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, p. 34 ss.; A. De Franceschi, *Il "pagamento" mediante dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 1381 ss.

[77] Dunque, l'ipotesi in oggetto è quella di consenso *condizionale*, senza il quale il contratto non può essere concluso, e non quella di consenso *opzionale*, nel quale la revoca del consenso certamente non incide – proprio in forza dell'eventualità dello stesso – sul vincolo contrattuale o sull'equilibrio delle prestazioni, qualificando di conseguenza la fornitura come *gratuita*. Cfr. S. Pagliantini, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1514 ss.

[78] Cfr. Gruppo di lavoro ex art. 29, *Guidelines on consent under Regulation 2016/679*, WP 259 rev. 01, adottate il 28 novembre 2017 e aggiornate il 10 aprile 2018, *passim*.

[79] A tal proposito, dottrina ha suggerito un'interpretazione evolutiva del concetto di «prezzo» ai fini della disciplina consumeristica di cui alla direttiva 2011/83/UE, ricomprendendovi ogni prestazione suscettibile di un valore economico, cfr. A. De Franceschi, *Il "pagamento" mediante dati personali*, cit., p. 1391.

Opportunamente, il legislatore tedesco ha previsto, al § 327q BGB, che l'esercizio dei diritti dell'interessato in materia di protezione dei dati personali non incide sulla validità del vincolo contrattuale, accordando di converso al professionista, in caso di revoca del consenso od opposizione al trattamento idonea a squilibrare il sinallagma contrattuale, il potere di recedere dai contratti di durata; infine, è espressamente esclusa la facoltà del professionista di chiedere il risarcimento del danno nel caso di esercizio dei diritti anzidetti. Il legislatore domestico, in sede di recepimento, ha omesso di inserire una norma volta a regolamentare la sorte del contratto nell'ipotesi di esercizio del diritto di revoca del consenso al trattamento, nonostante il primo inciso del *considerando* n. 15 della direttiva in oggetto, riprendendo il principio insito nel brocardo «*inadimplenti non est adimplendum*», sancisce che «Gli Stati membri dovrebbero inoltre mantenere la facoltà, ad esempio, di regolamentare i diritti delle parti di astenersi dall'adempiere gli obblighi o parte di essi finché l'altra parte non abbia adempiuto i propri obblighi»; parimenti, si rileva che la revoca del consenso al trattamento ulteriore dei dati non può in alcun modo essere assimilata all'esercizio del diritto di risoluzione[80] di cui all'art. 15 dir. 2019/770/UE, giustificante l'interruzione della fornitura di servizi o contenuti digitali, in ragione dello scioglimento del vincolo negoziale.

In dottrina sono state proposte diverse proposte volte a sciogliere tale nodo[81]: taluni hanno suggerito che la revoca del consenso possa essere considerata causa di parziale impossibilità sopravvenuta della prestazione *ex* 1464 c.c., sebbene tale assunto si scontri con la considerazione che l'impossibilità sopravvenuta deve essere *non imputabile*; si è sostenuto, dunque, che, nei contratti di durata, il professionista possa recedere[82], con effetto non retroattivo, a fronte della revoca del consenso al trattamento ulteriore, in forza del richiamo, operato dall'art. 135-*vicies ter*, alle regole in punto di «formazione, validità ed efficacia dei contratti, comprese le conseguenza della risoluzione del contratto e il diritto al risarcimento del danno». Si è giustamente obiettato, tuttavia, che, al pari della normativa tedesca, un tale esercizio del diritto di recesso debba tenere conto degli interessi delle parti[83] – in conformità, dunque, del canone di buona fede –, sicché lo stesso non potrà esercitato se la revoca non abbia comportato un apprezzabile squilibrio tra le prestazioni, attribuendo al

[80] A tal proposito, la disciplina dell'obbligazione restitutoria gravante sull'operatore economico di cui all'art. 135-*noviesdecies*, co. 1-2, c.cons., di entità inversamente proporzionale alle prestazioni legittimamente offerte dal professionista e godute dal consumatore, è reminiscente della disciplina del diritto di recesso di cui all'art. 1373, co. 2, c.c., per il quale si rimanda a E. RAVERA, *Il recesso*, Milano, 2004, *passim*.

[81] Cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1524 ss.; V. VERSACI, *Il valore negoziale dei dati personali del consumatore*, cit., p. 163 ss.

[82] Cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1524; T.M. UBERTAZZI, *Ripensando alla revoca del consenso nella prospettiva funzionale della* privacy, in *Contratto e impresa*, 2022, 2, p. 49 ss. V. pure, sul diritto di recesso nei contratti a esecuzione continuata o periodica, C.M. BIANCA, *Diritto civile*, 3, *Il contratto*, 3ª ed., Milano, 2019, p. 699 ss.; F. GALGANO-G. VISINTINI, *Degli effetti del contratto. Della rappresentanza. Del contratto per persona da nominare. Art. 1372-1405*, *sub* art. 1373, in F. GALGANO (a cura di), *Commentario del Codice civile Scialoja-Branca*, Bologna-Roma, 1993, p. 62 ss.

[83] Cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1525.

consumatore utilità ben più pregnanti, finanche permanenti, rispetto a quelle che il professionista ha potuto trarre dal trattamento di dati personali.

Ci si chiede, dunque, se un tale esercizio dei diritti attribuiti dal GDPR, preordinato a svuotare di ogni concretezza e valore la controprestazione consistente nella fornitura di dati personali, possa essere ritenuto contrario a buona fede, nonostante, ai sensi della normativa posta a tutela dei dati personali, il consenso sia sempre revocabile *ad nutum*.

In primo luogo, occorre qualificare l'atto di revoca del consenso od opposizione al trattamento nel quadro del contratto in cui si innesta. La formulazione dell'art. 135-*octies*, par. 4, c.cons., facendo riferimento alla circostanza che il consumatore «fornisce o si obbliga a fornire», sembra suggerire esplicitamente la qualificazione di tale fornitura quale controprestazione contrattuale, con la precisazione che oggetto della stessa non sono i dati in sé, bensì l'atto autorizzatorio al trattamento, nella specie, dunque, il consenso[84]. Occorre poi procedere a coordinare l'art. 7, par. 4, GDPR, con l'art. 135-*novies*, co, 6, c.cons. Ad oggi non si dubita, anche in ragione di recenti pronunce della Corte di legittimità sul punto, della possibilità di convenire il trattamento di dati personali quale posta contrattuale[85]; tale facoltà, tuttavia, deve conciliarsi con quanto sancito dalla normativa di settore[86], tale per cui, ad esempio, non si riterrà libero il consenso prestato per un servizio di natura *infungibile* e *irrinunciabile*[87]. Ne consegue, dunque, che la disciplina introdotta dalla direttiva in oggetto possa trovare applicazione solo per rapporti contrattuali dove l'offerta di servizi sia *fungibile* e dove la revoca del consenso non comporti un pregiudizio per l'interessato, pena violare il principio di libertà di revoca del consenso al trattamento *ex* art. 7 GDPR.

In conclusione, sembra potersi sostenere che la revoca del consenso costituisca, a tutti gli effetti, inadempimento, idoneo a legittimare la domanda di risoluzione del contratto e di risarcimento del danno[88] *ex* art. 1453 c.c. del professionista[89], ovvero il summenzionato recesso. Occorre tuttavia rilevare che la prospettiva di esporsi ad un'azione risarcitoria sembrerebbe rendere l'esercizio del diritto affatto agevole

---

[84] Cfr. F. Bravo, *Il commercio elettronico dei dati personali*, cit., pp. 118-119; Id., *Lo "scambio di dati personali nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto"*, cit., p. 44 ss.

[85] Cfr. Cass. civ., sent. 2 luglio 2018, n. 17278.

[86] È espressamente chiarito, al *considerando* n. 39 della direttiva 2019/770/UE, che «Il diritto alla cancellazione e il diritto del consumatore di revocare il consenso al trattamento dei dati personali dovrebbero applicarsi pienamente anche in relazione ai contratti disciplinati dalla presente direttiva».

[87] Cfr. F. Bravo, *Il commercio elettronico dei dati personali*, cit., p. 114, 117.

[88] Danno da quantificarsi nel valore economico del godimento dei servizi e contenuti di cui il consumatore si sia giovato in difetto di controprestazione consistente nella fornitura di dati.

[89] Estensivamente, sulla questione, cfr., G. Resta, *Autonomia privata e diritti della personalità*, cit., p. 250 ss.; esclude la possibilità di agire per l'adempimento, non essendo coartabile la prestazione del consenso al trattamento dei dati personali, afferendo tale situazione ai diritti della personalità, D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., p. 355. Si rileva che, nella disciplina in esame, la dottrina continua ad interrogarsi su aspetti più di dettaglio su cui la normativa tace, come l'eventuale l'integrazione del prezzo nei casi in cui il consenso al trattamento opzionale revocato fosse prestato per ottenere uno sconto sul prezzo, cfr. S. Pagliantini, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1555 ss.

e libero, ponendo piuttosto il consumatore in una condizione peggiore rispetto a quella originaria, in quanto costretto a corrispondere denaro invece che dati personali[90], andando a concretare quel pregiudizio che assume primario rilievo fra i canoni di giudizio della libertà di revoca del consenso[91]. Non si può parimenti ignorare, tuttavia, la consapevolezza del consumatore, al momento della conclusione del contratto, della natura di controprestazione del consenso prestato e del valore delle utilità percepite in ragione del contratto di fornitura: e se funzione della tutela risarcitoria non è quella di arricchire il danneggiato, bensì collocarlo nella «stessa curva di indifferenza in cui si sarebbe trovato se non avesse subito l'illecito»[92], allora non può parlarsi propriamente di *pregiudizio*, essendo l'onerato tenuto a corrispondere in denaro quanto egli avrebbe dovuto prestando il consenso. A voler ritenere altrimenti, in assenza di una norma eccezionale del medesimo tenore del § 327q, Abs. 3, BGB, difatti, dovrebbe ritenersi contrario all'art. 135-*novies*, co. 6, c.cons., e dunque nullo *ex* art. 1418, co. 1, c.c., il contratto avente ad oggetto, a fronte della necessaria prestazione del consenso al trattamento, la fornitura di contenuti e servizi digitali dotati di apprezzabile valore economico e idonei ad esporre il consumatore a pretese risarcitorie da parte del professionista, sostanzialmente limitando il campo d'applicazione della direttiva alle ipotesi di consenso opzionale nelle forniture gratuite, frustrando, tuttavia, la vera ragion d'essere della normativa, che risulta invero superflua, se volta a normare solo tale fattispecie. A livello sistematico, peraltro, così sono trattate in egual modo le ipotesi di trasmissione di dati inveritieri[93], in relazione alla quale, fuori dall'ipotesi di consenso del tutto opzionale, si ritiene che il consumatore risponda a titolo d'inadempimento, e quelle di revoca del consenso nei contratti non gratuiti.

Sembra dunque che, in tale ricostruzione, non vi sia spazio per la teorica dell'abuso del diritto, essendo gli strumenti approntati dall'ordinamento idonei a soddisfare le esigenze in cui tale istituto viene in rilievo. Risulta così scongiurata l'ipotesi di un esercizio *abusivo* dei diritti attribuiti all'interessato dal Regolamento: in ragione del doppio piano di operatività della fattispecie, a livello giuridico, l'esercizio libero del diritto di revoca è del tutto legittimo sul piano della normativa *privacy*; lo stesso, tuttavia, costituisce violazione del programma contrattuale e, di conseguenza, inadempimento[94], nei contratti di fornitura dove il consenso al trattamento costituisce la controprestazione convenuta.

---

[90] Cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., pp. 1525-1526.

[91] GRUPPO DI LAVORO EX ART. 29, *Guidelines on consent under Regulation 2016/679*, cit., p. 5.

[92] Cass. civ., 11 luglio 1978, n. 3507.

[93] Cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1555 ss.

[94] Invero, l'esistenza di una norma che escluda testualmente il risarcimento del danno o meglio, a valle, l'inadempimento del consumatore (cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE*, cit., p. 1523 ss.), nell'ipotesi di esercizio del diritto di revoca, avrebbe permesso di riproporre le considerazioni *supra* esposte nella chiave di violazione del dovere di buona fede *in executivis ex* art. 1375 c.c. e, dunque, fuori dal campo d'azione del principio di correttezza della normativa sulla tutela dei dati personali.

2.4. Correttezza e modalità operative

La vocazione *concreta* del Regolamento fa sì che sia riservato ampio spazio alla esplicazione puntuale di procedure e modalità operative che debbono essere adottate al fine di garantire il rispetto della normativa in oggetto, in particolare dei principi. In tale contesto, la correttezza si interseca con altri principi del GDPR, strettamente inerenti a tali modalità operative del trattamento, assurgendo a metro di giudizio dell'appropriatezza delle procedure adottate nell'attività di trattamento. A tal proposito, non può che ritenersi contrario a correttezza e buona fede un trattamento posto in essere con modalità non trasparenti[95], ovvero trattando dati non esatti[96], eccedenti e non pertinenti alle finalità del trattamento[97], con modalità tali da non garantirne l'integrità[98] o da consentire l'identificazione dell'interessato per un arco di tempo superiore al conseguimento delle finalità per le quali i dati sono trattati[99]. La correttezza, nelle sue normali esplicazioni, comprende tutte ipotesi che, forse con eccesso di zelo, sono state esplicitamente normate dal legislatore[100]: fanno eccezione il principio di limitazione delle finalità[101] e il principio di responsabilizzazione[102], dei quali si parlerà nel prosieguo. In considerazione di quanto esposto, non sembra possibile attribuire alcun pregio sistematico alla collocazione del principio di trasparenza di seguito a quello di liceità e quello di correttezza[103]. Difatti, né la trasparenza può assurgere ad esplicazione operativa per antonomasia, né le si può attribuire un particolare rilievo sistematico rispetto agli altri principi afferenti alle modalità operative del trattamento, essendo tutti eguali corollari specifici del principio di correttezza. Tuttavia, la particolare importanza *concreta* che l'obbligo di trasparenza assume, all'interno dell'attività di trattamento, ha, si suppone, persuaso il legislatore ad attribuire a tale principio una collocazione privilegiata.

Invero, il collegamento tra correttezza e trasparenza era già chiaro al legislatore europeo del '95, essendo sancito, al *considerando* n. 38 dir. 95/46/CE, al fine di poter trattare i dati personali secondo correttezza, «che le persone interessate (potessero) conoscere l'esistenza del trattamento e disporre, quando i dati che le riguardano sono forniti direttamente da loro, di un'informazione effettiva e completa in merito alle circostanze della raccolta». Parimenti, le linee guida sulla trasparenza redatte dall'ormai sciolto Gruppo di lavoro *ex* art. 29[104] si riferiscono al principio di

[95] Cfr. art. 5, par. 1, lett. *a*), GDPR.
[96] Cfr. art. 5, par. 1, lett. *d*), GDPR.
[97] Cfr. art. 5, par. 1, lett. *c*), GDPR.
[98] Cfr. art. 5, par. 1, lett. *f*), GDPR.
[99] Cfr. art. 5, par. 1, lett. *e*), GDPR.
[100] Dottrina in commento al Codice *privacy ante* riforma aveva già rilevato come il «principio di necessità», positivizzato all'ormai abrogato art. 3 d.lgs. n. 196 del 2003 e oggi ricondotto al principio di minimizzazione, fosse null'altro che esplicazione del più generale obbligo di correttezza nel trattamento dei dati personali, cfr. F. Piraino, *Liceità e correttezza*, cit., p. 855.
[101] Cfr. art. 5, par. 1, lett. *b*), GDPR.
[102] Cfr. art. 5, par. 2, GDPR.
[103] Cfr. art. 5, par. 1, lett. *a*), GDPR. Altresì, il *considerando* n. 39 fa riferimento a liceità, correttezza e trasparenza, ma disgiungendo, a livello sintattico, quest'ultima nozione dalle prime due.
[104] Gruppo di lavoro ex art. 29, *Guidelines on transparency under Regulation 2016/679*, WP 260, adottate il 29 novembre 2017 e revisionate l'11 aprile 2018, pp. 4-5.

trasparenza come *espressione*[105] del principio di correttezza di cui all'art. 8, co. 2, della Carta dei diritti fondamentali dell'Unione europea; più nettamente, il Gruppo di lavoro rimarca come l'uso di formule dubitative come "forse", "spesso" etc. nelle informazioni rese all'interessato possa essere indice di violazione del principio di *correttezza*[106], e non, più precisamente, del principio di *trasparenza*[107]. La trasparenza, come si evince nei *considerando* nn. 39 e 60 del GDPR, ben più analitici dei predecessori, si esplica in obblighi informativi, comunicativi e collaborativi a carico del titolare del trattamento, il quale avrà cura fornire le informazioni in modo *completo*, *chiaro*, *facilmente accessibile* e *comprensibile*; fine della previsione di obblighi informativi così puntualmente individuati è tutelare l'interessato da condotte decettive del titolare del trattamento.

Le regole ricavabili dai principi *operativi* sopra citati, *ivi* compresa la trasparenza, concorrono a formare quella che è stata definita come la «correttezza procedurale»[108], ovverosia quell'insieme di disposizioni volte a implementare i principi di *protezione dei dati fin dalla progettazione* e *protezione dei dati per impostazione predefinita*[109] e a disciplinare in modo granulare, dal punto di vista procedurale e operativo, i momenti di interazione tra titolare e interessato del trattamento. Del rispetto di tali modalità operative è onerato il titolare del trattamento stesso in ragione dell'art. 5, par. 2, il quale, in combinato con l'art. 82 GDPR, funge da criterio di allocazione della responsabilità[110], in considerazione dei larghi ambiti di discrezionalità del titolare del trattamento nel determinare le misure più appropriate per tutelare i diritti dell'interessato e garantire il rispetto della normativa di settore, e della posizione di genetica debolezza in cui giace l'interessato, tenuto conto della strutturale asimmetria dell'attività di trattamento dei dati personali.

---

[105] Il termine originale inglese adoperato è «*expression*».

[106] GRUPPO DI LAVORO EX ART. 29, *Guidelines on transparency under Regulation 2016/679*, cit., pp. 9-10.

[107] Cfr. GRUPPO DI LAVORO EX ART. 29, *Guidelines on transparency under Regulation 2016/679*, cit., p. 9.

[108] In originale, «*procedural fairness*» o «*procedural justice*». Tali espressioni sono state concepite e adoperate nello studio dell'omonima disciplina, di spiccata vocazione sperimentale, posta a metà tra sociologia e diritto, concernente la correttezza e giustizia sostanziale delle procedure volte a comporre controversie di diversa natura, cfr. J. THIBAUT-L. WALKER, *Procedural Justice: A Psychological Analysis*, Hillsdale, NJ: Lawrence Erlbaum Associates, 1975; E.A. LIND-T.R. TYLER, *The Social Psychology of Procedural Justice*, New York: Plenum, 1988; tali riflessioni sono state poi declinate in plurimi ambiti, incluso quello relative alla tutela dei dati personali, cfr. R.J. BIES, *Privacy and Procedural Justice in Organizations*, in *Social Justice Research*, 1993, 1, p. 69 ss.; E.F. STONE-D.L. STONE, *Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms*, in *Research in Personnel and Human Resources Management*, 1990, 8, p. 349 ss.; M.J. CULNAN, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, in *Organization Science*, 1999, 1, p. 104 ss.; D. CLIFFORD-J. AUSLOOS, *Data protection and the Role of Fairness*, cit., pp. 160, 162 ss.

[109] Cfr. art. 25 GDPR.

[110] Cfr. M. RATTI, *La responsabilità da illecito trattamento dei dati personali*, cit., p. 777 ss.; E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contratto e impresa*, 2020, 3, p. 1115 ss.

2.5. Regole deontologiche e codici di condotta

Secondo l'art. 2-*quater*, co. 4, d.lgs. 30 giugno 2003, n. 196[111], costituisce condizione essenziale, ai fini della valutazione della conformità del trattamento ai principi di liceità e correttezza, il rispetto delle regole deontologiche emanate ai sensi del primo comma dell'art. *de quo*[112]. Le regole deontologiche sono volte a dettare disposizioni ulteriori conformative dell'attività di trattamento in specifici settori, le cui peculiarità o rilievo sociale, tecnico o economico li rende meritevoli di attività regolatoria più specifica; non è un caso che, a tal fine, sia stato adoperato lo strumento delle regole deontologiche, il quale costituisce fonte di autoregolamentazione di formazione negoziale proveniente dai soggetti stessi cui tali regole si rivolgono[113].

Le regole deontologiche vengono tradizionalmente ricondotti nella categoria della *soft law*[114], traducibile come «legge debole», tradizionalmente caratterizzata dalla *non vincolatività*[115], la quale, tuttavia, non implica la non idoneità a produrre effetti giuridici[116]. Invero, già a far data dalla normativa previgente, la dottrina aveva espresso perplessità sull'incasellamento, nella gerarchia delle fonti, del fenomeno in oggetto[117] – posizione confortata dal Garante stesso, il quale nella Relazione al Parlamento del 2001 ha precisato come il «codice deontologico e di buon condot-

[111] Tale disposizione non costituisce un *novum* introdotto dal d.lgs. 10 agosto 2018, n. 101, dacché il dettato normativo ricalca quello dell'abrogato art. 12, co. 3, d.lgs. 30 giugno 2003, n. 196, talché la produzione dottrinale in commento alla normativa previgente risulta pienamente attuale; si rileva, peraltro, una sostituzione terminologica, avendo il legislatore ribattezzato come «regole deontologiche» i precedenti «codici di deontologia e buona condotta», per evitare confusione lessicale con i «codici di condotta» disciplinati dagli artt. 40 ss. GDPR. Sulla materia, si segnalano i seguenti contributi: G. Pino, *I codici di deontologia nella normativa sul trattamento dei dati personali*, in *Danno e responsabilità*, 2002, 4, p. 363 ss.; F. Bravo, *Regole generali applicabili a tutti i trattamenti di dati personali*, in J. Monducci-G. Sartor (a cura di), *Il Codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003 n. 196*, Padova, 2004, pp. 35-80 e, *ivi*, spec. il par. 3, a p. 50 ss., intitolato proprio «*Codici di deontologia e di buona condotta*»; G. De Minico, Commento *sub* art. 12, in C.M. Bianca-F.D. Busnelli (a cura di), *Commentario al d.lgs. 30 giugno 2003, n. 196 ("Codice della* privacy*")*, cit., p. 271 ss.; S. Sileoni, *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Padova, 2011; A.R. Popoli, *Codici di condotta e certificazioni*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, cit., p. 527 ss.; R. D'orazio, Commento *sub* art. 2-*quater*, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta, *Codice della privacy e data protection*, cit., p. 1026 ss., cui si rimanda per la bibliografia essenziale.

[112] Invero, fuori dall'ambito della tutela dei dati personali, la giurisprudenza già ritiene il mancato rispetto dei codici di condotta e autodisciplina elemento significativo ai fini della valutazione del rispetto degli obblighi di correttezza professionale *ex* art. 2598, co. 3, c.c., cfr. Cass. civ., sent. 15 febbraio 1999, n. 1259, in *Foro It.*, 1999, 9, p. 2572 ss.; Corte d'appello di Milano, sent. 30 luglio 1999, in *Dir. ind.,* 2000, p. 141 ss.

[113] F. Bravo, *Regole generali applicabili a tutti i trattamenti di dati personali*, cit., p. 50.

[114] A.R. Popoli, *Codici di condotta e certificazioni*, cit., pp. 530-531. Su tale categoria, cfr. E. Mostacci, *La* soft law *nel sistema delle fonti*, Padova, 2008, spec. p. 130 ss.; A. Somma (a cura di), *Soft law e hard law nelle società post-moderne*, Torino, 2009.

[115] Cfr. E. Mostacci, L*a* soft law *nel sistema delle fonti*, cit., p. 17 ss.

[116] Cfr. E. Mostacci, L*a* soft law *nel sistema delle fonti*, cit., p. 37 ss.

[117] Cfr. F. Bravo, *Regole generali applicabili a tutti i trattamenti di dati personali*, cit., p. 50 ss.; J. Monducci, *Diritti della persona e trattamento dei dati particolari*, Milano, 2003, p. 61 ss.

ta riguardante il trattamento dei dati personali effettuato nell'ambito dei servizi di comunicazione e informazione offerti per via telematica (...) non avrà valore di una qualunque altra disposizione di carattere deontologico, ma assumerà la veste di una vera e propria fonte dell'ordinamento generale, come si evince dal fatto che il rispetto delle disposizioni in esso contenute costituirà condizione essenziale per la liceità del trattamento dei dati»[118]. Uno degli effetti tipici della *soft law* è quello di considerare lecita la condotta conforme alle regole deboli senza che, tuttavia, la non osservanza delle stesse costituisca un illecito; al contrario, nel caso di specie, il rispetto delle regole deontologiche è condizione di liceità per i trattamenti verso cui tali regole si rivolgono. Il carattere peculiare delle stesse, tale da farle assurgere a rango di fonte *atipica* dell'ordinamento giuridico[119], si rinviene, tra le altre, nel fatto che le stesse contengono disposizioni che derogano[120] alle norme contenute nel GDPR e nel Codice *privacy*[121], nonché nel fatto che sono oggetto di pubblicazione nella Gazzetta Ufficiale[122]. Di contro, la tipica non vincolatività della *soft law* si rinviene precipuamente nei codici di condotta di cui agli artt. 40 ss. GDPR, la cui adozione da parte del titolare o del responsabile del trattamento (artt. 24, comma 3, e 28, par. 5, GDPR) è utile ai fini della prova che il trattamento sia conforme alla normativa[123].

Le regole deontologiche sembrano dunque sintetizzare la dialettica dei principi di liceità e correttezza esposta nei paragrafi precedenti, provvedendo a disciplinare in modo formale determinate attività di trattamento, contestualmente delineando il novero di significati attribuibili al principio di correttezza nell'ambito di specifiche

[118] GPDP, *Relazione 2001*, Roma, 2002, p. 89.

[119] In relazione al codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (emanate con provvedimento del Garante del 29 luglio 1998, pubblicate in Gazzetta Ufficiale del 3 agosto 1998, n. 179), Simoncini ritiene che «ci troviamo in presenza non di una norma di autodisciplina tipica di un ordinamento interno, quanto di una fonte secondaria atipica dell'ordinamento statale», A. SIMONCINI, *Codici deontologici di protezione dei dati personali nel sistema delle fonti. L'emersione di un nuovo «paradigma» normativo?*, in *Osservatorio sulle fonti*, Torino, 1999, p. 292; similmente, J. MONDUCCI, *Diritti della persona e trattamento dei dati particolari*, cit., p. 62; E. MOSTACCI, L*a* soft law *nel sistema delle fonti*, cit., p. 159 ss.; G. DE MINICO, *Commento* sub *art. 12*, cit., p. 272 ss.; S. SILEONI, *Autori delle proprie regole*, cit., p. 234 ss.; tale tratto trova conforto, in ragione della continuità tra i previgenti codici di condotta e le nuove regole deontologiche, anche nell'assetto normativo attuale, cfr. R. D'ORAZIO, *Commento sub art. 2*-quater, cit., p. 1033-1035; A.R. POPOLI, *Codici di condotta e certificazioni*, cit., pp. 532-533.

[120] Cfr. E. MOSTACCI, *La* soft law *nel sistema delle fonti*, cit., p. 150.

[121] Cfr. art. 12, co. 1, Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica, pubblicate in Gazzetta Ufficiale del 4 gennaio 2019, n. 3: «Al trattamento dei dati relativi a procedimenti penali non si applica il limite previsto dall'art. 10 del Regolamento, nonché dall'art. 2-octies del Codice».

[122] Cfr., J. MONDUCCI, *Diritti della persona e trattamento dei dati particolari*, cit., pp. 64-65; F. BRAVO, *Regole generali applicabili a tutti i trattamenti di dati personali*, cit., p. 51.

[123] Cfr. S. SILEONI, *Commento* sub *artt. 40-41*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA, *Codice della privacy e data protection*, cit., p. 595 ss.; EDPB, *Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679*, v. 2, 4 giugno 2019. In generale, su tali forme di autoregolazione, cfr. G. ALPA-P. ZATTI (a cura di), *Codici deontologici e autonomia privata*, Milano, 2006; N. LIPARI, *Fonti del diritto e autonomia dei privati (spunti di riflessione)*, in *Riv. dir. civ*., 2007, 1, p. 727 ss.; N. BRUTTI, voce «*Codici di comportamento: a) profili generali*», in *Enc. dir.*, *Annali*, VI, Milano, 2013, p. 149 ss.

categorie di trattamenti, limitando, dunque, l'intrinseca indeterminatezza dello stesso[124]; i codici di condotta, di contro, sono caratterizzati da una *vis* conformativa delle condotte dei soggetti cui si rivolgono attenuata, appropriandosi di una dimensione più vicina al principio di correttezza nella sua funzione valutativa[125].

2.6. Finalità del trattamento, ragionevoli aspettative

Le finalità del trattamento sono un aspetto dello stesso che interseca parimenti i principi di liceità e correttezza.

Il principio di limitazione delle finalità[126] impone che, nei limiti delle stesse, così come determinate dal titolare del trattamento o a monte dal legislatore, il trattamento deve ritenersi legittimo; nei casi in cui queste siano determinate dal titolare del trattamento, queste devono essere *esplicite* e *legittime*: al di fuori di tale requisito di liceità dello scopo, la discrezionalità nella selezione delle finalità da perseguire deve ritenersi *prevalentemente* libera[127].

A tal proposito, occorre rilevare che il *considerando* n. 50 e l'art. 6, par. 4, GDPR, dettati relativamente a trattamenti di dati per finalità diverse da quelle per cui i dati sono stati raccolti, impongono un requisito di compatibilità tra la finalità originaria e finalità ulteriore: tale giudizio di comparazione deve tenere conto di aspetti concreti e sostanziali del rapporto tra titolare e interessato e del contesto del trattamento avvenuto per il perseguimento della prima finalità; il giudizio di valutazione dell'opportunità e della congruità delle nuove finalità rispetto a quelle precedenti avviene sulla base sia di criteri indicati espressamente al par. 4 dell'art. 6 GDPR, sia secondo correttezza, la quale *ivi* opera come canone di bilanciamento tra gli interessi contrapposti. Tra i criteri indicati dal Regolamento per saggiare la pertinenza delle finalità del trattamento ulteriori, è attribuito particolare rilievo a quello delle *ragionevoli aspettative* dell'interessato[128]. Tale criterio, in quanto esplicazione del principio di trasparenza, viene usualmente ricondotto alla nozione generale di correttezza: «*at*

[124] Cfr. F. Bravo, *Regole generali applicabili a tutti i trattamenti di dati personali*, cit., pp. 46-49.

[125] Riflessioni simili sono state espresse in relazione ai codici di condotta di cui all'art. 2, co. 2, lett. *a-g)*, d.lgs. 28 dicembre 2001, n. 467, per i quali il co. 3 del medesimo articolo ne sanciva il rispetto quale condizione per la liceità del trattamento; in particolare, argomentando *a contrario*, si era sostenuto che i codici di condotta non ricompresi in tale novero si limitassero ad attingere alla correttezza del trattamento, «come se ciò implicasse una sottordinazione dei primi rispetto ai secondi nel sistema delle, e una diversa rilevanza in ordine al regime speciale di responsabilità civile», F. Bravo, *Regole generali applicabili a tutti i trattamenti di dati personali*, cit., p. 46

[126] Cfr. art. 5, par. 1, lett. *b)*, GDPR.

[127] Similmente, in riferimento alla previgente normativa, E. Navarretta, Commento *sub* art. 9, cit., p. 329: «gli stessi limiti a priori all'esercizio del diritto non sono in toto predeterminati dal legislatore, ma sono in parte affidati alla scelta del titolare del trattamento. In particolare, sul presupposto di un'opzione normativa volta ad escludere una generica libertà di trattamento dei dati personali, il titolare è chiamato a scegliere, entro le coordinate massime della legittimità dello scopo, una finalità specifica della sua attività che, a partire da quella scelta, configura un limite invalicabile nell'esercizio della situazione soggettiva».

[128] Cfr. EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, revisionate l'8 ottobre 2019, p. 6.

a very general level, the notion of fairness undoubtedly means that, in striving to achieve their data-processing goals, data controllers must take account of the interests and reasonable expectations of data subjects»[129]. Il rispetto delle aspettative, difatti, rende l'ulteriore attività di trattamento in una certa misura prevedibile, permettendo all'interessato di valutare compiutamente la portata di tale sopravvenienza. Ai sensi dell'art. 6, par. 4, GDPR si può fare a meno di tale requisito di compatibilità quando il trattamento per finalità diversa da quella per cui i dati sono stati raccolti sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri.

La direttiva 770/2019/UE, nel delineare la fattispecie di fornitura di servizi e contenuti digitali a fronte dell'autorizzazione al trattamento di dati personali ulteriori rispetto a quelli necessari per l'esecuzione del contratto, sembra delineare, almeno in parte, una fattispecie rientrante nell'art. 6, par. 4, GDPR: nello specifico, vi è un trattamento di dati necessari per l'esecuzione della prestazione di somministrazione del contenuto o servizio digitale[130], e un diverso trattamento, basato sul consenso – dunque su una differente condizione di liceità – che potrebbe, ma non *deve*, avere ad oggetto, in tutto o in parte, i dati già raccolti per l'offerta del contenuto o servizio digitale.

In relazione a tale secondo trattamento, occorre interrogarsi sui limiti della libertà attribuita al titolare del trattamento nel determinare le nuove finalità, nell'ipotesi di prestazione del consenso alle stesse. Come già precisato[131], i dati personali non possono essere considerati *merce di scambio* né ai sensi del GDPR, né ai sensi della direttiva 770/2019/UE. Ciò nonostante, la prestazione del consenso quale posta contrattuale è stata agevolata dal recente intervento normativo, e il rischio concreto è che, pur in considerazione delle cautele di fungibilità del servizio offerto e non pregiudizievolezza della revoca del consenso, l'operatore economico, facendo affidamento sul dato empirico della scarsa cura della propria riservatezza che notoriamente caratterizza gli utenti fruitori dei servizi digitali, possa abusare della – forse eccessiva – libertà attribuita dal legislatore europeo nel consentire la fornitura di dati ulteriori, senza alcun limite se non il consenso.

Tale riflessione porta a riconsiderare la effettiva estraneità della correttezza nella determinazione delle finalità, dunque sulla portata conformativa interna ed *ex ante* della correttezza. Da un lato, soprattutto in relazione al recente intervento normativo europeo sulla fornitura di servizi e contenuti digitali, la libertà concessa nella determinazione delle finalità del trattamento si presta ad abusi tali da vanificare lo strenuo sforzo di tutela dell'interessato e dei dati personali in quanto attributi della personalità estranei alle logiche mercificatorie ed economiche; dall'altro, il contemperamento *ex ante* di tale libertà nella determinazione delle finalità, facendo ricorso al principio di correttezza, deve ritenersi senz'altro ammissibile data la centralità e portata *universale* del principio in questione in relazione ad ogni attività di tratta-

[129] L.A. BYGRAVE, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Wolters Kluwer, 2002, p. 58.

[130] La cui base giuridica, dunque, si rinviene nell'art. 6, par. 1, lett. *b)*, GDPR.

[131] Cfr. par. 2.3 del presente scritto.

mento. Lo stesso Gruppo di lavoro *ex* art. 29 ha sancito che il requisito di legittimità richiesto dall'art. 5, par. 1, lett. *b)* debba essere interpretato estensivamente, andandovi a ricomprendere anche il principio di non discriminazione[132], il quale, come si è visto, non è altro che un'accezione della correttezza, nella sua veste di *equità*.

Deve dunque ritenersi che il giudizio sulla legittimità delle finalità non si riduce a un giudizio di accertamento del mero rispetto della cornice formale disposta dalle norme, bensì si spinge sino a valutare la potenziale contrarietà a correttezza delle finalità predisposte dal titolare del trattamento[133]. Se in ambito contrattuale il controllo sulla meritevolezza dell'interesse perseguito dalle parti nel contratto tende a coincidere con il giudizio sulla causa concreta, ovverosia del risultato pratico al cui raggiungimento il contratto è preordinato[134], in ambito *privacy*, di contro, tale vaglio si ritiene essere ben più pregnante e attinente al merito delle finalità perseguite: la giustificazione di un tale più severo giudizio rispetto al ramo civile dell'ordinamento si rinviene proprio nella qualità dell'ente "dato personale", il quale si inserisce nel contesto di rapporti contrattuali, anche di estrema rilevanza economica e sociale, senza che il suo carattere di attributo della personalità, meritevole di essere maggiormente attenzionato e cautelato dalla perigliosa autonomia privata, sia intaccato.

3. Applicazione del principio nella casistica

3.1. Estensione e limiti del principio di correttezza

Posta la frammentazione, a livello normativo, dei precipitati concreti più rilevanti del principio di correttezza, la prassi successiva all'entrata in vigore del Regolamento ha fatto larghissimo riferimento a tali ultimi principi, di accentuata attinenza pratica, in detrimento di uno sviluppo più compiuto e approfondito del principio di correttezza: difatti, alla violazione dei principi o di norme specifiche della normativa *de quo*, sovente, per tuziorismo, si accompagna la tautologica dichiarazione di violazione del principio di correttezza[135].

---

[132] Cfr. Gruppo di lavoro ex art. 29, *Opinion 03/2013 on purpose limitation*, WP 203, adottata il 2 aprile 2013.

[133] In tal senso Bravo, relativamente all'art. 11, comma 1, lett. *b)*: «lo scopo, in tal modo considerato, viene ad essere oggetto di un giudizio volto a valutarne la corrispondenza al dettato normativo e la sua non contrarietà agli interessi che l'ordinamento intende proteggere. La determinatezza dello scopo e la necessità della sua esplicitazione, pertanto, appaiono strumentale al sindacato di legittimità a cui intende far riferimento la lett. *b* e, *amplius*, al giudizio di liceità e correttezza di cui alla lett. *a*», F. Bravo, *Regole generali applicabili a tutti i trattamenti di dati personali*, cit., p. 49.

[134] Per tutti, C.M. Bianca, *Il contratto*, cit., p. 413; in giurisprudenza, *ex multis*, si richiama la recente pronuncia Cass. civ., sez. un., sent. 23 febbraio 2023, n. 5657.

[135] Tra i provvedimenti più recenti del Garante: Provv. 27 gennaio 2021, in *https://garanteprivacy.it*, doc. *web* n. 9544504, nel quale il Garante ha censurato un trattamento illecito di dati personali da parte di un'infermiera, la quale aveva comunicato informazioni riguardanti lo stato di salute di una paziente a soggetti non indicati dalla stessa (in violazione degli artt. 5, par. 1, lett. *a)*, e 9 del Regolamento), e ne ha rilevato la contrarietà a correttezza in quanto la condotta colpevole dell'operatrice sanitaria aveva leso l'affidamento e fiducia della paziente, la quale espressamente aveva richiesto che non fossero comunicati a terzi i propri dati personali; Id., Provv. 26 novembre 2020, *ivi*, doc. *web* n.

Spesse volte, le norme del GDPR richiedono l'adempimento di oneri non meramente formali, bensì sostanziali, i quali, dunque, sono sottoposti, in sede di accertamento, ad un'indagine ermeneutico-volitiva orientata primamente dal canone di correttezza: coerentemente, è stata sanzionata, in quanto contraria a correttezza, la predisposizione dell'informativa ai sensi dell'art. 13 GDPR caratterizzata da incompletezza e/o insufficiente specificità delle informazioni fornite, tali da non permettere all'interessato una valutazione informata delle modalità e finalità del trattamento ai fini della prestazione del consenso[136].

9533587, nel quale il Garante ha ritenuto contrario al principio di correttezza – oltre che all'art. 13 GDPR – il trattamento di dati personali effettuato mediante sistema di videosorveglianza da parte del datore di lavoro nei confronti dei propri dipendenti in assenza di informativa; ID., Provv. 12 giugno 2019, *ivi*, doc. *web* n. 9120218, nel quale il Garante ha ritenuto contrario a correttezza il trattamento di dati effettuato sulla base di un unico consenso prestato per più finalità di trattamento, in violazione dell'art. 23, co. 1 e 4, d.lgs. 30 giugno 2003, n. 196; ID., Provv. 26 ottobre 2017, *ivi*, doc. *web* n. 7339171, nel quale il Garante ha ritenuto contrario a correttezza il trattamento di dati effettuato, nell'ambito dell'attivazione di servizi telefonici non richiesti, in assenza di una base giuridica tra quelle previste dagli artt. 23-24 d.lgs. 30 giugno 2003, n. 196; ID., Provv. 21 settembre 2017, *ivi*, doc. *web* n. 7221917, nel quale il Garante ha ritenuto contrario al principio di correttezza e finalità (art. 11, comma 1, lett. *a)* e *b)*, d.lgs. 30 giugno 2003, n. 196), il trattamento per finalità pubblicitarie operato su dati personali raccolti. Orbene, nei casi in esame, la violazione di altre norme della normativa *privacy* ha indotto a ritenere sussistente anche violazione del principio di correttezza, e non del tutto scorrettamente, essendo ravvisabili condotte tipicamente ricondotte alla violazione della buona fede e della correttezza (la non trasparenza, l'elusione della legge, il mancato rispetto della volontà dell'interessato, etc.); purtuttavia, si obietta che (i) tali rilievi hanno mero carattere di rinforzo rispetto alle trancianti e assorbenti violazioni di altre precipue disposizioni, e (ii) la violazione stessa delle norme di tale settore dell'ordinamento è intrinsecamente connotata da un disvalore non solo giuridico, bensì sociale e/o morale – attingendo i dati personali alla sfera più intima e identitaria della persona – afferente *ex necesse* all'alveo di significati attribuibili alla clausola generale di correttezza.

[136] GPDP, Provv. 4 ottobre 2018, in *https://garanteprivacy.it*, doc. *web* n. 9058572: «l'informativa relativa alla condivisione non rispetta il principio di correttezza e, soprattutto, appare inidonea in quanto non contiene tutti gli elementi tassativamente previsti dall'art. 13 del Codice, con riferimento ai seguenti tre profili: i. nel messaggio di notifica viene solo comunicato un generico cambiamento della cd. privacy notice, non evidenziandosi in alcun modo l'elemento sostanziale che ha reso necessario modificare le informazioni agli interessati (vale a dire la condivisione con Facebook dei dati relativi all'account WhatsApp); ii. non è di agevole comprensibilità, anche nell'informativa integrale, quali siano i dati oggetto di comunicazione a Facebook; iii. le finalità perseguite dal trattamento in questione risultano vaghe, specie laddove fanno riferimento a un preteso "miglioramento delle esperienze con le inserzioni e i prodotti di Facebook", mentre si tratta di consentire, tra le altre, a operazioni di carattere pubblicitario effettuate, evidentemente, nell'interesse di Facebook»; ID., Provv. 19 luglio 2018, *ivi*, doc. *web* n. 9039945: «In relazione all'obbligo, posto in capo al titolare, di informare, prima dell'inizio dei trattamenti, i dipendenti circa le caratteristiche essenziali degli stessi, come prescritto dall'articolo 13 del Codice (dal 25 maggio 2018 dall'articolo 13 del Regolamento (UE) 2016/679) e conformemente al principio di correttezza di cui all'art. 11, comma 1, lett. a) del Codice (dal 25 maggio 2018 dall'art. 5, par. 1, lett. a) del Regolamento (UE) 2016/679), si è ritenuto che le informative rese non fossero conformi alla disciplina in materia di protezione dei dati personali. Infatti, nel corso degli accertamenti ispettivi è emerso che, per quanto riguarda i trattamenti di geolocalizzazione, la società non ha apposto sui veicoli geolocalizzati l'informativa "minima" (vetrofania). Inoltre, per quanto concerne l'informativa completa di tutti gli elementi previsti dal richiamato art. 13 si è ritenuto che l'informativa fornita all'atto della stipula del rapporto di lavoro (v. precedente punto 1.4.) non abbia soddisfatto i requisiti indicati dalla norma, in quanto non

Analizzando la prassi dell'Autorità garante, si è rilevato altresì come il principio di correttezza si ritenga violato qualora il trattamento non sia rispettoso della *dignità* dell'interessato, in quanto idoneo a esporlo, senza che vi sia un interesse apprezzabile a farlo, a vergogna o umiliazione[137], ovvero se posto in essere con modalità tali da ledere valori morali, quali ad esempio il sentimento di pietà verso i defunti[138].

Rilevante un recente provvedimento[139] nel quale, di contro, non veniva considerato contrario a correttezza il trattamento di dati personali effettuato nei confronti di un soggetto di pubblica rilevanza, nell'ambito di una trasmissione televisiva alla quale egli stava volontariamente prendendo parte vertente su tematiche politiche, dunque, di interesse pubblico. Nella specie, l'interessato non si era reso conto della conclusione della pausa pubblicitaria ed era stato ripreso a discorrere in termini dialettali e scurrili con altri invitati al programma televisivo. Si legge nel provvedimento del Garante: «non può ritenersi violato il principio di correttezza, in quanto non sono stati usati artifici volti a carpire dichiarazioni che avrebbero dovuto avere carattere riservato»; secondo tale inciso, dunque, non è necessariamente contrario a correttezza *ogni* trattamento idoneo a ledere la dignità o valori morali dell'interessato – qualità proprie del trattamento in oggetto – nonché, espandendo la portata del rilievo, di altri soggetti, dovendosi di converso valutare la contrarietà a correttezza tenendo conto di tutte le circostanze del caso concreto.

In circostanze simili, al contrario, è stata ritenuta contraria a correttezza la diffusione di un "fuori onda" avente ad oggetto la conversazione tenutasi fra un politico di spicco e altri soggetti, registrate sì in sala stampa, ma furtivamente e prima dell'inizio dell'intervista ufficiale che avrebbe avuto luogo poco dopo[140]. Parimenti, è stato ritenuto contrario a correttezza l'occulta raccolta di dati personali relativi alla salute effettuata dai giornalisti di un noto programma televisivo, finalizzata a disvelare chi, fra i politici interessati, facesse uso di droghe, effettuata tramite l'uso

contiene alcuna indicazione circa finalità e modalità del trattamento, nonché circa l'ambito di comunicazione ed i soggetti che possono venirne a conoscenza in qualità di responsabili o incaricati».

[137] GPDP, Provv. 30 novembre 2005, in *https://garanteprivacy.it*, doc. *web* n. 1213644: «In occasione dello svolgimento delle attività di recupero crediti deve altresì essere osservata la clausola generale di correttezza (art. 11, comma 1, lett. a), del Codice: in base ad essa sono preclusi, sia in fase di raccolta delle informazioni sul debitore, sia nel tentativo di prendere contatto con il medesimo (anche attraverso terzi), comportamenti suscettibili di incidere sulla sua dignità, qui riguardata sul solo piano della disciplina di protezione dei dati personali»; Id., comunicato stampa del 22 gennaio 2018, *ivi*, doc. *web* n. 7536868, nel quale il Garante richiama i *media* da evitare di riportare informazioni idonee a identificare l'identità di una vittima di violenza sessuale e dunque a ledere la riservatezza e la dignità di tutti i familiari coinvolti.

[138] GPDP, Provv. 13 novembre 2003, in *https://garanteprivacy.it*, doc. *web* n. 1067167, nel quale il Garante ha dichiarato contrario a correttezza il trattamento di dati personali consistente nella raccolta e pubblicazione, su un noto settimanale nazionale, di immagini rinvenute nei luoghi di sepoltura di fanciulli rimasti vittime di una calamità naturale, in quanto idoneo a offendere il ricordo e la pietà dei defunti, nonché il legittimo interesse al decoro e riserbo personale e familiare delle famiglie interessate.

[139] GPDP, Provv. 7 novembre 2019, in *https://garanteprivacy.it*, doc. *web* n. 9217365.

[140] GPDP, Provv. 22 luglio 1998, in *https://garanteprivacy.it*, doc. *web* n. 39813; Id., Provv. 30 luglio 1998, *ivi*, doc. *web* n. 48869.

di un duplice artifizio: prima costoro sono stati irretiti con il pretesto di una fasulla intervista, successivamente una falsa truccatrice, nell'asciugare loro il sudore dalla fronte, ha raccolto materiale biologico con cui poi effettuare l'esame[141]. Ferme le violazioni del codice di deontologia giornalistico, l'Autorità garante ha rilevato la violazione del principio di correttezza nell'uso di artifici per indurre l'interessato a fornire i propri dati. Parimenti, l'accortezza predisposta dal programma televisivo di non rendere identificabile chi, tra gli esaminati, fosse positivo, è misura comunque lesiva della dignità e riservatezza dell'interessato, dacché non affranca mai coloro non positivi dal dubbio, ingenerato nel pubblico spettatore, che potessero rientrare nella cerchia di soggetti facenti uso di tali sostanze.

3.2. Uno sguardo concreto alla correttezza "procedurale"

La correttezza in senso procedurale[142] è uno degli esiti dell'interpretazione dell'omonimo principio sotto l'egida della nuova normativa per la protezione dei dati personali. Germi di tale accezione sostanzialistica del principio di correttezza, tuttavia, si rinvengono anche nella prassi relativa alla precedente normativa più recente. Rilevante, a tal proposito, un provvedimento del Garante[143] reso poco prima dell'emanazione del d.lgs. 101/2018, nel quale sono state considerate contrarie a correttezza plurime procedure predisposte da un noto operatore telefonico per consentire l'esercizio dei diritti di cui all'abrogato art. 7 d.lgs. 196/2003; il Garante ha rilevato che la procedura predisposta dall'operatore per consentire agli interessati di controllare e/o modificare la volontà resa rispetto al trattamento dei dati personali per tali finalità fosse connotata da superflui e fuorvianti passaggi, volti e disincentivare l'interessato dall'uso di tali sistemi di controllo: «per variare la volontà manifestata in ordine al trattamento dei dati per finalità di marketing è necessario accedere alla sezione dedicata all'"area clienti" previo inserimento delle credenziali individuali; quindi, la modifica del consenso all'attività di marketing può essere effettuata solo previa modifica della password di accesso a detta sezione, altrimenti tale variazione viene inibita»; tanto rilevato, «in relazione alle modalità predisposte dalla Società per consentire ai clienti di modificare la dichiarazione di volontà resa rispetto al trattamento dei dati personali a sé riferiti per finalità di marketing, dopo aver avuto accesso all'area di self care messa a loro disposizione, la circostanza della necessità di procedere previamente a modificare la password di accesso all'area clienti (...) si pone come indebito ostacolo all'esercizio del diritto all'autodeterminazione informativa e comporta una violazione del principio di correttezza nel trattamento dei dati personali (art. 11, comma 1, lett. a), del Codice. Tale operazione, non infatti necessaria per identificare univocamente il dichiarante, atteso che lo stesso ha già avuto accesso all'area a sé dedicata nel sito web della Società, si sostanzia quindi in un adempimento ulteriore che rende più oneroso l'esercizio dei diritti da parte degli interessati». A ciò consegue che «le misure tecnico-organizzative che ciascun titola-

[141] GPDP, Provv. 10 ottobre 2006, doc. *web* n. 1345622; ID., Provv. 14 dicembre 2006, *ivi*, doc. *web* n. 1370954.
[142] Cfr. par. 2.4 del presente scritto.
[143] GPDP, Provv. 22 maggio 2018, doc. *web* n. 8995285.

re del trattamento è tenuto a porre in essere per dare compiuta attuazione a tali diritti (quelli di cui all'abrogato art. 7 d.lgs. 30 giugno 2003, n. 196) devono essere ispirate a questi principi (correttezza, *privacy by design*; *n.d.a.*)». Il Garante conclude rilevando che «le condotte che ostacolano o comunque comportano un più oneroso esercizio dei diritti per l'interessato rispetto al paradigma fissato dal legislatore integrano in capo al titolare del trattamento una violazione del principio di correttezza sancito all'art. 11, comma 1, lett. a), del Codice e devono pertanto essere rimosse».

In questa dimensione, il principio di correttezza assume un ruolo di centrale rilevanza, in quanto costituisce il metro di giudizio per valutare l'adeguatezza delle procedure sostanzialmente poste in essere per garantire un'adeguata tutela dell'interessato. Tale obbligo, posto a carico del titolare o del responsabile del trattamento, trova conforto e riconoscimento positivo negli artt. 25, par. 1 e 28, par. 1, GDPR. A tal proposito, il titolare del trattamento può servirsi dei meccanismi di certificazione di cui all'art. 42 GDPR per dimostrare la conformità del trattamento a tale requisito (art. 25, par. 3, GDPR), mentre per il responsabile del trattamento, oltre a tale strumento, è possibile aderire a un codice di condotta (art. 28, par. 5, GDPR) di cui all'art. 40 GDPR. Appare così chiaro che al responsabile del trattamento è concesso un percorso agevolato, rispetto al titolare, nella prova dell'adempimento degli obblighi in parola, in ragione dell'astratto maggior grado di responsabilizzazione che investe la figura del titolare del trattamento; si rileva, tuttavia, che nell'odierno contesto economico tale rapporto è rovesciato, dacché vi sono pochi responsabili del trattamento di elevata rilevanza economica e imprenditoriale cui si rivolgono un elevato numero di titolari del trattamento, costituendo rapporti basati su contratti-tipo predisposti dal responsabile del trattamento da sottoscrivere sostanzialmente «per adesione»[144].

4. Riflessioni conclusive

A conclusione del discorso fin qui condotto può precisarsi che il principio di correttezza assolve la funzione di norma di chiusura dell'impianto normativo preposto alla protezione dei dati personali, in quanto volto sia a regolare il novero di fattispecie – seppur rare – non già analiticamente disciplinate da disposizioni specifiche, sia ad orientare l'applicazione e l'interpretazione di quest'ultime. A tal fine, ruolo di primario rilievo è attribuito al Garante, sia in ragione della copiosa attività provvedimentale avente ad oggetto tale principio, sia avendo riguardo del potere regolamentare attribuitogli dall'art. 2-*quater* d.lgs. 30 giugno 2003, n. 196.

Il principio di correttezza, primamente, opera quale canone di valutazione a posteriori delle condotte dei soggetti coinvolti nel trattamento; altresì, in ragione del regime di responsabilità che lo assiste in caso di violazione dello stesso[145], è caratterizzato da immediata precettività[146], tale da conformare la condotta dei soggetti

[144] Cfr. F. Pizzetti-L. Greco, Commento *sub* art. 28, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della privacy e data protection*, cit., pp. 467-468.

[145] Cfr. art. 83, par. 5, lett. *a)*, GDPR.

[146] Cfr. F. Piraino, *Liceità e correttezza*, cit., p. 851.

anche nei momenti precedenti al trattamento: ciò è evidente per quei trattamenti che rinvengono la propria base giuridica nell'art. 6, par. 1, lett. *f)*, GDPR, nonché in ragione dell'esistenza dei codici di condotta e delle regole deontologiche, precipuamente volte a conformare *ex ante* la condotta dei soggetti interessati dalle disposizioni *ivi* contenute.

Invero, tra tutti i principi che abitano tale settore dell'ordinamento, di quello di correttezza assume una posizione di rilievo, tale per cui plurimi tra quelli espressamente contemplati dalla normativa non costituiscono altre che specificazioni del primo. Tale frammentazione, tuttavia, ha in certa parte inibito un pieno sviluppo dogmatico del principio in oggetto, in quanto gran parte del suo ambito elettivo è confluito in altri principi aventi ormai dignità autonoma; ciò non di meno, il principio di correttezza mantiene un proprio spettro applicativo esclusivo da individuare in tutti i momenti in cui ai soggetti coinvolti nell'attività di trattamento è demandata un'attiva valutativa o di bilanciamento di interessi in conflitto.

Capitolo IV
Il principio di trasparenza

*Federica Cilia - Silvia Dalle Nogare - Raffaella Pozzi**

SOMMARIO: 1. Inquadramento normativo. – 1.1. L'enunciazione del principio di trasparenza nel GDPR. – 1.2. Il principio di trasparenza nell'evoluzione normativa in materia di protezione dei dati personali. – 1.3. Ancora sulla trasparenza nel GDPR come principio del diritto europeo in materia di protezione dei dati. – 2. Portata del principio. – 2.1. Contenuti del principio di trasparenza. – 2.2. Principio di trasparenza, diritti dell'interessato e obblighi di informazione in relazione alle attività di trattamento. Connessioni tra principio di trasparenza e principio di liceità. – 2.3. Ancora su principio di trasparenza e diritti dell'interessato. – 2.4. Il principio di trasparenza nei trattamenti effettuati dalla Pubblica Amministrazione. – 3. Applicazione del principio nella casistica. – 3.1. Il principio di trasparenza nell'adempimento dell'obbligo di informativa. – 3.2. Il principio di trasparenza rispetto all'uso di nuove tecnologie e ai diritti dell'interessato. – 3.3. Pubblica Amministrazione e trattamenti dei dati personali tramite processi decisionali automatizzati. Bilanciamento tra principio di trasparenza e diritto d'autore.

1. Inquadramento normativo

1.1. L'enunciazione del principio di trasparenza nel GDPR

Nel Regolamento UE n. 679/2016 il principio di trasparenza è enunciato dall'art. 5, par. 1, lett. *a)*, il quale dispone che «i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza")»[1].

L'espressa menzione del principio in commento, autonomamente contemplato accanto a quello di liceità e di correttezza, rappresenta un mutamento decisivo rispetto a quanto è possibile riscontrare nella Direttiva 95/46/CE (oggi abrogata), il cui art. 6, par. 1, lett. *a)*, richiamava formalmente i principi di liceità e correttezza, ma non quello di trasparenza[2]. Va, invero, precisato che il principio di trasparenza emergeva comunque nell'impianto della direttiva citata ed era comunque da tempo considerato

---

* Pur essendo lo scritto frutto di riflessione comune, il par. 1 è da attribuire a Raffaella Pozzi, il par. 2 a Silvia Dalle Nogare, il par. 3 a Federica Cilia.

1 Per un esame del principio di trasparenza v. in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, i commenti agli artt. 5 (di G. MALGERI, pp. 183 ss.), 12 (di A. GENOVESE, pp. 276 ss.), 13-14 (di L. LIGUORI, pp. 287 ss.) e 15 (di A.M. GAMBINO-M. SIRAGUSA, pp. 304 ss.) del Reg. UE n. 679/2016.

2 Cfr. art. 6, par. 1, lett. *a)*, Direttiva 95/46/CE: «Gli Stati membri dispongono che i dati personali devono essere: a) trattati lealmente e lecitamente».

espressione dei principi di correttezza e di liceità ed «elemento fondamentale di questi due principi»[3], seppur non espressamente riportato nel dettato normativo[4].

Nell'articolazione del Reg. UE n. 679/2016, l'esplicita enunciazione congiunta del principio di trasparenza con i principi di correttezza e liceità appare in linea con la sua accresciuta importanza nell'evoluzione normativa in tale materia e, comunque, giustificata dal perseguimento di un medesimo obiettivo, a cui sono orientati tutti e tre i principi dianzi citati (liceità, correttezza e trasparenza), ossia quello di «evitare trattamenti abusivi opachi, sleali o comunque illeciti»[5] ed accordare, così, un elevato sistema di protezione in favore dell'interessato.

1.2. Il principio di trasparenza nell'evoluzione normativa in materia di protezione dei dati personali

Per comprende appieno la declinazione del principio di trasparenza nel Reg. UE n. 679/2016 è utile ripercorrere la sua disciplina nell'ambito dell'evoluzione normativa sulla protezione dei dati personali.

Nelle prime norme rese in tale materia in ambito internazionale[6] e nell'allora Comunità europea[7], così come, in sede di attuazione, nell'ordinamento interno[8], il principio di trasparenza – come s'è già avuto modo di rimarcare – non ha avuto una precisa e definitiva esplicitazione con riguardo al trattamento dei dati personali[9].

Del resto, è emersa in tempi relativamente recenti l'esigenza di tutelare in maniera sistematica le persone fisiche contro i rischi derivanti dal trattamento dei dati personali. Tralasciando il discorso sulle origini del diritto alla *privacy*[10] e sulla successiva evoluzione quale diritto alla protezione dei dati personali, va rimarcato che in ambito europeo, com'è noto, si deve attendere l'immediato dopoguerra per

---

[3] In questo senso, Gruppo Di Lavoro Ex Art. 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679 WP260 rev.01*, documento disponibile su Internet all'indirizzo https://ec.europa.eu/newsroom/article29/items/622227/en (consultato da ultimo in data 3 aprile 2023).

[4] Diverse disposizioni della direttiva deponevano in questo senso, prime fra tutte quelle che fissavano, per l'interessato, il diritto all'informativa (artt. 10 e 11), il diritto di accesso (art. 12) e il consenso informato [art. 2, par. 1, lett. *h)* e artt. 6, par. 1, lett. *a)* e 7, par. 2, lett. *a)*].

[5] G. Malgieri, *I principi (comm. all'art. 5 GDPR)*, in R. D'orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *op. cit.*, pp. 183 ss., con particolare riferimento al par. 4, interamente dedicato al principio di trasparenza.

[6] Cfr. Convenzione di Strasburgo n. 108 del 1981, resa dal Consiglio d'Europa.

[7] Cfr., *in primis*, Direttiva 95/46/CE, poi abrogata e sostituita dal Reg. UE n. 679/2916.

[8] Cfr. l. 675/1996, poi confluita, con altre disposizioni di settore, nel d.lgs. 196/2003 e ss.mm.ii. (Codice in materia di protezione dei dati personali).

[9] Va precisato che la trasparenza è principio da tempo consolidato nel diritto dell'Unione Europea, in ambiti diversi rispetto a quello di protezione dei dati personali: l'art. 1 del TUE si riferisce a decisioni prese «nel modo più trasparente possibile e il più vicino possibile ai cittadini», mentre l'art. 11, par. 2, indica che «le istituzioni mantengono un dialogo aperto, trasparente e regolare con le associazioni rappresentative e la società civile». L'art. 15 del TFUE impone alle istituzioni, agli organi e organismi dell'UE di assicurare la trasparenza dei lavori svolti.

[10] Cfr. S.D. Warren-L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Rev.*, 1980, 4, pp. 193 ss. L'elaborato rappresenta il punto di partenza per la più moderna concezione della *privacy* vista non solo come diritto a non subire intromissioni nella propria sfera personale ma anche come diritto al controllo del flusso delle proprie informazioni.

l'affermazione della tutela della vita privata quale diritto fondamentale dell'individuo: l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), adottata il 4 novembre 1950, sancisce il diritto al rispetto della vita privata e familiare, interpretato anche come diritto alla protezione delle informazioni di carattere personale[11].

Il contesto sociale ed economico dell'epoca non imponeva ancora la formalizzazione di un apparato normativo *ad hoc* per la protezione dei dati personali. Lo sviluppo della tecnologia e la correlata crescente necessità di proteggere i dati personali hanno portato, nel corso del tempo, ad una sempre più estesa interpretazione del concetto di *privacy* espresso dall'art. 8 CEDU, nonché all'applicazione di diverse ulteriori fonti normative, che, a livello internazionale, potessero meglio definire l'ambito di tutela nei confronti del crescente fenomeno del trattamento automatizzato dei dati personali.

In tale contesto, è particolarmente significativa la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del Consiglio d'Europa (Convenzione 108), firmata il 28 gennaio 1981, che ha definito fin dall'art. 1 la protezione dei dati personali degli individui come parte integrante dei diritti fondamentali dell'uomo: «*The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy*»[12].

Il testo originario della Convenzione n. 108 proseguiva con un inciso volto a restringere l'ambito di protezione ai soli casi di «*elaborazione automatica*» dei dati personali, ma l'inciso è stato poi eliminato nella versione aggiornata della Convenzione, avutasi con il protocollo emendativo del 2018 (c.d. Convenzione 108+).

---

[11] L'art. 8 CEDU, rubricato «*Diritto al rispetto della vita privata e familiare*», dispone che «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».
In tale articolo, utilizzato per tutelare le informazioni di carattere personale contro ogni ingerenza, non compare espressamente il principio di trasparenza. Una sua traccia può tuttavia rinvenirsi nell'obbligo di prevedere con legge le ingerenze da parte di un'autorità pubblica: tale fonte normativa, oltre a garantire una maggiore tutela per l'individuo (in quanto richiede che sia emanata a seguito di un articolato iter, che in uno Stato democratico assicura la necessaria ponderazione delle scelte ivi adottate), soddisfa in *nuce* le esigenze di trasparenza, richiedendo la sua preventiva pubblicazione (in Gazzetta Ufficiale) al fine della sua conoscibilità.

[12] Il mutato contesto sociale ed economico che giustifica la protezione dei dati personali è ben rappresentato nel preambolo della Convenzione 108, ai sensi del quale gli Stati firmatari hanno ritenuto «auspicabile estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica».

L'art. 5 della Convenzione 108[13], nel testo originario del 1981, declinava, sotto la rubrica «*Qualità dei dati*», i "principi" del trattamento, menzionandoli non espressamente, in quanto tali, ma implicitamente, attraverso l'enunciazione delle "caratteristiche" di tipo "qualitativo" che i dati devono avere. Fra questi – per quanto di interesse nel presente elaborato – si trovavano riportati, in tal modo, i "principi" di lealtà, liceità (i dati devono essere «ottenuti ed elaborati lealmente e legalmente») e finalità del trattamento (i dati devono essere «registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini»)[14].

Oltre ad essere implicito nelle citate disposizioni dell'art. 5, il principio di trasparenza è stato comunque posto a fondamento delle ulteriori disposizioni contenute negli artt. 8[15] e 9[16] della Convenzione 108, regolanti, rispettivamente, i diritti dell'interessato e le ipotesi in cui sono possibili eccezioni e restrizioni a talune disposizioni della convenzione stessa.

---

[13] L'art. 5 della Convenzione n. 108/1981, nel suo testo originario, rubricato «*Qualità dei dati*», prevedeva che «I dati a carattere personale oggetto di elaborazione automatica devono essere: *a)* ottenuti ed elaborati lealmente e legalmente; *b)* registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini; *c)* adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati; *d)* esatti e, se necessario, aggiornati; *e)* conservati sotto una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati».

[14] Come si preciserà anche più avanti, l'aggiornamento della Convenzione n. 108/81, ad opera del protocollo emendativo del 2018, ha portato ad una significativa modifica anche dell'art. 5, con l'inserimento di un esplicito riferimento alla trasparenza, assente nel testo originario della Convenzione.

[15] V. art. 8 («*Garanzie supplementari per la persona interessata*») della Convenzione n. 108/81 (testo originario): «Ogni persona deve avere la possibilità di: *a)* conoscere l'esistenza di una collezione automatizzata di dati a carattere personale, i suoi fini principali, nonché l'identità e la residenza abituale o la sede principale del responsabile della collezione; *b)* ottenere a ragionevoli intervalli e senza eccessivo ritardo o spesa la conferma dell'esistenza o meno, nella collezione automatizzata, di dati a carattere personale che la riguardano e la comunicazione di tali dati in forma intellegibile; *c)* ottenere, all'occorrenza, la rettifica di tali dati o la loro cancellazione qualora essi siano stati elaborati in violazione delle disposizioni di diritto interno che danno attuazione ai principi fondamentali enunciati negli articoli 5 e 6 della presente Convenzione; *d)* disporre di un ricorso se non viene dato seguito ad una domanda di conferma o, a seconda dei casi, di comunicazione, di rettifica o di cancellazione ai sensi delle lettere *b)* e *c)* del presente articolo». Oggi l'art. 8 della Convenzione n. 108+ è significativamente rubricato «*Transparency of processing*», con ambito di applicazione esteso significativamente anche ai trattamenti non automatizzati e con modifiche che hanno portato a rimodulare e ampliare gli obblighi informativi (ad es., estendendoli anche alla base giuridica del trattamento).

[16] V. art. 9 («*Eccezioni e restrizioni*») della Convenzione n. 108/81 (testo originario): «1. Non è ammessa alcuna eccezione alle disposizioni degli articoli 5, 6 e 8 della presente Convenzione salvo che nei limiti definiti nel presente articolo. – 2. È possibile derogare alle disposizioni degli articoli 5, 6 e 8 della presente Convenzione quando tale deroga è prevista dalla legge della Parte e costituisce una misura necessaria, in una società democratica: *a)* per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati; *b)* per la protezione della persona interessata e dei diritti e delle libertà di altri. – 3. Restrizioni all'esercizio dei diritti di cui alle lettere *b)*, *c)* e *d)* dell'articolo 8 possono essere previste dalla legge per le collezioni automatizzate di dati a carattere personale utilizzati per fini statistici o di ricerca scientifica, allorché chiaramente non vi sia rischio di pregiudizio alla vita privata delle persone interessate». Tale articolo, nel testo attuale della Convenzione n. 108+, si trova ora riportato, con modifiche, all'art. 11, con la medesima rubrica («*Exceptions and restrictions*»).

Sotto il primo profilo, la trasparenza viene declinata nel diritto dell'interessato a conoscere finalità e modalità del trattamento, anche per esercitare i diritti di controllo sulla gestione dei dati personali e sulla liceità del loro utilizzo, nella prospettiva della sua "autodeterminazione informativa".

Quanto al secondo profilo, relativo alle eccezioni e restrizioni, va evidenziato come la necessità che le stesse siano previste da una legge e costituiscano «misura necessaria in una società democratica per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati»[17] nonché «per la protezione della persona interessata e dei diritti e delle libertà di altri»[18], richiama, tra gli altri, non solo il concetto di correttezza, ma anche di trasparenza nel trattamento dei dati personali. Infatti, per un verso, si viene a determinare il corretto bilanciamento tra tutela della propria vita personale e familiare ed esigenze di sicurezza, e, per altro verso, come già precisato, la trasparenza è assicurata anche dal ricorso alla fonte legislativa, che necessita della sua pubblicazione in Gazzetta Ufficiale, per garantirne la conoscibilità prima della sua applicabilità[19].

Gli anni '90, testimoni del processo di integrazione del mercato unico europeo culminato con il Trattato di Maastricht, la creazione della Comunità Europea e l'istituzione dell'area Schengen con il sistema di libera circolazione delle persone, delle merci e dei capitali, oltre che di libera prestazione dei servizi, hanno portato ad un ulteriore sviluppo delle norme a protezione dei dati personali[20]. Tale nuovo contesto ha richiesto, per la realizzazione del mercato unico e del processo stesso di integrazione europea, che anche i dati personali potessero circolare liberamente; da qui l'esigenza di una normativa quadro a livello europeo sul trattamento dei dati personali, che potesse coniugare il regime di libera circolazione di tali dati con quello di protezione della persona dai rischi derivanti dal trattamento. In questa chiave di lettura «mercato e persona sono due temi che, nell'ottica eurounitaria, vengono perseguiti in una logica di sintesi e non di contrapposizione, nel segno di una costante ricerca di equilibrio, di bilanciamento proporzionale degli interessi, nella prospettiva che lo sviluppo economico possa contribuire al benessere dei popoli e delle persone»[21].

---

[17] Cfr. art. 9, Convenzione n. 108/81, cit.

[18] Cfr. art. 9, Convenzione n. 108/81, cit.

[19] Questi concetti saranno poi rinnovati anche nella Direttiva 95/46/CE cit., oltre che nella Direttiva 2016/68/UE del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[20] Tale sviluppo si registra anche a livello nazionale con l'adozione della l. n. 675 del 31 dicembre 1996 sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Seguendo un'impostazione analoga rispetto a quella della Convenzione n. 108/81 e della Direttiva 95/46/CE, la l. n. 675/1996 non richiamava espressamente il principio di trasparenza, ma lo rendeva implicito nelle modalità di raccolta dei dati personali, negli oneri informativi in capo al titolare del trattamento e nel riconoscimento a favore dell'interessato di specifici diritti di controllo e gestione dei dati personali.

[21] F. Bravo, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 202.

Venne così emanata la Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla *tutela delle persone fisiche* con riguardo al trattamento dei dati personali, nonché alla *libera circolazione di tali dati*, oggi abrogata e sostituita dal Reg. UE n. 679/2016. Come già ricordato, nell'art. 6 della Direttiva emergevano in maniera esplicita solamente i "principi" di liceità e correttezza, ma non anche quello di trasparenza. Quest'ultimo era tuttavia presente nelle maglie della Direttiva e pervadeva l'intera disciplina in materia di protezione dei dati personali ivi delineata[22].

A livello nazionale, si è registrato un progressivo sviluppo del concetto di trasparenza nel settore pubblico, attuato attraverso la regolamentazione del diritto di accesso a partire dal 1990[23], che ha influenzato anche il tessuto normativo in materia di protezione dei dati personali.

Il 30 giugno 2003 veniva adottato il d.lgs. n. 196/2003 («Codice in materia di protezione dei dati personali»), in cui è andata a confluire la l. n. 675/96 di prima attuazione della Direttiva 95/46/CE. All'interno di tale Codice di settore, l'art. 68, collocato nel Capo IV («*Finalità di rilevante interesse pubblico*») e successivamente abrogato per le esigenze di coordinamento con il Reg. UE n. 679/2016, disponeva che «il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la *trasparenza* delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute»[24].

Il principio di trasparenza era dunque espressamente richiamato in relazione alle specifiche attività della pubblica amministrazione, ma non nella disciplina generale in tema di protezione dei dati personali: era tuttavia implicitamente ricavabile dall'intero sistema normativo e dall'interpretazione estensiva di altri principi, come quello di liceità, correttezza e finalità del trattamento, la cui declaratoria era implicitamente desumibile dalla disposizione con cui erano state definite le caratteristiche qualitative dei dati personali (art. 11 del Codice)[25].

---

[22] Ciò risulta, tra l'altro, anche dal *considerando* n. 63, ove si precisava che le autorità di controllo nazionali in materia di protezione dei dati personali «(…) devono disporre dei mezzi necessari all'adempimento dei loro compiti, siano essi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali; che esse debbono contribuire alla *trasparenza* dei trattamenti effettuati nello Stato membro da cui dipendono».

[23] Si rinvia per un approfondimento sul concetto della trasparenza nella pubblica amministrazione al par. 2.4. del presente elaborato.

[24] Le norme relative ai trattamenti svolti per un interesse pubblico rilevante sono ora riportate all'art. 2-*sexies* del Codice in materia di protezione dei dati personali, come novellato dal d.lgs. n. 1018/2018 e da successivi interventi normativi del 2021.

[25] L'art. 11 («*Modalità del trattamento e requisiti dei dati*») del Codice della *privacy*, nel testo originario (poi abrogato con la riforma del 2018, per le esigenze di coordinamento con le nuove disposizioni contenute nel Reg. UE n. 679/2016), prevedeva espressamente che «1. I dati personali oggetto di trattamento sono: *a)* trattati in modo lecito e secondo correttezza; *b)* raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; *c)* esatti e, se necessario, aggiornati; *d)* pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; *e)* conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Nel 2009, il Trattato di Lisbona conferisce carattere giuridicamente vincolante all'interno dell'ordinamento dell'Unione alla Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza)[26]. Quest'ultima, oltre a prevedere tra gli altri l'inviolabilità della dignità umana, della libertà, dell'uguaglianza e della solidarietà, sancisce – oltre al diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni (art. 7) – anche il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano (art. 8), che viene declinato, in maniera autonoma, senza menzionare espressamente la trasparenza, ancora una volta ricavabile in maniera implicita dal contesto[27].

Con l'adozione del Reg. UE n. 679/2016, applicabile in maniera omogenea e cogente in tutti gli Stati membri per creare «un quadro di maggiore certezza del diritto e di maggiore uniformità tra i vari Paesi dell'Unione Europea (…); una sorta di *ius commune* in materia *privacy*»[28], il principio di *trasparenza* trova una espressa collocazione nell'ambito dell'art. 5 e, come del resto anche nella Direttiva 95/46/CE, viene declinato in ulteriori disposizioni che disciplinano i diritti di informazione, di comunicazione, di accesso e di autodeterminazione, funzionali ad esercitare un controllo sul trattamento dei dati personali da parte dell'interessato. L'emanazione del Reg. UE n. 679/2016 ha richiesto un intervento di riforma del Codice in materia di protezione dei dati personali, al fine di operare un raccordo con la fonte europea.

Nell'opera di armonizzazione delle norme unionali in materia di protezione dei dati personali, si è posta particolare attenzione anche alle fonti internazionali: il

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati».

Alla lett. *a)* del co. 1, in linea con quanto previsto nel testo della Direttiva 95/46/CE, compare il riferimento espresso alla liceità e alla correttezza, ma non a quello della trasparenza.

[26] L'art. 6 del Trattato di Lisbona stabilisce «1. L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni.

2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati.

3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali.».

[27] L'art. 8 («*Protezione dei dati di carattere personale*») della Carta dei diritti fondamentali dell'UE stabilisce che «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[28] Si veda il contributo di C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018. L'A. sottolinea che era giunto il momento di approdare ad un concetto nuovo: «*one continent, one law*».

considerando n. 105[29] del Reg. UE n. 679/2016 richiama espressamente la Convenzione 108 e il Protocollo addizionale dell'8 novembre 2001[30], a cui ha fatto seguito l'ulteriore protocollo addizionale del 2018, di ammodernamento della Convenzione, che ha preso la denominazione di Convenzione 108+. È proprio nel suo novellato art. 8, eloquentemente rubricato «*Transparency of processing*» che il principio di trasparenza viene indicato quale obbligo del titolare di fornire all'interessato, in modo trasparente, le informazioni relative alle attività di trattamento (anche con riguardo alle finalità, alle basi giuridiche, alle modalità e alle caratteristiche del trattamento) in modo da consentirgli di controllare che le stesse si svolgano correttamente e lecitamente[31].

L'*Explanatory Report* della Convenzione 108+ si sofferma in più occasioni sul concetto di trasparenza, sia in relazione al trattamento dei dati personali sia rispetto alla valutazione del livello di adeguamento delle Parti firmatarie e alle attività delle autorità di controllo[32]. In particolare, quanto al primo ambito, il par. 48 precisa che i dati personali dovrebbero essere trattati in modo lecito, corretto e trasparente e raccolti per finalità esplicite e determinate. La trasparenza deve, inoltre, essere garantita anche in caso di trattamenti ulteriori, posti in essere per finalità compatibili con quella sussistente al momento di acquisizione dei dati, al fine di mantenere le attività del trattamento nella sfera di «prevedibilità» («*predictability*»)[33]. I paragrafi

---

[29] Il *considerando* n. 105 del Reg. UE n. 679/2016 dispone: «Al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, la Commissione dovrebbe tenere in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, soprattutto in relazione alla protezione dei dati personali, nonché all'attuazione di tali obblighi. In particolare si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale. La Commissione, nel valutare l'adeguatezza del livello di protezione nei paesi terzi o nelle organizzazioni internazionali, dovrebbe consultare il comitato».

[30] Si fa qui riferimento al Protocollo addizionale dell'8 novembre 2001, «*Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*», già applicabile alla data di pubblicazione del Reg. UE n. 679/2016, che risale al 2016.

[31] Si riporta il testo della disposizione in commento: «Art. 8 ("*Transparency of processing*"). – 1. *Each Party shall provide that the controller informs the data subjects of*: a) *his or her identity and habitual residence or establishment*; b) *the legal basis and the purposes of the intended processing*; c) *the categories of personal data processed*; d) *the recipients or categories of recipients of the personal data, if any*; *and* e) *the means of exercising the rights set out in Article 9, Convention 108+ as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.*

2. *Paragraph 1 shall not apply where the data subject already has the relevant information.*

3. *Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts*».

[32] L'*Explanatory Report* è allegato alla Convenzione n. 108+, consultabile al seguente indirizzo: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (ivi, pp. 15 ss.).

[33] In tale ambito, il par. 49 rimarca che: «*The concept of compatible use should not hamper the* transparency*, legal certainty,* predictability *or fairness of the processing. Personal data should not be further processed in a way that the data subject might consider unexpected, inappropriate or other-*

67 e 68 evidenziano, infine, come solo la completa comprensione sia delle caratteristiche del trattamento sia del novero dei diritti dell'interessato, riservatigli dalla disciplina in esame, consente a quest'ultimo di esercitare in modo pieno quell'autodeterminazione informativa in cui si sostanzia il diritto alla protezione dei dati personali; ne deriva che il titolare ha l'obbligo di agire in modo trasparente e proattivo, fornendo le informazioni essenziali in modo accessibile, comprensibile e adeguato rispetto all'interessato, al fine di consentirgli il pieno esercizio dei propri diritti[34].

1.3. Ancora sulla trasparenza nel GDPR come principio del diritto europeo in materia di protezione dei dati

Come già ricordato nella parte iniziale del presente contributo, sebbene il principio di trasparenza sia stato espressamente enunciato dall'art. 5 del Reg. UE n. 679/2016 (unitamente al principio di liceità e correttezza), si può notare che nelle disposizioni del Regolamento il concetto stesso di trasparenza non sia stato specificamente definitivo: i confini interpretativi di tale principio vanno dunque individuati dall'interprete. Di ausilio, a tal fine, è senz'altro il *considerando* n. 39, ai sensi del quale «dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un

wise objectionable. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data is initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia, any link between those purposes and the purposes of the intended further processing; the context in which the personal data has been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to its further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations».

[34] I par. 67 e 68 precisano che «*The controller is required to act transparently when processing data in order to ensure fair processing and to enable data subjects to understand and thus fully exercise their rights in the context of such data processing*» (par. 67) e che «*Certain essential information has to be compulsorily provided in a proactive manner by the controller to the data subjects when directly or indirectly (not through the data subject but through a third-party) collecting their data, subject to the possibility to provide for exceptions in line with Article 11 paragraph 1. Information on the name and address of the controller (or co-controllers), the legal basis and the purposes of the data processing, the categories of data processed and recipients, as well as the means of exercising the rights can be provided in any appropriate format (either through a website, technological tools on personal devices, etc.) as long as the information is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (for example, in a child friendly language where necessary). Any additional information that is necessary to ensure fair data processing or that is useful for such purposes, such as the preservation period, the knowledge of the reasoning underlying the data processing, or information on data transfers to a recipient in another Party or non-Party (including whether that particular non-Party provides an appropriate level of data protection, or the measures taken by the controller to guarantee such an appropriate level of data protection) is also to be provided*» (par. 68).

linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguarda».

Il principio di trasparenza risulta essere un principio più personalistico che legalistico, incentrato sull'utente prima e sull'interessato poi, che si concreta in specifici obblighi a carico di titolari e responsabili e viene declinato in tre elementi essenziali: la correttezza delle informazioni rese all'interessato nel momento della raccolta dei dati, le modalità con cui il titolare informa l'interessato dei suoi diritti, le modalità con cui l'esercizio di questi diritti viene agevolato e garantito dal titolare stesso[35].

Il principio in commento risulta essere criterio ispiratore di una serie di ulteriori innovazioni presenti nel Reg. UE n. 679/2016: i maggiori requisiti di chiarezza negli obblighi informativi declinati negli artt. 12, 13 e 14, la portata più ampia che assumono il diritto di accesso ai dati personali e l'esercizio dei diritti di cui agli artt. 15-22, i più stringenti requisiti in materia di consenso enunciati nell'art. 7.

Quanto agli obblighi informativi del titolare, già nell'art. 5 viene espressa la correlazione tra il principio di correttezza e il principio di trasparenza che trovano la loro più ovvia espressione nella informativa quale strumento atto a formare un consenso che sia libero e consapevole.

Il *considerando* n. 58 esplicita funzioni e contenuto dell'informativa precisando che «il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione[36]. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito *web*. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità *online*. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente»[37].

---

[35] È in particolare l'art. 12 del Reg. UE n. 679/2016 a declinare il principio di trasparenza nei tre elementi essenziali indicati nel testo, prescrivendo le modalità con le quali il titolare deve rendere l'informativa *ex* artt. 13 e 14, rispondere alle richieste di esercizio dei diritti da parte dell'interessato ai sensi degli artt. 15-22 e comunicare, ove necessario, la violazione dei dati *ex* art. 34.

[36] Sul punto il *considerando* n. 60 indica che le informazioni «possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico». Sull'utilizzo delle icone, l'Autorità Garante per la Protezione dei Dati Personali è stata un precursore, prevedendo tali esemplificazioni nei Provvedimenti dell'8 aprile 2010 sulla Videosorveglianza e del 7 marzo 2013 sulla geolocalizzazione dei veicoli aziendali.

[37] Rispetto alle attività *online*, il GPDP prescrive l'utilizzo di informative «su più livelli» o «multistrato» sia per la profilazione (*Linee guida in materia di trattamento di dati personali per profilazione*

I contenuti dell'informativa prescritti dagli artt. 13 e 14 del Reg. UE n. 679/2016 sono più ampi rispetto alle previgenti disposizioni: il titolare del trattamento deve, infatti, fornire indicazioni in merito al Responsabile per la protezione dei dati (se nominato), al periodo di conservazione, alle condizioni per il trasferimento dei dati verso paesi od organizzazione Extra UE, alla base giuridica del trattamento.

Il concetto di trasparenza nella accezione contemporanea ed innovativa del Reg. UE n. 679/2016 ci consegna un ulteriore profilo degno di nota: quello temporale. Difatti la trasparenza rileva anche sotto il profilo del tempo entro cui l'interessato deve ricevere le comunicazioni che, ai sensi dell'art. 12, par. 3, debbono essere rese dal titolare «(…) senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa» indicando un indubbio criterio di tempestività con cui il titolare deve adempiere, a meno di opportuna giustificazione[38]. Gli artt. 13 e 14 stabiliscono precise tempistiche per il rilascio dell'informativa nelle diverse fattispecie in cui i dati sono o non sono ottenuti presso l'interessato: nel primo caso, una prima parte di informazioni (quelle indicate dal primo comma dell'art. 13) deve essere fornita «nel momento in cui i dati personali sono ottenuti»[39], mentre la comunicazione di ulteriori informazioni – quali quelle relative alla conservazione, ai diritti dell'interessato ecc. – può essere posticipata ad un (non meglio precisato) momento successivo alla raccolta dei dati.

È il terzo paragrafo dell'art. 14 a definire le tempistiche di rilascio delle informazioni non acquisite presso l'interessato come segue: «*a)* entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali».

Rispetto all'esercizio dei diritti dell'interessato, il principio di trasparenza si lega al principio di responsabilizzazione[40] del titolare del trattamento: l'informazione sul trattamento dei dati personali, secondo i contenuti e nel rispetto delle tempistiche testé citati, costituisce il fondamento per esercitare i diritti di gestione e controllo riconosciuti all'interessato. Non solo: la trasparenza deve essere rispettata anche nelle modalità di riscontro rispetto ai diritti[41].

---

on line, 2015) che per l'utilizzo dei *cookie* (*Linee guida cookie e altri strumenti di tracciamento*, 2021).

[38] Il terzo paragrafo dell'art. 12 dispone che «tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta».

[39] Quindi in via preventiva o per lo meno contestuale alla raccolta dei dati.

[40] Tale principio è declinato nel secondo paragrafo dell'art. 5 del Reg. UE n. 679/2016: «Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")».

[41] Il *considerando* n. 63 del Reg. UE n. 679/2016 precisa sul punto «Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni

L'esercizio consapevole dei propri diritti si riferisce, in modo più specifico, al consenso che l'art. 4, par. 1, n. 11 definisce come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». Appare chiaro come il principio di trasparenza operi tanto rispetto al contenuto delle informazioni fornite dal titolare, quanto in relazione alle modalità con cui il consenso deve essere acquisito[42]: l'art. 7 del Reg. UE n. 679/2016 prevede in modo espresso che «se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante». Vi è quindi un contemperamento fra il principio di libertà di forma e gli strumenti attraverso i quali viene garantita la formazione di un consenso libero e consapevole[43].

Alla luce di quanto precede, la trasparenza si rivela principio di ampia portata, che permea tutta la durata del trattamento, potendo esso spingersi anche oltre la fine del rapporto contrattuale sottostante (basti pensare alle norme collegate alla *data retention*), oltre ad avere un taglio trasversale con impatti notevoli sugli altri principi di cui costituisce la base fondamentale.

---

quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il *software*. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce».

[42] Il *considerando* n. 32 del Reg. UE n. 679/2016 precisa, in particolare, che «Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito *web*, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

[43] Sul punto cfr. F. CAGGIA, *Condizioni per il consenso*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *op. cit.*, p. 218.

Fra tutti, il principio di limitazione delle finalità: «l'esplicitezza delle finalità» è un concetto «strettamente connesso al principio di trasparenza (*considerando* n. 39) e si esplica nell'obbligo di informare il soggetto interessato in merito alle finalità del trattamento (…) ed avvisarlo in caso di nuove finalità (…)»[44].

Infine, la trasparenza è centrale ove occorra una violazione dei dati suscettibile di presentare un rischio elevato per i diritti e le libertà dell'interessato. L'art. 34 impone, infatti, al titolare del trattamento di descrivere all'interessato, senza ingiustificato ritardo e con un linguaggio semplice e chiaro, la natura della violazione, le probabili conseguenze e le misure adottate o adottande, fornendo altresì i riferimenti di contatto (siano essi relativi al Responsabile della protezione dei dati o ad altro soggetto) al fine di consentire all'interessato stesso una più completa e dedicata informazione.

2. Portata del principio

2.1. Contenuti del principio di trasparenza

Come già precisato nel precedente par. 1, la trasparenza costituisce un elemento fondamentale degli ulteriori principi elencati dall'art. 5, par. 1, lett. *a)* del Reg. UE n. 679/2016, con i quali presenta evidenti connessioni.

Ad esso però va attribuita un'autonomia, avendo contenuti propri che attengono, innanzitutto, alla veicolazione di informazioni, al loro successivo accesso, alla loro completezza e chiarezza.

L'onere informativo, di cui il principio di trasparenza costituisce un presupposto, si può ritenere correttamente adempiuto ove l'interessato abbia compreso le informazioni ricevute e sia consapevole degli effetti del trattamento, anche nella prospettiva del successivo utilizzo delle informazioni medesime.

In tale contesto, la trasparenza è altresì intesa come «dovere di *clare loqui*» posto a carico del titolare del trattamento, ossia un dovere di adottare un linguaggio semplice e chiaro[45]. La violazione di tale dovere porta alla illiceità del trattamento, almeno nel caso in cui è richiesto il consenso come manifestazione di volontà libera, consapevole ed inequivocabile dell'interessato.

Ne deriva che il principio di trasparenza riguarda tanto le informazioni fornite al soggetto prima dell'inizio del trattamento[46], quanto le informazioni a cui il soggetto interessato deve avere facile accesso nel corso del trattamento, e si riferisce infine

[44] G. Malgieri, *I principi (comm. art. 5 GDPR)*, cit., p. 185 (con particolare riferimento ivi, al par. 5, dedicato al principio di limitazione della finalità.

[45] Sulle differenti declinazioni della trasparenza si veda G. Di Lorenzo, *La circolazione dei dati personali tra tutela della persona e ordine giuridico del mercato,* in *Federalismi.it*, 2019, 21. L'A. sottolinea come nella accezione di *clare loqui* la trasparenza non sia un criterio predeterminabile in astratto e univoco, ma variabile in base alla tipologia del destinatario di riferimento (da qui la speciale trasparenza da adottare nel caso di informazioni destinate in maniera specifica ai minori).

[46] Quindi in una fase precedente all'acquisizione dello *status* di interessato.

alle informazioni che, in seguito all'esercizio del diritto di accesso, vengono messe a disposizione dell'interessato.

Come rilevato dal Gruppo di lavoro *ex* art. 29 nelle «Linee guida sulla trasparenza ai sensi del regolamento 2016/679» (versione emendata adottata l'11 aprile 2018) «i principi di correttezza e responsabilizzazione di cui al regolamento impongono al titolare del trattamento di decidere il momento in cui fornire le informazioni di cui all'articolo 14 considerando sempre le ragionevoli aspettative degli interessati e l'effetto che il trattamento potrebbe avere sugli stessi e sulla loro capacità di esercitare i diritti di cui godono in relazione al trattamento».

Da una più ampia prospettiva, la trasparenza si sostanzia nel Reg. UE n. 679/2016 in un obbligo trasversale che si esplica attraverso (i) la fornitura agli interessati delle informazioni in relazione alle attività di trattamento, (ii) le modalità con le quali il titolare del trattamento comunica agli interessati i contenuti dei loro diritti[47], (iii) le modalità con le quali il titolare del trattamento agevola l'esercizio dei diritti da parte degli interessati[48].

Appare chiaro che il principio di trasparenza permea «tutto il ciclo di vita del trattamento»[49] e consente al titolare di dimostrare il rispetto degli obblighi che il Reg. UE n. 679/2016 impone, in ragione del principio di responsabilizzazione di cui all'art. 5, par. 2. Proprio per le caratteristiche che essa racchiude, si sostiene che la trasparenza possieda una «virtualità multipla»[50].

In un'ottica di prevenzione, riduzione ed eliminazione di possibili violazioni nel Reg. UE n. 679/2016 emerge, a differenza del passato, un approccio di tipo proattivo. Più in particolare, nella innovativa impostazione del Reg. UE n. 679/2016, il titolare deve valutare autonomamente e secondo un approccio basato sul rischio quali misure tecniche ed organizzative siano adeguate al fine di ottenere una efficace protezione dei dati, consentendo all'interessato, proprio grazie all'applicazione di tali misure, la comprensione delle attività e finalità di trattamento e l'esercizio dei diritti di controllo e gestione dei dati personali.

Il rispetto del principio di trasparenza si esplica, inoltre, attraverso la protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita *(privacy by default*) durante l'intero ciclo di vita del trattamento, come dispone l'art. 25 del Reg. UE n. 679/2016. Infatti, come chiarito dall'EDPB nelle Linee guida n. 4/2019 in tema di *privacy by design* e *by default*, gli elementi chiave della progettazione e dell'impostazione predefinita dovrebbero includere: «chiarezza – le informazioni sono fornite in un linguaggio chiaro e semplice, conciso e comprensibile; semantica – la comunicazione deve avere un significato chiaro per il pubblico a cui è rivolta; accessibilità – le informazioni sono facilmente accessibili per l'interessato; contestualità – le informazioni devono essere fornite al momento opportuno e nella

[47] Cfr. artt. 12-13-14 GDPR.

[48] In questo senso, Gruppo di Lavoro ex Art. 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679 WP260 rev.01,* documento disponibile su Internet all'indirizzo https://ec.europa.eu/newsroom/article29/items/622227 (consultato da ultimo in data 3 aprile 2023).

[49] *Ibidem.*

[50] L. Califano, *Trasparenza e privacy nell'evoluzione dell'ordinamento costituzionale*, in *Giornale di storia costituzionale*, 2016, 31, p. 77.

forma adeguata; pertinenza – le informazioni devono essere pertinenti e applicabili all'interessato specifico; progettazione universale – le informazioni sono accessibili a tutti gli interessati, compreso l'utilizzo di linguaggi leggibili da una macchina per agevolare e automatizzare la leggibilità e la chiarezza; comprensibilità[51] – gli interessati devono avere una buona comprensione di ciò che possono aspettarsi dal trattamento dei loro dati personali, in particolare quando si tratti di minori o di soggetti appartenenti ad altre categorie vulnerabili; multicanalità – le informazioni dovrebbero essere fornite attraverso canali e mezzi di comunicazione diversi, non solo quelli testuali, per aumentare la probabilità che raggiungano efficacemente l'interessato; approccio multilivello – le informazioni devono essere fornite secondo un approccio multilivello, in modo da garantire un equilibrio tra completezza e comprensibilità, rispecchiando le ragionevoli aspettative degli interessati»[52].

Nella struttura del Reg. UE n. 679/2016 la trasparenza si pone, quindi, nella duplice veste di tutela *ex post* – già nota in ambito pubblico tramite la regolamentazione del diritto di accesso[53], quasi con funzione di controllo della correttezza dell'azione amministrativa – e di tutela *ex ante*, quale elemento che ha caratteri di innovatività.

L'ampiezza della portata del principio di trasparenza si coglie ponendoci proprio nella prospettiva dell'interessato: non è mero adempimento previsto *ex lege*; la trasparenza è, piuttosto, un principio che permea l'intero ciclo di vita del trattamento e si pone anche come condizione che consente l'effettiva conoscenza sul contenuto delle attività di trattamento (quali sono i soggetti coinvolti, quali i mezzi e le finalità, ecc.) e, conseguentemente, la consapevolezza dell'interessato rispetto all'impatto che tali attività hanno sul diritto alla protezione dei dati e alle azioni a tutela del medesimo[54].

---

[51] Sul punto cfr. pagina informativa della *Commission Nationale De L'informatique Et Des Libertés* sul principio di trasparenza, nella quale si precisa: «*Il n'y a pas une seule façon de bien informer les personnes. Cette information doit être: adaptée aux situations et aux supports de collecte; accessible et compréhensible. Le RGPD pousse ainsi à la mise en place de solutions innovantes. Une approche combinant différentes modalités d'information, par étapes complémentaires, permet d'atteindre l'objectif de transparence*», disponibile su Internet all'indirizzo https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence (consultato da ultimo il 3 aprile 2023).

[52] Cfr. EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita Versione 2.0*, adottate il 20 ottobre 2020, documento disponibile su Internet all'indirizzo https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf (consultato da ultimo il 3 aprile 2023).

[53] Per un approfondimento si rinvia al par. 2.4.

[54] Come indicato da P. Hayes, *An ethical intuitionist account of transparency of algorithms and its gradations*, in *Business Research*, 2020, p. 850, nella sua accezione descrittiva, la trasparenza può essere descritta come «*a state of affairs conducive to the acquisition of knowledge about some X (for instance, an algorithm) characterised by availability, accessibility, findability and understandability/explainability of relevant information*», e come tale «*transparency connotes the availability, accessibility, and findability of information as part of its visibility component, and understandability or explainability of this information as a part of the understandability component. If something is visible, and understandable, it promotes knowledge, which is an important intrinsic moral value. The moral value of transparency is, therefore, tied instrumentally to its potential for leading to knowledge creation and dissemination. When something is transparent, it can be known, which is*

2.2. Principio di trasparenza, diritti dell'interessato e obblighi di informazione in relazione alle attività di trattamento. Connessione tra principio di trasparenza e principio di liceità

La Sezione 1 del Capo III del Reg. UE n. 679/2016, intitolata «Trasparenza e modalità», delinea gli ambiti di applicazione del principio di trasparenza nelle fasi del «ciclo di vita del trattamento» [55], ossia in relazione ai contenuti delle informazioni, ai mezzi, all'esercizio dei diritti. Più in particolare, l'art. 12 del Reg. UE n. 679/2016[56] definisce i criteri attraverso i quali si concretizza la trasparenza (e quindi la correttezza e la liceità) dei contenuti e delle informazioni che il titolare deve trasferire all'interessato sia nella fase di raccolta dei dati che nella fase eventuale di esercizio dei diritti da parte dell'interessato.

Le informazioni devono essere:

(i) coincise, trasparenti, intelligibili e facilmente accessibili;
(ii) fornite con un linguaggio semplice e chiaro;
(iii) fornite per iscritto o con altri mezzi, anche oralmente o attraverso icone;
(iv) fornite gratuitamente;
(v) fornite nel rispetto di una determinata tempistica.

Il dovere di trasparenza va inteso in una duplice prospettiva, l'una sostanziale – riferita alla chiarezza delle informazioni – l'altra funzionale, relativa al percorso che l'interessato deve seguire per raggiungere le informazioni[57]. In questo senso è

---

good in itself, but also if it can be known, it can be acted upon or responded to in appropriate ways. Therefore, knowledge itself has instrumental features which are commonly necessary to promote the values traditionally associated with transparency, for instance, human dignity».

[55] Gruppo di Lavoro ex Art. 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679 WP260 rev.01,* documento disponibile su Internet all'indirizzo https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=622227 (consultato da ultimo in data 3 aprile 2023).

[56] All'art. 12 («*Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato*»), par. 1-2-3, GDPR, viene stabilito che «1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.
3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato».

[57] L. Aulino, *Consenso al trattamento dei dati e carenza di consapevolezza: il* legal design *come un rimedio ex ante,* in *Dir. inf.*, 2020, 2, p. 303.

intervenuta in più occasione l'Autorità Garante per la protezione dei dati personali, sottolineando come il linguaggio debba essere adeguato rispetto all'interlocutore-interessato[58] e promuovendo l'uso di infografiche in modo da migliorare la *user experience* nel rinvenimento delle informazioni sul trattamento[59].

A tal riguardo è utile sottolineare anche la posizione del Gruppo di lavoro *ex* art. 29 sull'importanza del principio di trasparenza rispetto ai minori, là dove s'è rimarcato che «la trasparenza è un diritto a sé stante, che si applica tanto ai minori quanto agli adulti. Il Gruppo sottolinea in particolare che i minori non perdono i loro diritti alla trasparenza in quanto interessati semplicemente per il fatto che il consenso è stato dato/autorizzato dal titolare della responsabilità genitoriale in una situazione in cui trova applicazione l'articolo 8 del regolamento. Sebbene in molti casi tale consenso sia concesso o autorizzato *una tantum* dal titolare della responsabilità genitoriale, il minore (come qualsiasi altro interessato) gode di un diritto permanente alla trasparenza per tutta la durata del rapporto con il titolare del trattamento»[60].

Nell'ambiente digitale, caratterizzato dalla velocità con cui le informazioni sono scambiate e dalla complessità (e sempre crescente innovazione) delle tecnologie in uso[61], è fondamentale facilitare l'accesso alle informazioni e la loro chiarezza. Il *legal design*[62] può essere considerato un utile strumento a difesa degli utenti e a tutela dei consumatori: «il *legal design*, infatti, può trovare un compromesso tra la necessità di facilitare l'uso del servizio e l'offrire un'esperienza, accessibile e trasparente. Emerge, ancora una volta, l'esigenza di garantire l'interesse del consumatore/interessato, non solo di ricevere le informazioni, ma di comprenderne effettivamente il significato»[63].

---

[58] In particolar modo per quanto attiene ai minori, anche attraverso specifiche campagne di informative e di *awareness* presenti sul sito del GPDP al seguente *link* https://www.garanteprivacy.it/temi/minori (consultato da ultimo in data 3 aprile 2023).

[59] Da ultimo, si segnala il *contest* dal titolo «Informative privacy più chiare grazie alle icone? È possibile», indetto dal GPDP, disponibile al *link* https://www.garanteprivacy.it/temi/informativechiare (consultato da ultimo in data 3 aprile 2023).

[60] Cfr. Gruppo di Lavoro ex Art. 29, *op. cit.*, p. 10.

[61] «*For the average citizen, navigating the digital ecosystem in search of their data may feel overwhelming. The complexity involved in data collection creates a cloud of opacity around understanding where one's data entered the ecosystem, its trajectory, and who to reach out to for access to this data. Taking on this endeavor alone can be daunting, if not impossible*». Così P.O Dehaye-I. Hahn-G. Jargalsaikhan, *Platforms and personal data processing: the potential for achieving systemic transparency*, in *Personal Data.IO,* disponibile in formato elettronico al *link* https://ssrn.com/abstract=3552930 (consultato da ultimo in data 3 aprile 2023).

[62] L. Aulino, *op. cit*. Secondo l'Autore «questa nuova disciplina, attraverso un approccio pratico ed una metodologia proattiva *ex ante*, coniuga diritto, tecnologia, etica, filosofia, semiotica e comunicazione. La tecnologia fa da ponte tra diritto e comunicazione, nella realizzazione delle icone visive che, attraverso il *design*, aiutano l'utente a comprendere il concetto legale secondo i principi di trasparenza e chiarezza. Ne consegue che la redazione di informative *privacy* attraverso l'uso delle metodologie della *user experience* (UX) e dell'*interaction design*, quali tecniche delle scienze comportamentali, congiuntamente ai principi del diritto civile, facilitano *ex ante* le operazioni di comprensione dell'utente, rendendo espliciti i vincoli e gli oneri più rilevanti nell'interesse dell'interessato».

[63] L. Aulino, *op. cit*.

La trasparenza delle informazioni relative alle attività di trattamento, nel duplice significato appena delineato, impatta anche sulle condizioni di liceità come indicate agli artt. 6 e 9 del Reg. UE n. 679/2016. È evidente che, in assenza di una chiara informazione sulle singole attività di trattamento e sulla correlata base giuridica, l'interessato non può essere in grado (o lo può essere solo parzialmente) di determinarsi[64] sul conferimento dei dati e, in modo particolare, sull'eventuale consenso al trattamento: «se il titolare del trattamento non fornisce informazioni accessibili, il controllo dell'utente diventa illusorio e il consenso non costituirà una base valida per il trattamento»[65].

Nell'economia *data driven*[66] il dato personale – o, meglio, la facoltà di un suo utilizzo[67] – assume una ulteriore (e diversa) funzione di scambio commerciale rispetto ai servizi e prodotti offerti[68]: «non più la merce ma il dato incorpora, infatti, una relazione tra persone e assume il ruolo tradizionalmente svolto da capitale e lavoro, nella sua duplice veste, tuttavia, di risorsa economica e di oggetto di un diritto fondamentale»[69].

---

[64] Al riguardo s'è evidenziato che «*Above all transparency constitutes a substantial founding principle of data protection strictly interrelated with fairness. Unless individuals are provided with appropriate information and control, they "will be subject to decisions that they do not understand and have no control over". A normative view on algorithmic transparency implies that such systems may only be used if their underlying reasoning can be (adequately) explained to users*». Così L. MITROU, *Data protection, artificial intelligence and cognitive services. Is the general data protection regulation (GDPR) "artificial intelligence-proof"?*, disponibile in formato elettronico al *link*: https://ssrn.com/abstract=3386914 (consultato da ultimo in data 3 aprile 2023).

[65] GRUPPO DI LAVORO EX ART. 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, WP 259 rev. 01*, adottate il 28 novembre 2017, modificate e adottate da ultimo il 10 aprile 2018, disponibili al *link* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (consultato da ultimo in data 3 aprile 2023).

[66] Si parla di "datificazione" per identificare il processo di trasposizione in dati dei fenomeni che caratterizzano la società per successiva elaborazione. Sul punto ed in relazione agli impatti dell'intelligenza artificiale cfr. L. MITROU, *op. cit.*: «*To a great extent the rapid evolution of Artificial Intelligence is to be attributed to the exponential growth of "datafication". In the two first decades of 21st century the confluence of machine learning and the large datasets results to an increased number of products and services, in public and private sector, in any kind of application. What is making Artificial Intelligence the major trigger for the "Fourth Industrial Revolution" is not only, though primarily, the ever more sophisticated technological potential and the availability and processability of vast amount of data but also the fact that AI is no more "the domain of a few nerdy specialists working mainly in academia, financial services or large marketing departments". The AI research is shifting from being driven by academic curiosity to being driven by economic and social demands. The AI developments can be found across the full range of business activities. AI is becoming a reality. In their everyday professional and private life people are dealing increasingly with AI artefacts*».

[67] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, pp. 110 ss.

[68] Per un esame dell'approccio negoziale ai dati personali, G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf.*, 2020, 3, p. 634.

[69] GPDP, *Relazione annuale per il 2018. Discorso del Presidente Antonello Soro*, Roma, 7 maggio 2019 disponibile al *link* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9109221 (consultato da ultimo in data 3 aprile 2023).

Questa ulteriore funzione, anche negoziale, consente di ampliare le prospettive di tutela del consumatore-interessato, rafforzando il principio di trasparenza quale obbligo del fornitore di informare l'utente, in modo chiaro e completo, dell'utilizzo commerciale dei suoi dati personali[70]. Come indicato nelle sentenze del TAR Lazio, sez. I, 10 gennaio 2020 n. 260 e 261, «il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un social *network*»[71].

Ritornando al rapporto fra principio di trasparenza e consenso, l'art. 7, par. 4 del Reg. UE n. 679/2016 pone quale elemento di valutazione della condizione di liceità la subordinazione dell'esecuzione di un contratto alla prestazione del consenso che non sia necessario ai fini dell'esecuzione stessa di tale contratto. Pur non essendo la subordinazione vietata *tout court* dalla disposizione in commento[72] la stessa «è posta come un campanello dall'allarme, un indizio sintomatico di una negoziazione del trattamento dei dati che potrebbe non essere ammessa»[73].

---

[70] Non si può trascurare il fatto che in alcuni ambiti digitali, in particolare con l'utilizzo dei *big data*, le finalità del trattamento possono essere determinate solo *ex post*, all'esito della rielaborazione e analisi dei dati. In questo senso, cfr. A. Fedi, *Big data and AI: an issue for general law and data protection*, in *Jus Civile*, 2020, 1, p. 169: «*The third related issue is that the data controller should be able to inform the customer of all uses of his/her data but nobody can precisely define that at that stage, also because the inferred knowledge that data analytics will provide (and the uses of those knowledge once it has emerged) is unknown before the analytics is done and the outcome of the analysis is delivered. The data analytics will in other terms often shed light on unexpected correlations or patterns and, only once those correlations have emerged (ex post), their value and the potential use of those will become clear. (…) Large amounts of different data are put in the turbine of data analytics and unexpected and non-searched correlations emerge, which of course have a value but were not intended to be found. But then, if it is so, how can a controller inform the data subject on consequences of the processing when the outcomes of the analytics are defined only at the end of the process and not before?* ».

[71] Per un commento critico alle sentenze citate v. F. Bravo, *La «compravendita» di dati personali?*, in *Diritto di Internet*, 2020, 3, pp. 521-540. Le pronunce erano state rese dal TAR a seguito dell'impugnazione del provvedimento sanzionatorio reso dall'AGCM n. 27432/2018 con cui era stata ravvisata una condotta censurabile ai sensi della disciplina in tema di pratiche commerciali scorrette nei confronti di Facebook. Le pronunce del TAR hanno trovato una conferma innanzi al Consiglio di Stato, con sent. n. 2331/2021.

[72] Cfr., in tal senso, Cass., sez. I, sent. n. 17218/2018, su cui si veda, segnatamente, F. Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, n. 1, pp. 34-58.

[73] G. D'ippolito, *op. cit.* L'Autore sottolinea che «il trattamento dei dati basato sul contratto o, meglio e secondo le parole della norma richiamata, "l'esecuzione del contratto" non dovrebbe, in astratto, essere condizionato (c.d. *tying*). Se così fosse, ben potranno le Autorità di controllo sindacare la necessità dei trattamenti coinvolti, il loro condizionamento al consenso, la libertà dello stesso e, quindi, la validità del rapporto obbligatorio e dell'operazione negoziale. In altre parole, fermo restando che la subordinazione al consenso del trattamento basato sul contratto non è dalla norma vietato *tout court* (ma "tenuto nella massima considerazione"), la stessa è posta come un campanello dall'allarme, un indizio sintomatico di una negoziazione del trattamento dei dati che potrebbe non essere

La crescente importanza del trattamento dei dati personali nell'ambito dei servizi della società dell'informazione sembra – ad oggi – non essere accompagnata da una adeguata trasparenza e accessibilità delle informazioni sulle attività di trattamento e i relativi diritti esercitabili dall'interessato[74]: come rilevato dall'Autorità Garante per la protezione dei dati personali nelle «Linee guida su cookie e altri strumenti di tracciamento» del 10 giugno 2021, «deve essere tenuta in considerazione l'evoluzione comportamentale degli stessi utenti della rete, sempre più orientati alla moltiplicazione delle proprie identità digitali come risultanti dall'accesso a plurimi servizi e funzioni disponibili e, in primo luogo, ai *social network*. Tale fenomeno comporta infatti il rischio che le informazioni personali oggetto di trattamento siano raccolte proprio incrociando i dati anche relativi all'utilizzo di funzionalità e servizi diversi, ai quali è possibile accedere utilizzando molteplici terminali (cd. *enrichment*), con l'effetto della creazione di profili sempre più specifici e dettagliati. Si impone, di conseguenza, la necessità di un quadro rafforzato di tutele maggiormente orientate a favorire e a rendere effettivo il controllo sulle informazioni personali oggetto di trattamento e, in definitiva, la capacità di autodeterminazione del singolo».

2.3. Ancora su principio di trasparenza e diritti dell'interessato

L'interessato dispone di una serie di diritti di accesso, gestione e controllo sui dati personali[75] disciplinati dagli articoli da 15 a 22 del Reg. UE n. 679/2016. L'esercizio di tali diritti ha come presupposto la completezza, l'accessibilità e la comprensibilità delle informazioni, come indicato nei precedenti paragrafi, ma la sua efficacia può essere misurata solo in rapporto alle singole esigenze e alla fattispecie concreta e, comunque, in relazione ai singoli specifici diritti dell'interessato.

Parte di tali diritti (segnatamente i diritti di comunicazione, informazione e accesso di cui agli artt. 12, 13, 14, 15, 22 e 34 del Reg. UE n. 679/2016) mirano a realizzare il principio di trasparenza, in funzione dell'esercizio di poteri di controllo e di intervento sul trattamento riconosciuti da altri diritti dell'interessato (si pensi,

ammessa. Sebbene non dia particolari indicazioni utili per l'interprete, la norma sembrerebbe comunque porre una presunzione relativa di illiceità, un'ipotesi di vizio della volontà che renderebbe il consenso non effettivo e il relativo trattamento illecito». La citata sentenza della Cass. n. 17218/2018 rimarca tuttavia la differenza tra vizi di volontà, in ambito contrattuale, e nullità del consenso reso dall'interessato in materia di protezione dei dati personali.

[74] Per una interessante analisi sul rispetto della normativa relativa alla protezione dei dati personali nei *social network sites* cfr. A.R. Popoli, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *Diritto dell'Informazione e dell'Informatica*, 2019, 6, p. 1289.

[75] A.R. Popoli, *op. cit.* «L'interessato non è un soggetto che passivamente subisce le operazioni di trattamento effettuate sui propri dati personali; al contrario, egli vanta un ampio potere di controllo e di intervento sui dati personali che si declina lungo specifiche prerogative, le quali sono esercitabili senza particolari formalità. Attraverso il controllo sulle proprie informazioni, la persona determina le modalità di costruzione della propria dimensione individuale. I diritti dell'interessato rappresentano, quindi, declinazioni della più generale pretesa del singolo di potersi proiettare liberamente nel mondo attraverso le proprie informazioni, mantenendo, purtuttavia, il controllo sul modo in cui queste informazioni circolano e vengono utilizzate, indipendentemente dalla sussistenza di una violazione».

ad esempio, al diritto alla cancellazione, al diritto di opposizione e di limitazione, nonché al diritto alla portabilità dei dati).

A tal riguardo va altresì tenuto presente che, in base al principio di *accountability*, il titolare del trattamento ha l'obbligo non solo di rispettare i diritti dell'interessato, ma anche di adottare «misure tecniche e organizzative» appropriate per assicurare, a monte, che l'interessato possa concretamente esercitare tali diritti e possa dunque essere destinatario delle comunicazioni e delle informazioni relative ai diritti di cui agli articoli da 12 a 22 e 34 del Reg. UE n. 679/2016. Per consentire il rispetto di tale obbligo, il titolare deve – ad esempio – dotarsi di procedure interne di gestione e di un adeguato apparato organizzativo, nonché tracciare i flussi di dati, così determinando le specifiche attività che impattano sui dati personali e l'ambito del trattamento affidato a (eventuali) responsabili del trattamento, soggetti autorizzati, destinatari, ecc. Il principio di trasparenza, infatti, si rende effettivo – nelle logiche dell'*accountability* e del corretto adempimento degli obblighi speculari ai diritti dell'interessato – anche attraverso la corretta definizione dei "ruoli *privacy*", in cui inquadrare i soggetti che vengono coinvolti a diverso titolo nelle attività di trattamento, e dei compiti loro assegnati.

Va poi considerato il contesto nel quale vengono esercitati i diritti dell'interessato nel quale la trasparenza entra in rilievo: si pensi, ad esempio, ad un'istanza di accesso presentata in contesti in cui l'esercizio del diritto da parte dell'interessato e il riscontro da parte del titolare possono risultare più difficoltosi, in particolare se si tratta di attività *online*[76], *social network*[77] o utilizzo di *Big Data*[78].

---

[76] Per un'analisi sul ruolo privacy delle piattaforme e del relativo impatto sul raggiungimento della trasparenza cfr. P.O Dehaye-I. Hahn-G. Jargalsaikhan, *Platforms and personal data processing: the potential for achieving systemic transparency*, in *Personal Data.IO*, disponibile in formato elettronico al *link* https://ssrn.com/abstract=3552930 (consultato da ultimo in data 3 aprile 2023): «*The authors' experience so far has revealed a tendency for platforms to respond that they are simply a processor, and that the data subject should instead contact the data controller. As explained earlier, one could argue this renders the access right ineffective by denying to the data subject the ability of reaching scale, and that this is a failure by the platform in their duty of care and fairness towards the data subject. Platforms also tend to have an interest in not contractually accounting for the data breadcrumbs that are core to their business models, as it allows them to easily repurpose data without the need to change their contracts with a multitude of apps. A void thus emerges that can be exploited on behalf of the data subject: a more precise accounting of the data collected by platforms can challenge the notion that the platform merely acts as a processor*».

[77] Sull'adeguata protezione dei dati personali da parte di Facebook rispetto al trasferimento gli Stati Uniti d'America cfr. la sentenza della CGUE del 16 luglio 2020 che ha invalidato la decisione di adeguatezza "*Privacy Shield*" adottata nel 2016 dalla Commissione europea.

[78] La raccolta e rielaborazione di *Big Data* da parte del titolare può avvenire anche senza contatto diretto con il soggetto interessato, il quale non risulta correttamente informato rispetto alla «filiera del trattamento» e al conseguente soggetto «responsabile» per l'esercizio dei diritti. Nella sostanza, una non corretta gestione dei rapporti fra i titolari può avere un significativo impatto anche in relazione al principio di responsabilizzazione e al regime di tutela applicabile. Cfr. A. Fedi, *Big data and AI: an issue for general law and data protection*, cit., p. 169: «*But in certain instances the Big Data controller first collects data from various sources (social networks, public data, sellers of data bases, large retail businesses), then puts them together and finally makes the analysis without having had any direct relationship with the data subjects. In this second scenario, the data subject should be informed from the beginning (say – from the time he/she subscribes a fidelity card in a shop or*

Resta quindi il problema di rendere effettivo l'esercizio dei diritti dell'interessato – con riferimento, ai fini del nostro discorso, a quelli maggiormente connessi al principio di trasparenza – tenendo conto del particolare contesto tecnologico in cui il trattamento viene effettuato[79]. Sebbene il Reg. UE n. 679/2016 sia una «*technology-independent legislation*»[80], il principio di trasparenza impone al titolare di informare il soggetto interessato sull'esistenza di un processo decisionale automatizzato, compresa la profilazione, e di rendere «informazioni significative sulla logica utilizzata, nonché sull'importanza e le conseguenze previste di tale trattamento per l'interessato» (cfr. art. 13, par. 2, lett. *f)* e art. 14, par. 2, lett. *g)*, Reg. UE n. 679/2016).

L'art. 22 del Reg. UE n. 679/2016 riconosce il diritto di qualsiasi persona a non essere sottoposta a decisioni basate esclusivamente su trattamenti automatizzati di dati, quando tali decisioni possono produrre effetti giuridici o altri impatti significativi sulla vita delle persone stesse. Rispetto a tale disposizione, la rilevanza del principio di trasparenza è ben chiarita dal *considerando* n. 71, dove, fra le misure di garanzia per l'interessato, si include l'obbligo per il titolare di fornire all'interessato specifiche informazioni sul trattamento automatizzato e una spiegazione delle conseguenti decisioni adottate[81].

---

a membership in a social network) that his/her personal data can go through the whole chain from the shop to the distributor to the manufacturer to the Big Data player and, here is the point, the data subject should be informed since that very moment of the purpose for which his/her data will be processed by each player along the chain. The second issue is the legal relationship between controllers down the chain. Are they autonomous controllers, or co-controllers or one is a processor and the other the real controller? Clearly, the liability regime (vis-à-vis data subjects and authorities) may change».

[79] Neanche l'anonimizzazione dei dati, di per sé, può essere considerata *tout court* una soluzione adeguata, ove le tecnologie e i metodi di analisi dei *Big Data* consentano comunque di identificare il soggetto interessato. Cfr. A. Fedi, *op. cit.*: «*With respect to anonymized data, instead, all the legal framework of the GDPR bases on the possibility to draw a clear line distinguishing between personal data and anonym data, but that line appears today tiny, pale and controversial. Here lays the first problem: data may appear anonymized but the great power entrenched in Big Data analysis may decrypt them and re-associate those data to identifiable individuals. The European Data Protection Supervisor indeed recognized that in its Opinion 7/2015 of November 19, 2015: "One result is the emergence of a revenue model for Internet companies relying on tracking online activity. Such Big Data should be considered personal even where anonymization techniques have been applied: it is becoming and will be ever easier to infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media. Furthermore, with the advent of the 'Internet of Things', much of the data collected and communicated by the increasing number of personal and other devices and sensors will be personal data: the data collected by them can be easily related to the users of these devices whose behaviour they will monitor. These may include highly sensitive data including health information and information relating to our thinking patterns and psychological make-up". This is what is otherwise called in literature as 'singling-out': data which are apparently anonymized can be used to retrieve 'personal' data using analytics*».

[80] L. Mitrou, *op. cit.*: « *GDPR does not specifically address AI. Although the difficulties and complexities of digital environments have been taken into account by the designing of the data protection regulatory strategy, the regulatory choice in GDPR consists more in what we perceive as "technology – independent legislation". Refraining from technology-specific terminology and provisions seems to be a conscious choice to be attributed to the "technological neutrality approach"*».

[81] Cfr. *considerando* n. 71 del GDPR: «In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto

Al fine di garantire un trattamento corretto e trasparente il *considerando* n. 71 precisa che «tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione[82], metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello *status* genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni».

Fermo il diritto dell'interessato di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, disciplinato dall'art. 22 del Reg. UE n. 679/2016, le modalità con le quali il titolare agevola l'esercizio dei diritti dell'interessato devono tenere in debita considerazione la protezione di diritti ulteriori rispetto alla riservatezza. È il caso del bilanciamento tracciato dal *considerando* n. 63 del Reg. UE n. 679/2016 fra il diritto di accesso e la protezione dei diritti di proprietà intellettuale e del segreto industriale[83].

Rispetto all'uso degli algoritmi, in particolare, vi sono barriere sia legali – quali quelle poc'anzi elencate in relazione ai diritti di proprietà intellettuale e altre relative alla sicurezza nazionale – sia tecniche, che possono impedire l'effettiva applicazione del principio di trasparenza[84].

---

di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore».

[82] Per un approfondimento sull'utilizzo di processi decisionali automatizzati cfr. N. Muciaccia, *Algoritmi e procedimento decisionale: alcuni recenti arresti della giustizia amministrativa*, in *Federalismi*, 2020, 10.

[83] F. Bravo, *Trasparenza del codice sorgente e decisioni automatizzate*, in *Dir. inf.*, 2020, 4, p. 69: «Per garantire il diritto di accesso funzionale per salvaguardare i diritti fondamentali dell'interessato di fronte ai processi decisionali automatizzati, non si arriva mai ad obbligare il titolare del trattamento a fornire i codici sorgenti per soddisfare il principio di trasparenza, che deve però essere assicurato ugualmente in altro modo. (…) La trasparenza dovrebbe implicare anche la chiarezza e la comprensibilità del linguaggio utilizzato e non l'occasione per carpire segreti industriali a discapito di chi abbia mantenuto, per bando e per contratto, la segretezza del codice sorgente e i diritti di proprietà intellettuale sul *software*».

[84] L. Mitrou, *op. cit.*: «*Legal and procedural responses are necessary to create some necessary conditions for transparency, but technical ones are also needed. In this context, we should not ignore the legal and technical barriers set to algorithmic transparency. Transparency about models and processes may infringe intellectual property rights and trade secrets that may restrict the extent of information to be provide. State secrets and pursue of public interests may present another legal ground for restricting to right to information as they cannot be revealed to the public. An – intrinsic – difficulty in providing information for an artificial intelligence algorithm and its uses lies in the logic behind the machine reasoning that may not be expressible in human terms. Another technical limitation results from design processes that involve some element of randomness produce unpredic-*

Il pervasivo ricorso a servizi e strumenti ICT pone l'ulteriore necessità di concretizzare il principio di trasparenza anche a seguito di una violazione di dati[85]: tale principio è implicitamente richiamato dal secondo comma dell'articolo 34 del Reg. UE n. 679/2016, ai sensi del quale, ove la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve informare l'interessato con «un linguaggio semplice e chiaro». L'obbligo di comunicazione mira a rendere edotto l'interessato sui potenziali rischi relativi ai dati personali ed alla riservatezza, ad offrire gli elementi per interpretare l'accaduto, i riferimenti per ricevere ulteriori informazioni e l'indicazione delle misure che l'interessato stesso può avviare per la propria tutela[86].

Un altro versante nel quale opera la trasparenza riguarda il rapporto di contitolarità del trattamento, che impone ai *joint-controllers* di rendere edotti gli interessati in ordine agli elementi essenziali dell'accordo di contitolarità, in cui sono riportate le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Reg. UE n. 679/2016, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14.

Nel diritto interno vanno poi richiamati due specifici obblighi del titolare del trattamento di informare i propri lavoratori: il primo riferito agli amministratori di sistema, come stabilito dai provvedimenti dell'Autorità Garante per la protezione dei dati personali del 2008 e 2009[87], il secondo relativo a «sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori» regolato dall'art. 4 del d.lgs. 104/2022[88].

---

table results that are not reproductive by design. Furthermore, we have to take into consideration the dynamic nature of algorithms, which are continuously updated and changed».

85 A sensi dell'art. 4, n. 12 del GDPR per una violazione dei dati personali si intende: «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

86 Cfr. *considerando* n. 86 GDPR: «Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione».

87 Cfr. GPDP, Provv. 27 novembre 2008, doc. *web* n. 1577499 e Provv. 25 giugno 2009, doc. *web* n. 1626595.

88 D.lgs 27 giugno 2022, n. 104, attuazione della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea.

Tale ultima disciplina può essere considera quale *lex specialis* «pienamente compatibile con quanto previsto dall'art. 88 del Regolamento, in quanto introduce, a livello nazionale, misure più appropriate e specifiche, con riferimento all'attuazione, nel contesto lavorativo, del principio di trasparenza e garanzie determinate in caso di impiego di sistemi decisionali o di monitoraggio nell'ambito dei rapporti di lavoro»[89].

Fra le informazioni ulteriori rispetto a quelle previste dagli artt. 13 e 14 del Reg. UE n. 679/2016, il decreto in commento comprende: funzionamento dei sistemi, parametri di programmazione o addestramento, misure di controllo, impatti potenzialmente discriminatori delle metriche utilizzate.

L'obbligo informativo deve essere adempiuto «in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico»[90]. In applicazione del principio di liceità, correttezza e trasparenza del Reg. UE n. 679/2016 l'Autorità Garante per la protezione dei dati personali auspica «che tutte le informazioni siano complessivamente fornite al lavoratore prima dell'inizio del trattamento, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (v. art. 12 del Regolamento)».

2.4. Il principio di trasparenza nei trattamenti effettuati dalla Pubblica Amministrazione

Per concludere l'analisi sulla portata del principio, merita un separato approfondimento l'evoluzione del concetto di trasparenza nelle attività della Pubblica Amministrazione la cui applicazione si confronta – e necessita di essere bilanciata – con il diritto alla protezione dei dati personali, il quale è segnato, a propria volta, sia da logiche di riservatezza, sia da logiche di trasparenza, in un equilibrio talvolta difficile da realizzare.

Nel *considerando* n. 154 il Reg. UE n. 679/2016 «ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali» e prosegue precisando che «i dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali»[91].

---

[89] Cfr. GPDP, *Questioni interpretative e applicative in materia di protezione dei dati connesse all'entrata in vigore del d. lgs. 27 giugno 2022, n. 104 in materia di condizioni di lavoro trasparenti e prevedibili (c.d. "Decreto trasparenza"),* doc. *web* 9844960.

[90] Come previsto dal novellato art. 1-*bis*, co. 6, d.lgs. n. 152/1997.

[91] Corte Cost., sent. n. 20/2019 con la quale è stata definita la questione di legittimità costituzionale sollevata dal TAR Lazio (ord. n. 9828 del 19 settembre 2017) dell'art. 14 commi 1-*bis* e 1-*ter* del d.lgs. 14 marzo 2013 n. 33 sul diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni. Nella pronuncia, la Corte individua nei principi di proporzionalità, pertinenza e non eccedenza, previsti a livello comunitario in materia di protezione dei dati personali, i parametri di riferimento per bilanciare la disciplina nazio-

Nell'ambito delle attività del settore pubblico, la trasparenza è stata, da un lato, identificata con la pubblicità e l'accesso ai dati e alle informazioni, dall'altro con la comprensibilità delle informazioni[92]. Più in particolare, il principio di trasparenza è stato attuato nel settore in commento attraverso la regolamentazione del diritto di accesso, oggetto di molteplici interventi.

Il primo intervento si riferisce al diritto di accesso documentale, previsto dalla l. n. 241 del 1990, motivato dal soggetto istante che vanta un interesse tutelato giuridicamente diretto, concreto, attuale e collegato al documento per cui viene richiesto l'accesso. Il co. 7 dell'art. 24 della legge in commento dispone che «deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici (…)». Si pone tuttavia l'obbligo di attuare un bilanciamento di interessi nel caso di documenti contenenti dati «particolari» (sensibili) o giudiziari, per i quali l'accesso è «consentito nei limiti in cui sia strettamente indispensabile»[93].

Nel diverso caso dei dati c.d. «sensibilissimi» (ossia di dati genetici o dati relativi alla salute, alla vita sessuale o all'orientamento sessuale), il bilanciamento tra il diritto di difesa e l'interesse dei soggetti a mantenere il riserbo su questioni riferibili a tali informazioni deve essere effettuato in ossequio alle prescrizioni stabilite dall'art. 60 del Codice della *privacy*, con ciò significando che non solo l'interesse all'ostensione deve essere indispensabile per tutelare situazioni giuridiche meritevoli di protezione ma anche che tali situazioni siano di «rango»[94] almeno pari a quelle riferibili al contrapposto diritto alla riservatezza, dovendo quindi consistere, a loro volta, in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile[95].

Pertanto, se in alcuni casi l'equilibrio riesce a raggiungersi grazie alle valutazioni compiute *ex ante* dal legislatore e basate sui criteri di proporzionalità rispetto

nale sull'accesso. Come indicato da C. DELLA GIUSTINA, *Alla ricerca di un ragionevole equilibrio tra principio di trasparenza e tutela della riservatezza*, in *Nomos*, 2020, 1, «si nota sin da subito come lo stesso (giudice) ritenga che il diritto alla *riservatezza* e alla *trasparenza* debbano essere considerati diritti aventi entrambi fondamento costituzionale nonché rilevanza uguale. Questi diritti, di conseguenza, devono essere bilanciati secondo il canone di proporzionalità il quale esige che il legislatore scelga all'interno dell'insieme relativo alle misure idonee a perseguire il fine legittimo quella meno restrittiva dei diritti che si contrappongono».

[92] In questo senso F. MANGANARO, *Evoluzione ed involuzione delle discipline normative sull'accesso a dati, informazioni ed atti delle pubbliche amministrazioni*, in *Diritto amministrativo*, 2019, 4, p. 743. In materia di trasparenza nella pubblica amministrazione si rimanda, *amplius*, a A.G. OROFINO, *Profili giuridici della trasparenza amministrativa*, Bari, 2013, nonché ID., *La trasparenza oltre la crisi. Accesso, informatizzazione e controllo civico*, Bari, 2020.

[93] Art. 27, co. 7, l. n. 241/1990.

[94] L'espressione, originariamente formulata da Cons. di Stato. sez. VI, sent. 30 marzo 2001, n. 1882, è stata poi ripresa testualmente dalla lettera dell'articolo 60 del d.lgs. n. 196/2003.

[95] L'art. 60 del Codice in materia di protezione dei dati personali prevede infatti che «Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale».

alla finalità di trasparenza, su altri profili il bilanciamento è maggiormente problematico e sarà necessaria una valutazione caso per caso da parte dell'amministrazione che, nel dubbio, sarà tenuta a privilegiare l'interesse conoscitivo[96].

Un ulteriore sviluppo del diritto in commento si segnala con il d.lgs. n. 33 del 2013[97] che disciplina l'accesso civico quale strumento per «favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche», in un'ottica anti-corruzione[98].

La differenza sostanziale rispetto all'accesso documentale sta proprio nell'assenza di motivazione e nella legittimazione dell'esercizio del diritto in capo a ogni individuo[99]. In tale contesto, il diritto alla riservatezza potrà essere limitato solo a condizione che non vi siano altre soluzioni idonee a proteggere entrambe le situazioni soggettive[100], ad esempio riducendo al minimo l'utilizzo di dati personali nel rispetto del principio di proporzionalità ed attraverso l'istituto dell'accesso parziale, ovvero rendendo i dati personali accessibili solamente nel momento in cui l'amministrazione riterrà che il rischio relativo alla verificazione del pregiudizio possa considerarsi azzerato[101].

---

[96] Cfr. Linee Guida dell'ANAC (delibera n. 1309 del 28/12/16) e Circolare ministeriale n. 2/2017.

[97] Il GPDP ha fornito supporto ai soggetti pubblici con le «Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati» (Pubblicato sulla G.U. n. 134 del 12 giugno 2014 – Registro dei provvedimenti n. 243 del 15 maggio 2014), definendo i contenuti dell'obbligo di trasparenza e tracciandone i limiti rispetto alla protezione dei dati personali. A tal riguardo si veda A. Incerti, *Trasparenza amministrativa e* privacy, in *giustiziacivile.com*, 2021, 9, pp. 73 ss.; Id., *Le linee guida del garante per la protezione dei dati personali e dell'autorità nazionale anticorruzione in tema di bilanciamento fra* privacy *e trasparenza*, in *Diritto di Internet*, 2021, 4, pp. 803 ss.

[98] Sul punto vedi C. Della Giustina, *Alla ricerca di un ragionevole equilibrio tra principio di trasparenza e tutela della riservatezza*, in *Nomos*, 2020, 1: «Posto che il fine principale perseguito dall'istituto della trasparenza amministrativa concerne l'instaurazione di un rapporto comunicativo proficuo con gli amministratati si deve registrate come nella normativa italiana più recente spicchi l'esistenza del rapporto tra trasparenza amministrativa e contrasto della corruzione. Oltre a questo la trasparenza è chiarezza e comprensibilità dell'azione amministrativa idonea a garantire che l'accesso e la pubblicità non risultino essere vani posto che questi non avrebbero alcun significato se le informazioni pubblicate o rese accessibili risultassero essere non comprensibili al destinatario».

[99] Sulla modifica del modello cfr. I.A. Nicotra, *Privacy vs trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, in *Federalismi.it*, 2019, 7, p. 1: «Il modello di pubblicazione obbligatoria delle informazioni introdotto in Italia con il d.lgs. n. 33 del 2013 cambia profondamente la prospettiva nei rapporti tra istituzioni e cittadini, imprimendo immediatezza al diritto di accesso civico. La visibilità diviene la regola e il segreto, l'eccezione. La promozione di maggiori livelli di trasparenza – in linea con i precetti contenuti nell'articolo 97 della Costituzione – costituisce un obiettivo strategico di ogni amministrazione che deve tradursi nel diritto di informare, quale canone fondamentale dei pubblici poteri. All'interno di ogni amministrazione il responsabile per la prevenzione della corruzione, cui di norma, sono attribuite anche le funzioni di responsabile per la trasparenza svolge stabilmente un'attività di controllo sull'adempimento da parte della p.a. degli obblighi di pubblicazione. Egli è tenuto ad assicurare la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate».

[100] G. Scaccia, *Gli "strumenti" della ragionevolezza nel giudizio costituzionale*, Milano, 2000, p. 352

[101] Cfr. art. 5-*bis*, co. 4-5, d.lgs. n. 33/2013.

Lo stesso art. 1, par. 2 del d.lgs. n. 33/2013 dichiara, infatti, che esistono dei limiti alla trasparenza in funzione di altri interessi protetti dall'ordinamento sia di natura pubblica, come quelli che si evincono dalle «disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico»[102], che di natura privata, come quelli in materia di protezione dei dati personali, libertà e segretezza della corrispondenza, interessi economici e commerciali, ivi compresi la proprietà intellettuale e il diritto d'autore[103].

Da ultimo, il d.lgs. n. 97 del 2016 ha introdotto il diritto di accesso civico generalizzato, ampliandone l'oggetto a tutti i documenti e dati[104] che non sono già diffusi *online* in forza dell'obbligo di pubblicazione da parte della Pubblica Amministrazione[105]. Tale forma di *full disclosure*, definita dalla dottrina come «terza generazione della trasparenza amministrativa in Italia»[106], è lo strumento applicativo maggiormente idoneo a produrre effetti immediati nei rapporti tra Istituzioni e amministrati[107].

[102] Cfr. art. 5-*bis*, co. 3, d.lgs. n. 33/2013, introdotto dal d.lgs. n. 97/2016. Tra le eccezioni assolute rientrano anche i casi previsti dall'art. 24, co. 1, della l. n. 241/90 in materia di accesso documentale.

[103] Eccezioni al diritto di accesso civico generalizzato sono previste nelle Linee guida dell'ANAC, di cui alla delibera n. 1309 del 28 dicembre 2016 e nell'art. 24 della l. n. 241/90. art. 5-*bis*, co. 1 e 2, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016. Nel caso di controinteressati, è previsto che l'amministrazione debba attivare uno specifico procedimento di comunicazione, che consenta ai controinteressati di presentare eventuale motivata opposizione (cfr. art. 5, co. 5, d.lgs. 33/2013). Cfr., *amplius*, A. INCERTI, *Le linee guida del garante per la protezione dei dati personali e dell'autorità nazionale anticorruzione in tema di bilanciamento fra* privacy *e trasparenza*, cit., pp. 803 ss.

[104] Secondo C. COLAPIETRO, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *Federalismi.it*, 2020, 14, con il d.lgs. n. 97 del 2016 «la nozione di trasparenza subisce un'ulteriore espansione, in quanto da allora non si fa più riferimento alle «informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni», bensì ai «dati e documenti detenuti dalle pubbliche amministrazioni». La nuova normativa persegue il duplice obiettivo di razionalizzare gli obblighi informativi previsti dal d.lgs. n. 33/2013 e di ampliare lo spettro di conoscibilità dell'azione amministrativa, attraverso il riconoscimento di un diritto di accesso civico generalizzato al patrimonio informativo pubblico, secondo il modello del *Freedom of Information Act* di matrice statunitense».

[105] Sarà onere della singola amministrazione effettuare un bilanciamento delle esigenze contrapposte e valutare se accogliere o meno la richiesta. Sul punto, F. MANGANARO, *op. cit.*, ritiene che «la molteplicità dei tipi di accesso previsti in tempi diversi dal legislatore e la stratificazione/sovrapposizione delle loro differenti regolamentazioni rendono la materia assai complessa , finendo così per attribuire ampia discrezionalità al bilanciamento tra opposti interessi, effettuato caso per caso dalle amministrazioni e dalla giurisprudenza, un'incertezza che non giova alla tutela del diritto di accesso, che meglio andrebbe disciplinato con un'armonizzazione dell'intera materia».

[106] Cfr. C. COLAPIETRO, *La "terza generazione" della trasparenza amministrativa. Dall'accesso documentale all'accesso generalizzato, passando per l'accesso civico*, Napoli, 2016.

[107] V.M. CUCCINIELLO-G.A. PORUMBESCU-S. GRIMMELIKHUIJSEN, *25 Years of Transparency Research: Evidence and Future Directions*, in *Public Amministration Review*, Vol. 77, Issue No. 1, 32-44.

I diversi tipi di accesso brevemente illustrati «rispecchiano l'evoluzione sociale, tradottasi in una crescente richiesta di apertura dell'amministrazione[108] e di ridimensionamento del suo tradizionale carattere autoritativo»[109].

Nel tempo, a seguito degli interventi legislativi e dei regolamenti ad essi applicabili[110], il principio di trasparenza si è orientato ad una finalità anti-corruttiva[111] e di controllo sociale sull'azione amministrativa, mettendo in secondo piano la funzione partecipativa e l'impatto in termini di efficienza della Pubblica Amministrazione[112].

Può pertanto ritenersi che la disciplina in materia di trasparenza nella Pubblica Amministrazione sia da intendersi complementare e non antagonista con la disciplina della protezione dei dati personali[113].

---

[108] Apertura che trova comunque un limite nel diritto individuale alla trasparenza. Sul punto, I.A. Nicotra, *Privacy vs trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, cit., p. 1. Secondo l'Autore, «la pubblicazione di quantità incontrollata di notizie non si traduce automaticamente in un regime di visibilità di maggiore conoscenza. Anzi, proprio un enorme quantità di materiale contenuto in rete può comportare rischi di alterazione, manipolazione e riproduzione, restituendo informazioni non corrispondenti al vero. D'altra parte, una massiccia dose di dati finisce per provocare quella che, con efficace espressione, è stata definita "opacità per confusione". Solo i soggetti "complessi", capaci di elaborare dati sovrabbondanti ed eccessivamente diffusi, sarebbero in grado di decodificare masse di dati presenti in rete, frustrando l'ispirazione ad una reale trasparenza da parte della collettività tutta».

[109] S. Rossa, *Open data e amministrazioni regionali e locali. riflessioni sul processo di digitalizzazione partendo dall'esperienza della Regione Piemonte*, in *Dir. inf.*, 2019, 4, p. 1121.

[110] Quali le «Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016» dell'ANAC.

[111] I.A. Nicotra, *Privacy vs trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, cit., p. 1: «L'edificio ordinamentale si basa sull'assunto che la trasparenza costituisce un deterrente rispetto alla commissione di fatti corruttivi, inducendo l'amministrazione a porre in essere comportamenti legittimi e volti al buon funzionamento e all'imparzialità. Essa, indiscutibilmente, diminuisce le "zone grigie" e rappresenta una risorsa per anticipare i casi di *maladministration*».

[112] F. Manganaro, *Evoluzione ed involuzione delle discipline normative sull'accesso a dati, informazioni ed atti delle pubbliche amministrazioni*, in *Diritto Amministrativo*, 2019, 4. Cfr. anche I. Piazza, *L'organizzazione dell'accesso generalizzato: dal sistema di* governance *all'attuazione amministrativa*, in *Diritto Amministrativo*, 2019, 3, p. 645, secondo cui «La disciplina italiana del diritto d'accesso si caratterizza, quindi, per la coesistenza di diversi tipi di accesso, che rischiano di confondersi o sovrapporsi, muovendo gli interpreti alla ricerca di differenze che, sul piano pratico, non risultano sempre chiare».

[113] Cfr. A. Incerti, *Le linee guida del garante per la protezione dei dati personali e dell'autorità nazionale anticorruzione in tema di bilanciamento fra* privacy *e trasparenza*, cit., p. 804, la quale rimarca altresì che «Le due discipline possono pertanto dirsi complementari: da un lato, la trasparenza amministrativa, individuata quale principio generale dell'attività e dell'organizzazione amministrativa ed intesa quale accessibilità totale a dati e documenti, al fine di garantire forme diffuse di controllo; dall'altro, la *privacy* da intendersi non solo quale riservatezza, ma anche quale diritto all'identità personale, alla corretta rappresentazione della persona e alla protezione dei dati. In linea con tale principio, il Regolamento UE n. 2016/679 disattende pertanto qualunque visione meramente oppositiva o antagonista del diritto alla *privacy* nei confronti della trasparenza amministrativa. Al *Considerando* n. 4 si prevede infatti che "il diritto alla protezione dei dati personali non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va contemperato con gli altri diritti fondamentali in ossequio al principio di proporzionalità" ed al *Considerando* n. 154 si dispone altresì che "l'accesso del pubblico ai documenti ufficiali può essere considerato di

3. APPLICAZIONE DEL PRINCIPIO NELLA CASISTICA

3.1. Il principio di trasparenza nell'adempimento dell'obbligo di informativa

Come abbiamo visto nei precedenti paragrafi di questo contributo, alla luce del forte collegamento con l'identità del singolo e della profonda incidenza sulla persona, la trasparenza si configura come diritto a conoscere e ad essere informati dettagliatamente dell'esistenza e delle caratteristiche di un trattamento dei propri dati personali: «solo rendendo pienamente consapevole l'interessato sul trattamento dei propri dati attraverso un'informativa trasparente, quindi, completa, chiara e facilmente accessibile, infatti, il titolare adempie a quanto prescritto dall'art. 5, par. 1, lett. *a)* in relazione all'art. 13 del Regolamento»[114]. La fattispecie riguardava il trattamento dei dati personali dei c.d. *riders*, effettuato tramite piattaforma informatica con processi decisionali automatizzati, da una nota società di *food delivery*, nei cui confronti il Garante ha contestato, tra le altre cose, che «Il documento informativo (…), esaminato il suo contenuto, risulta essere stato reso in violazione (…) dell'art. 5, par. 1, lett. *a)* del Regolamento in relazione al *principio di trasparenza* con riferimento alla omessa indicazione: 1. delle concrete modalità di trattamento dei dati relativi alla posizione geografica così come emerse in sede di accertamento (visualizzazione su mappa del percorso effettuato e raccolta sistematica del dato ogni 15 secondi) a fronte di un'indicazione del tutto generica sul punto ("il titolare potrà ricevere informazioni riguardo la posizione geografica del dispositivo mobile"), 2. della tipologia dei dati raccolti, in particolare i dati relativi alle comunicazioni intraprese via *chat*, *email* e telefono con il *call center*, le valutazioni espresse sul *rider* da parte degli esercenti e dei clienti (…)»[115].

Sul punto va fatta una doverosa precisazione: come rilevato dall'*European Data Protection Board* (di seguito per brevità «EDPB») nella *Binding decision* 1/2021 resa rispetto alla pronuncia della *Supervisory Autorithy* irlandese rispetto alle informative rilasciate da WhatsApp Ireland Limited e alle relative condivisioni di

interesse pubblico. I dati personali, contenuti in documenti conservati da un'autorità pubblica o da un organismo, dovrebbero poter essere diffusi da detta autorità o da un organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti" il quale deve "conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali". L'art. 6 del Regolamento UE n. 2016/679, ancora, rubricato "liceità del trattamento", dispone che nel caso di pubblicazione di dati per finalità di trasparenza, la base giuridica che legittima il trattamento da parte degli enti pubblici è data dall'art. 6, par. 1, lettera e), dello stesso Regolamento: il trattamento può quindi lecitamente essere svolto quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, in ossequio ad una norma del diritto dell'Unione o del diritto di uno Stato membro cui è soggetto il titolare stesso».

[114] Cfr. GPDP, Provv. del 10 giugno 2021, doc. *web* n. 9675440.

[115] *Ibidem*.

dati con le società del Gruppo Facebook[116], la violazione del *principio di trasparenza* non è circoscritta solamente al mancato rispetto delle prescrizioni di cui agli artt. 12-13-14 del GDPR, che ne costituiscono una concretizzazione. Il *principio di trasparenza* è generale e rinforza tanto gli altri principi declinati dall'art. 5 del GDPR quanto diverse disposizioni del Regolamento stesso, quali i principi di *privacy by design* e *by default*[117].

Nella decisione in commento, l'EDPB rileva che «*the GDPR distinguishes the broader dimension of the principle from the more specific obligations. In other words, the transparency obligations do not define the full scope of the transparency principle. (…) That being said, the EDPB is of the view that an infringement of the transparency obligations under Articles 12-14 GDPR can, depending on the circumstances of the case, amount to an infringement of the transparency principle. (…) In this particular case, the question that the EDPB is confronted with is whether the infringements of specific transparency obligations by WhatsApp IE (WhatsApp Ireland Limited,* ndr*) amount to an infringement of the overarching principle of transparency under Article 5(1)(a) GDPR. (…) Taking all the above into consideration, the EDPB is of the view that, in this particular case, there has been an infringement of the transparency principle under Article 5(1)(a) GDPR, in light of the gravity and the overarching nature and impact of the infringements, which have a significant negative impact on all of the processing carried out by WhatsApp IE*»[118].

Vengono, pertanto, in rilievo due caratteristiche essenziali che l'informativa deve possedere in ossequio al principio di trasparenza: il contenuto, conforme alle disposizioni degli artt. 12-13-14 del GDPR, e la sua accessibilità.

Quanto al contenuto[119], il livello di dettaglio che il titolare deve rispettare si coglie in alcune pronunce dell'Autorità Garante per la protezione dei dati personali.

Rispetto ad attività promozionali tramite operatore telefonico, l'Autorità Garante, sulla base della documentazione acquisita, ha rilevato la carenza dell'informativa rispetto «all'indicazione delle modalità del contatto promozionale, essendo rappresentata soltanto la finalità pubblicitaria perseguita, alla individuazione dei

[116] EDPB, *Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR*, del 28 luglio 2021, disponibile su internet all'indirizzo https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf (consultato da ultimo il 3 aprile 2023).

[117] Tale assunto risulta dalla lettera dell'art. 83, par. 5, del GDPR che disciplina in modo separato la violazione di singoli obblighi di trasparenza (quali quelli prescritti dagli artt. 12-13-14 del GDPR) rispetto alla violazione del principio di trasparenza.

[118] Nella *Binding decision 1/2021* cit., che qui si commenta, l'EDPB stabilisce che la decisione resa dalla *Supervisory Authority* irlandese deve essere modificata, includendo la violazione del principio di trasparenza *ex* art. 5, par. 1, lett. *a)*, del GDPR.

[119] Oltre al contenuto, inteso in senso stretto, deve essere rispettato anche un criterio di "*tempestività*" dell'informativa: come rilevato dal GPDP con Provv. del 29 settembre 2021, doc. *web* n. 9719914 «I trattamenti di dati personali, anche nell'ambito del rapporto di lavoro, devono rispettare, tra gli altri, i principi di trasparenza e correttezza; ciò comporta, in particolare, che le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori prima che il trattamento venga effettuato (v. sul punto art. 5, par. 1, lett. *a)* del Reg. UE 679/2016o nonché, in proposito Provv. 1° marzo 2007, n. 13 "Linee guida per posta elettronica e internet", in G. U. n. 58 del 10.3.2007). Il trattamento dei dati in assenza di informativa ne comporta l'illiceità».

soggetti terzi e/o delle categorie merceologiche delle Società terze cui vengono comunicati i dati per fini promozionali, alla chiara identificazione delle Società terze di rilevazione della qualità dei servizi alle quali (la Società, *n.d.a.*) comunica i dati personali degli utenti; al riferimento al diritto alla limitazione (*ex* art. 18 del Regolamento), nell'ambito dell'elenco dei diritti esercitabili dall'interessato»[120].

Sempre nel medesimo settore economico, ma in altra fattispecie concreta, viene ribadito anche il dovere di identificare chiaramente il titolare del trattamento nel contesto delle informative rese agli interessati, senza richiedere agli stessi di effettuare specifiche ricerche in merito, in particolar modo quando i dati personali sono acquisiti presso terzi nell'ambito di comunicazioni promozionali[121]. Sicché il Garante, nel caso specifico sottoposto al suo vaglio, ha rimarcato che «Sulla base di quanto dichiarato in atti e considerato il contenuto delle e-mail promozionali inviate al reclamante, non risulta che la Società abbia fornito le informazioni previste dall'art. 14 del Regolamento. Le e-mail, difatti, risultavano prive persino dell'identità del mittente, cui il reclamante è pervenuto solo a seguito di una più approfondita ricerca. Nel caso di specie, è indubbia la titolarità del trattamento in capo alla (…) [Società, n.d.a.] che ne ha determinato la finalità (promozionale) ed i mezzi (*e-mail*); spettava pertanto a tale autonomo titolare l'invio di una idonea informativa agli interessati i cui dati erano stati acquisiti da un soggetto terzo. Ciò al fine di renderli edotti del trattamento posto in essere da parte di un titolare che essi, evidentemente, non potevano conoscere. Ciò premesso, si ritiene integrata la violazione dell'art. 14 del Reg. (UE) 2016/679 e si rende necessario ammonire la (…) [Società, n.d.a.] circa l'illiceità dell'invio di comunicazioni promozionali senza fornire agli interessati adeguate informazioni»[122].

Vanno altresì evitate forme tautologiche ed estremamente generiche, spesso utilizzate in relazione alla conservazione dei dati. Sul punto si è pronunciata l'Autorità Garante rispetto al documento «*privacy policy* del *rider* per l'Italia» resa da una società multinazionale attraverso un *link* e disponibile nel proprio sito internet[123]: rispetto ai tempi di conservazione, il documento riporta affermazioni quali «non conserveremo le tue informazioni per un periodo più lungo di quanto pensiamo sia necessario»[124], oppure «(periodo) indefinito per i dati relativi alle fatture»[125]. Sulla base delle indagini svolte dall'Autorità Garante, alla indeterminatezza di tali affermazioni, si aggiunge la contraddittorietà delle indicazioni contenute nel registro delle attività di trattamento, dal quale risultano termini di «6 anni dopo la scadenza del contratto/rescissione per i dati ricollegati al contratto e trattati per attività di supporto *rider*; (…) 6 anni per le rilevate discrepanze in sede di gestione dell'ordine; 1 anno per le conversazioni telefoniche fino alla data di modifica della *policy* in materia di

[120] Cfr. GPDP, Provv. n. 217 del 27 maggio 2021, doc. *web* n. 9689375.
[121] Cfr. GPDP, Provv. n. 267 del 10 dicembre 2020, doc. *web* n. 9557571.
[122] *Ibidem*.
[123] Cfr. GPDP, Provv. del 22 luglio 2021, doc. *web* n. 9685994.
[124] *Ibidem*.
[125] *Ibidem*.

data retention, comunicata il 10.7.2019, che allo stato, secondo quanto dichiarato, prevede la conservazione per 28 giorni solo da parte della capogruppo (…)»[126].

Nel medesimo settore di attività appena esaminato e sempre in relazione al trattamento dei dati dei *riders*[127], in altra fattispecie concreta l'Autorità Garante ha rilevato – ancora una volta – l'indeterminatezza e l'inesattezza dell'informativa rispetto ai termini di conservazione dei dati, osservando che «relativamente ai tempi di conservazione, tale documento si limita a fornire un'indicazione del tutto generica sul punto ("i dati sono trattati per il solo tempo strettamente necessario a conseguire le finalità per cui sono stati raccolti e, in ogni caso, non oltre la cessazione del rapporto di collaborazione"), nonché inesatta considerato che nel corso degli accertamenti la società ha dichiarato di conservare i dati anche oltre la cessazione del rapporto di lavoro. Pertanto (…) [la Società, n.d.a.] omette di fornire i precisi tempi di conservazione di alcune tipologie di dati così come risultanti sia dalle attività di accertamento (…) sia dal registro dei trattamenti»[128]. Nel caso di specie, inoltre, è stato contestato dall'Autorità Garante l'uso del termine «anonimizzati» che risulta «improprio – se non fuorviante – in quanto la società continua a trattare dati relativi alla posizione geografica riferibili ai c.d. "passaggi chiave"»[129], ossia ai dati relativi alle fasi di consegna dei prodotti ai consumatori finali, poi utilizzati per la determinazione del compenso[130].

In relazione alla seconda caratteristica essenziale che l'informativa deve possedere in ossequio al principio di trasparenza, l'Autorità Garante, così come le altre *Supervisory Authorities* e l'EDPB, hanno più volte sottolineato come accessibilità e fruibilità dell'informativa siano requisiti previsti (in particolare) dall'art. 12 del GDPR e da collocare, appunto, nel «più ampio contesto del basilare principio di trasparenza»[131].

A tal riguardo, ad esempio, è stata considerata non conforme alle prescrizioni dell'art. 12 del GDPR l'informativa relativa ai possibili controlli del datore di lavoro, resa disponibile al dipendente in una cartella condivisa del *server* ove non vi sia la prova che la documentazione «sia stata effettivamente e adeguatamente posta a conoscenza di tutti i dipendenti (compresi i reclamanti), ad esempio attraverso notifiche (anche via *email*) contenenti l'invito a prenderne conoscenza, al momento dell'adozione e/o in occasione del loro eventuale aggiornamento. L'adeguata ed effettiva pubblicizzazione di documenti relativi alla possibilità di effettuare tali controlli è tanto più necessaria, in applicazione dei principi di trasparenza e correttezza da parte del datore di lavoro, quanto più il grado di controllo prospettato è profondo ed intrusivo»[132]. Nella medesima fattispecie l'Autorità Garante, prosegue esplicitando i concetti di accessibilità e fruibilità, nell'alveo del principio di trasparenza, in relazione alla lingua dei documenti, nonché al loro coordinamento e contenuto,

[126] Cfr. anche GPDP, Provv. 9 gennaio 2020, doc. *web* n. 9263597.
[127] Cfr. GPDP, Provv. del 10 giugno 2021, doc. *web* n. 9675440.
[128] *Ibidem*.
[129] *Ibidem*.
[130] *Ibidem*.
[131] In questo senso cfr. GPDP, Provv. del 27 maggio 2021, doc. *web* n. 9689375.
[132] Cfr. GPDP, Provv. del 15 aprile 2021, doc. *web* n. 9670738.

ricordando che l'art. 12 del Reg. UE n. 679/2016 impone al titolare del trattamento l'adozione di misure appropriate per fornire all'interessato tutti gli elementi utili a tal proposito[133]. L'Autorità Garante ha poi sottolineato, sul punto, che «la predisposizione di una pluralità di documenti contenenti riferimenti alla medesima attività di controllo della società, l'assenza di coordinamento tra gli stessi sul punto, l'assenza della traduzione in italiano in relazione all'*Investigation Action Protocol e al Protected Disclosure (Whistleblowing) Policy* e alla relativa informativa, il riferimento esclusivo all'ICO come autorità di controllo presso la quale esercitare i diritti degli interessati, la mera messa a disposizione dei documenti all'interno di una cartella condivisa, non siano conformi al contenuto dell'obbligo posto in capo al titolare del trattamento dall'art. 12 – in relazione all'art. 5, par. 1, lett. *a)* – del Regolamento in base al quale devono essere adottate misure appropriate per fornire all'interessato tutti gli elementi anche relativi all'esercizio dei diritti "in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro"»[134].

In altri termini, si tratta del «dovere di *clare loqui*» – già menzionato nel secondo paragrafo di questo elaborato – che si ricollega ai più ampi principi di *privacy by design* e *accountability*, con cui si richiede al titolare di essere adeguatamente organizzato, in rapporto all'ambito del trattamento (mezzi, finalità, tipologia e quantità di dati personali), per garantire, sin dalla fase di progettazione, il rispetto dei principi e della disciplina previsti in materia di protezione dei dati personali, «posto che un'adeguata strutturazione di sistemi, organizzazione e cicli lavorativi, in base a quanto stabilito, in termini generali, dall'art. 25 del Regolamento e, più nello specifico, dall'art. 12, paragrafo 1, in tema di trasparenza, dovrebbe portare a escludere la ricorrenza di siffatta tipologia di errori»[135]. Nella fattispecie si trattava di una fornitura non richiesta attivata da primaria compagnia telefonica per asserito "errore umano" o "non documentato errore di sistema", contestato dall'Autorità Garante nei termini espressi.

Rispetto al rapporto tra principio di trasparenza e principio di *accountability*, l'Autorità Garante precisa che «quella di non procedere all'attivazione di offerte o servizi nel momento in cui non vi sia prova che gli stessi siano stati correttamente proposti all'utente in base alle disposizioni che regolano le modalità di svolgimento dei contatti promozionali, non costituisce una mera facoltà del titolare del trattamento ma un preciso obbligo dettato dal combinato disposto degli artt. 5, comma 2, 6 e 7 del GDPR e degli artt. 2-*decies* e 130 del Codice. In base alle norme del GDPR, infatti, il titolare è tenuto a comprovare che i trattamenti dallo stesso svolti, anche

[133] *Ibidem*.

[134] *Ibidem*.

[135] Cfr. GPDP, Provv. del 12 novembre 2020, doc. *web* n. 9485681. Vedi anche Provv. n. 143 del 9 luglio 2020, doc. *web* n. 9435753 citato nel provvedimento in commento, laddove si evidenzia che «l'intero impianto del Regolamento si sostiene sulla *accountability* del titolare del trattamento. Questi, in ragione della circostanza che i dati personali dei soggetti contattati che abbiano aderito alle offerte promozionali sono destinati a confluire nei database societari, dovrebbe adottare misure di particolare garanzia al fine di comprovare che i contratti e le attivazioni registrati nei propri sistemi siano originati da contatti effettuati nel pieno rispetto delle disposizioni in materia di protezione dei dati personali, in particolare quelle di cui agli artt. 5, 6 e 7 del Regolamento relative al consenso».

tramite responsabili, siano conformi ai principi di liceità, trasparenza e correttezza (in particolare con riferimento al consenso), principi che, nell'ambito dei contatti promozionali sono declinati dall'art. 130 del Codice, e qualora ciò non sia possibile, il primo effetto che ne deriva è costituito dall'inutilizzabilità dei dati trattati (art. 2-*decies*, del Codice) e quindi dalla loro estromissione dal patrimonio informativo e operativo della Società».

Seppure permanga in capo al titolare una certa libertà di forma rispetto alle concrete modalità con cui rendere l'informativa, così come alla tipologia di informazioni integrative (rispetto al mero dettato normativo) che intende fornire all'interessato, tale libertà non può in ogni caso prescindere dalla *completezza* delle informazioni «favorendo un livello di intellegibilità e di trasparenza sotteso al fondamentale principio di autodeterminazione dell'interessato in ordine al trattamento dei suoi dati personali»[136].

È il caso delle informative «multistrato» utilizzate in particolare dalle piattaforme *social network* e dai fornitori di servizi *web*. A parere di alcune *Supervisory Autorities* tale modalità crea una «*information fatigue*» e diluisce l'effettiva portata delle informazioni prescritte dal GDPR. In questo senso si è espressa la *Data Protection Commission* irlandese nella decisione del 20 agosto 2021 sulle informative rese da WhatsApp Ireland Limited[137], con cui, in particolare, è stata contestata una massiva fornitura di informazioni, avente struttura "multistrato" di livello molto elevato e di carattere generale, a discapito di una maggiore sintesi e di una migliore selezione dei contenuti che consentirebbero all'interessato, sotto il profilo sia formale che sostanziale, di meglio comprendere finalità e modalità del trattamento richiesto[138].

---

[136] Cfr. GPDP, Provv. del 27 maggio 2021, doc. *web* n. 9689375, relativa ad attività di *telemarketing* e *newsletter* per le quali le informative sono messe a disposizione nel sito internet del titolare in modo stratificato, costringendo così l'interessato ad effettuare ricerche all'interno del sito per ricevere tutte le necessarie informazioni.

[137] *Data Protection Commission* irlandese, decisione del 20 agosto 2021 resa in tema di informative fornite da WhatsApp Ireland Limited, documento disponibile su Internet all'indirizzo https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf- (consultato da ultimo il 3 aprile 2023).

[138] Cfr. *Data Protection Commission* irlandese nella decisione del 20 agosto 2021 cit.: «*As is evident from the assessments that follow, my view is that the Privacy Policy and related material frequently demonstrate an over-supply of very high level, generalised information at the expense of a more concise and meaningful delivery of the essential information. Further, while WhatsApp has chosen to provide its transparency information by way of pieces of text, there are other options available, such as the possible incorporation of tables, which might enable WhatsApp to provide the information required in a clear and concise manner, particularly in the case of an information requirement comprising a number of linked elements. The importance of concision cannot be overstated, in this regard. For the avoidance of doubt, however, I am not saying that WhatsApp is not entitled to provide additional information to its users, above and beyond that required by Articles 13 and 14. WhatsApp is free to provide whatever additional information it wishes, providing that it has firstly complied with its statutory obligations and, secondly, that the additional information does not have the effect of creating information fatigue or otherwise diluting the effective delivery of the statutorily required information*».

Alla generalità delle informazioni sulla tipologia di dati e sulle finalità del trattamento, si accompagna spesso una eccessiva frammentazione dei contenuti tale da rendere l'informativa non conforme alle prescrizioni degli artt. 12-13-14 del GDPR.

La *Commission Nationale de l'Informatique et des Libertés* (*Supervisory Authority* francese) è intervenuta nei confronti di un noto motore di ricerca per la violazione del principio di trasparenza di cui all'art. 12 del GDPR, evidenziando come le informazioni essenziali siano disseminate in modo eccessivo in diversi documenti, con utilizzo di *link* da selezionare per accedere a contenuti aggiuntivi. L'utilizzatore, a parere dell'Autorità francese, non è in grado di comprendere appieno l'ambito del trattamento a causa dell'utilizzo di un linguaggio vago e generico, della scarsa chiarezza dei contenuti, in particolare rispetto alle basi giuridiche del trattamento, e tenuto conto della invasività dei trattamenti oggetto di analisi[139].

Quanto più è complesso ed invasivo l'ambito del trattamento, tanto più chiara e accessibile deve essere l'informativa rispetto a ciascuno degli elementi essenziali richiesti dagli artt. 13 e 14 del GDPR. Ciò vale anche rispetto all'esenzione di cui all'art. 14, par. 5, lett. *b)*, che impone al titolare di adottare misure appropriate per «tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni». Nella citata decisione del 20 agosto 2021, la *Supervisory Authority* irlandese ha ben chiarito la portata di tale esenzione: «*to be absolutely clear about the position, the alternative condition, set out in Article 14(5)(b), requiring the controller to make the prescribed information publicly available is not optional or something to be assessed on a case by case basis; if a data controller is entitled to avail of the Article 14(5)(b) exemption, then it must make the prescribed information publicly available so that the data subjects concerned are nonetheless enabled to receive the Article 14 transparency information. This is clear not only from the text of Article 14(5)(b) but also from the limited nature of the exemptions provided by Article 14, which support the default position that the data subject must be provided*

[139] Cfr. Commission Nationale de l'Informatique et des Libertés (CNIL), *Deliberation of the Restricted Committee* SAN-2019-001, of 21 January 2019, *pronouncing a financial sanction against* Google LLC: «*(…) the general* structure *of the information chosen by the company does not enable to comply with the Regulation. Essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for the ads personalization, are excessively disseminated across several documents, with buttons and links on which it is required to click to access complementary information. The relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions. For instance, this is the case when a user wants to have a complete information on his or her data collected for the personalization purposes or for the geotracking service. Moreover, the restricted committee observes that some information is not always clear nor comprehensive. Users are not able to fully understand the extent of the processing operations carried out by Google. But the processing operations are particularly massive and intrusive because of the number of services offered (about twenty), the amount and the nature of the data processed and combined. The restricted committee observes in particular that the purposes of processing are described in a too generic and vague manner, and so are the categories of data processed for these various purposes. Similarly, the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company. Finally, the restricted committee notices that the information about the retention period is not provided for some data*».

with the prescribed information, save in very limited circumstances (which do not include those described by Article 14(5)(b)».

Aggiunge, infine, l'Autorità irlandese che l'obbligo di trasparenza nelle informazioni è «*ongoing*», in modo analogo agli altri adempimenti prescritti dal GDPR, tale da imporre al titolare un monitoraggio continuo dei contenuti.

In relazione alle connessioni tra informativa e base giuridica del trattamento, L'Autorità Garante ha precisato che quest'ultima deve essere univoca per ogni trattamento e chiaramente identificata, soprattutto nei casi in cui viene richiesto il consenso dell'interessato, chiarendo – con riguardo ad una fattispecie relativa a trattamenti di dati per finalità promozionali, tramite consenso acquisito per mezzo di un sito *web* finalizzato alla vendita di prodotti odontoiatrici direttamente ai professionisti – che «La formulazione utilizzata nella precedente versione dell'informativa resa agli interessati non è risultata idonea a rappresentare con chiarezza la base giuridica adottata, che deve essere univoca per ogni finalità del trattamento. Questo, pertanto, non risulta essere stato effettuato in modo lecito, corretto e trasparente dal momento che agli interessati non sono state rese informazioni chiare in merito alle basi giuridiche relative alle diverse finalità del trattamento: l'informativa *privacy*, infatti, faceva riferimento sia al consenso che al legittimo interesse anche se, di fatto, veniva richiesto di esprimere un consenso; inoltre, si domandava il consenso anche per le finalità connesse all'esecuzione del contratto (la cui base giuridica è invece quella indicata dall'art. 6, par.1, lett. b) del Regolamento)»[140].

3.2. Il principio di trasparenza rispetto all'uso di nuove tecnologie e ai diritti dell'interessato

L'uso di tecnologie sempre più sofisticate ed innovative e le attività di profilazione richiedono una informativa «rafforzata». L'Autorità Garante si è pronunciata in questo ambito con particolare riferimento all'utilizzo di sistemi di geolocalizzazione in una fattispecie relativa all'uso delle piattaforme per la gestione dell'attività di *food delivery* tramite i c.d. *riders*, sottolineando come «la particolare invasività del trattamento in esame impone la necessità di fornire indicazioni circa le specifiche modalità del trattamento e sulla cadenza temporale della rilevazione della posizione geografica: in assenza di tali informazioni, l'interessato non può avere adeguata consapevolezza del trattamento dei propri dati. Ciò comporta quindi la violazione dell'art. 5, par. 1, lett. *a)* del Regolamento in relazione al principio di trasparenza»[141].

In modo analogo, ma con maggior enfasi rispetto alla effettiva comprensione delle attività di trattamento da parte dell'interessato, con ordinanza del 10 giugno 2021 l'Autorità Garante ha avuto modo di precisare, in altra fattispecie di geolocalizzazione dei *riders* nel settore delle consegne a domicilio, che «in ottemperanza, quindi, ai principi di trasparenza e correttezza, la società avrebbe dovuto fornire, per iscritto o con altri strumenti idonei comunque documentabili, agli interessati, seppur con un linguaggio facilmente comprensibile, tutte le informazioni previste dall'art.

[140] Cfr. GPDP, Provv. del 27 gennaio 2021, doc. *web* n. 9711630.
[141] Cfr. GPDP, Provv. del 22 luglio 2021, doc. *web* n. 9685994, cit.

13 del Regolamento in merito anche al trattamento dei dati relativi alla posizione geografica; non rileva, in proposito, che i *rider* fossero semplicemente consapevoli dell'attività di geolocalizzazione in quanto "vedono loro stessi il percorso suggerito sulla mappa dell'Applicazione" né che la geolocalizzazione sia ritenuta dalla società "essenziale per la fornitura del servizio" nonché una "prassi comune e consolidata nel settore dei trasporti e della *delivery*". Evidente, in proposito, è la differenza intercorrente tra l'eventuale mera conoscenza della possibilità di essere geolocalizzati e la piena consapevolezza in merito allo specifico trattamento effettuato in relazione ai dati derivanti dalla geolocalizzazione. Solo rendendo pienamente consapevole l'interessato sul trattamento dei propri dati attraverso un'informativa trasparente, quindi, completa, chiara e facilmente accessibile, infatti, il titolare adempie a quanto prescritto dall'art. 5, par. 1, lett. *a)*, in relazione all'art. 13 del Regolamento»[142]. Nella medesima ordinanza, il Garante ha significativamente aggiunto che «Con riferimento, poi, all'omessa indicazione della tipologia dei dati raccolti, in particolare i dati relativi alle comunicazioni intraprese via *chat*, *email* e telefono con il *call center* nonché alle valutazioni espresse sul *rider* da parte degli esercenti e dei clienti, in base a quanto dichiarato nelle memorie difensive tali informazioni sarebbero state fornite durante "il colloquio che precede l'iscrizione all'Applicazione e in sede di *onboarding*, nonché nell'applicazione stessa". In relazione a quanto sarebbe stato comunicato a tutti i *rider* durante il predetto colloquio e in sede di "*onboarding*", però, non emergono evidenze né può ritenersi adeguato a provare ciò il documento denominato "*Training Calendars Customer & Courier Onboarding*" in quanto privo di qualsiasi riferimento sul punto; per quanto riguarda, invece, le informazioni che sarebbero state fornite attraverso l'applicazione, delle quali sono stati allegati alcuni *screenshot* (v. all. 4 alle memorie difensive), non emerge la presenza di tali specifiche informazioni – e quindi la loro conoscibilità nell'applicazione – anche al momento dell'ispezione. Ad ogni buon conto, tali informazioni risultano generiche e non sufficientemente chiare per rendere consapevoli i *rider* del trattamento di tali dati»[143].

Ove vi sia anche un'attività di profilazione dell'interessato, il Garante ha chiarito, nella casistica affrontata, che ai fini del rispetto del principio di *trasparenza*, devono essere fornite specifiche informazioni rispetto alla *logica* utilizzata, all'importanza e alle conseguenze previste per l'interessato e che il titolare deve, inoltre, adottare misure tecniche ed organizzative adeguate volte alla verifica periodica dell'accuratezza e della correttezza dei risultati dei sistemi algoritmici e del relativo trattamento di dati personali, in modo da ridurre al massimo il rischio di effetti distorsivi o discriminatori[144].

Il rispetto del principio di trasparenza nelle informative che il titolare deve rendere per la messa a disposizione di servizi ICT e correlate tecnologie va parametrato non solo rispetto alla invasività delle stesse (come analizzato nei paragrafi precedenti) ma anche – e, in modo non secondario – in relazione alla tipologia di utente.

[142] Cfr. GPDP, Provv. del 10 giugno 2021, doc. *web* n. 9675440, cit.
[143] *Ibidem*.
[144] Cfr. GPDP, Provv. del 10 giugno 2021, doc. *web* n. 9675440, cit.

A riguardo, in relazione alle applicazioni per dispositivi mobili messe a disposizione da una compagnia telefonica[145], l'Autorità Garante ha rilevato un trattamento non conforme al principio di trasparenza, oltre che a quello di correttezza, in ordine alle modalità di acquisizione del consenso a fronte:

– dell'impostazione di una procedura congiunta di accettazione dei termini di servizio e dell'informativa sul trattamento dei dati personali;
– della dichiarazione di più finalità diverse fra loro e di diverse operazioni di trattamento (nel caso di specie l'informativa faceva riferimento a finalità promozionali, di geolocalizzazione e di comunicazione a terzi per finalità promozionali), a fronte di un unico consenso[146].

Nell'ambito di una fattispecie relativa all'uso di *App* dedicate anche ai minori, l'Autorità Garante rilvevava come, all'esito delle indagini svolte concernenti anche le informative in materia di protezione dei dati personali, non fosse «risultato che tali informative contenessero elementi adeguati, in termini di contenuto e di chiarezza della formulazione, riguardo agli effettivi trattamenti di dati effettuati dalla Società mediante tali *App*»[147]. Nella casistica richiamata, la trasparenza e la correttezza sono intese dal Garante, innanzitutto come esigenze di effettiva e agevole comprensibilità, tanto più se si tratta di *App* (quale la "*TIM Smart Kid*") rivolte (anche) a minori e altri soggetti vulnerabili, ai quali la trasparenza andrebbe assicurata in concreto anche con idonei mezzi grafici, come, ad esempio, icone "standardizzate"[148].

La maggiore complessità degli strumenti utilizzati per il trattamento, unita alla elevata quantità di dati (che in alcuni casi rivela informazioni significative sulla sfera privata dell'interessato) e alla quasi illimitata possibilità di combinazione degli

[145] Cfr. GPDP, Provv. n. 7 del 15 gennaio 2020, doc. *web* n. 9256486, cit.

[146] Nel caso in cui il titolare intenda utilizzare il legittimo interesse quale base giuridica del trattamento (che richiede un bilanciamento di interessi e la concreta attuazione di misure adeguate per garantire i diritti degli interessati), il GPDP, nel Provv. del 22 febbraio 2018 contenente indicazioni volte a favorire la corretta applicazione delle disposizioni del Reg. UE 679/2016, ha chiarito che il titolare del trattamento «dovrà fornire un'informativa che evidenzi opportunamente – specie qualora il trattamento preveda l'uso di nuove tecnologie o strumenti automatizzati – agli interessati la circostanza che sta trattando i dati che li riguardano sulla base di tale presupposto, nonché esplicitare quale sia il legittimo interesse in concreto perseguito, che andrà quindi opportunamente evidenziato come tale, a beneficio dell'interessato (artt. 13, par. 1, lett. *d*, e 14, par. 2, lett. *b*, del Reg. UE 679/2016). In particolare, può essere una buona prassi, quella di fornire all'interessato le indicazioni essenziali risultanti dal bilanciamento effettuato in relazione al caso concreto, che ha portato il titolare a scegliere di far affidamento sull'interesse proprio o di terzi quale presupposto di liceità del trattamento ai sensi dell'art. 6, par. 1, lett. *f)*, del Reg. UE 679/2016 (v. *Guidelines on transparency under Regulation 2016/679*, WP 260, in fase di definizione). Considerata la peculiare fonte di legittimazione del trattamento, il titolare dovrà sottolineare in special modo, il diritto di opposizione attribuito agli interessati [v. artt. 13, par. 2, lett. *d)*, 14, par. 2, lett. *c)*, e 21, par. 4, del Reg. UE 679/2016]. In questo quadro, potrà anche essere presa in considerazione la possibilità di rendere pubblica la valutazione d'impatto effettuata dal titolare (o parte di essa). Sebbene una tale pubblicazione non sia richiesta dal Regolamento, in alcune circostanze, potrebbe rappresentare uno strumento utile per dimostrare *trasparenza* e responsabilizzazione da parte del titolare e per rafforzare la fiducia degli interessati riguardo al trattamento dei loro dati». Cfr. GPDP, Provv. del 22 febbraio 2018, doc. *web* n. 8080493.

[147] GPDP, Provv. n. 7 del 15 gennaio 2020, doc. web n. 9256486.

[148] GPDP, Provv. n. 7 del 15 gennaio 2020, doc. *web* n. 9256486.

stessi, richiede che l'interessato sia messo nelle concrete condizioni di controllare i propri dati e di rilasciare un valido (ed informato) consenso[149].

In tale direzione si veda il caso Mevaluate, deciso dal Garante con Provv. n. 488 del 24 novembre 2016, doc. *web* n. 5796783, e successivamente da Cass., del 24 maggio 2021 n. 14381, ove è stata affermata l'invalidità del consenso al trattamento dei dati personali effettuato tramite una piattaforma *web* di *rating* reputazionale, per difetto di trasparenza in ordine al funzionamento dell'algoritmo utilizzato dal sistema[150].

3.3. Pubblica Amministrazione e trattamenti dei dati personali tramite processi decisionali automatizzati. Bilanciamento tra principio di trasparenza e diritto d'autore

Altre specifiche questioni relative ai trattamenti algoritmici sono state affrontate con riguardo ai procedimenti posti in essere dalla p.a.

Con le sentenze del TAR, Lazio-Roma, sez. III-*bis*, del 21 marzo 2017 n. 3742 e del 22 marzo 2017, n. 3769, per la prima volta in Italia viene aperta la c.d. *black box:* meccanismo matematico che governa ormai gran parte dei nostri comportamenti mediante automatismi guidati da un algoritmo[151].

L'uso degli algoritmi nei procedimenti decisionali della p.a. assume rilevanza sia in materia di protezione dei dati personali, con riguardo ai processi decisionali automatizzati di cui all'art. 22 GDPR, sia in tema di procedimenti amministrativi digitalizzati.

Nelle sentenze in parola, il TAR ha reinterpretato il concetto di documento amministrativo accessibile ai sensi dell'art. 22 della l. n. 241/90, come riformata dalla l. n. 15/2005[152] e ha ritenuto che il programma per elaboratore e l'algoritmo in esso contenuto costituiscono "rappresentazione" di attività di pubblico interesse, laddove la sua elaborazione venga a costituire l'atto finale dell'azione amministrativa[153].

---

[149] Cfr. Commission Nationale de l'Informatique et des Libertés, *Deliberation of the Restricted Committee* SAN-2019-001 du 21 janvier 2019, documento disponibile su Internet all'indirizzo https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/ (consultato da ultimo in data 3 aprile 2023).

[150] Cass., ord. 24 maggio 2021, n. 14381, ha precisato che il corretto assolvimento dell'informativa, ai fini della corretta acquisizione del consenso al trattamento automatizzato per il calcolo del rating reputazionale, basato sull'uso di algoritmi, deve riguardare anche lo «schema esecutivo» dell'algoritmo e gli «elementi» di cui esso si compone. In materia di veda, *amplius*, F. Bravo, *Rating reputazionale e trasparenza dell'algoritmo. Il caso* «*Mevaluate*», in *Dir. inf.*, 2021, 6, pp. 1001-1029.

[151] M. Mezza, *Algoritmi di libertà. La potenza del calcolo tra dominio e conflitto*, Roma, 2018. Per la ricostruzione degli indirizzi giurisprudenziali del TAR e del Consiglio di Stato si veda anche F. Bravo, *Trasparenza del codice sorgenze e decisioni automatizzate*, cit., p. 693.

[152] Nella fattispecie, un gruppo di insegnanti si rivolge al TAR perché venga espressamente ordinato al MIUR di esibire il codice sorgente del programma che aveva elaborato le assegnazioni relativi ai trasferimenti interprovinciali, reputando di esser stati destinatari di illegittimi provvedimenti relativi alla propria destinazione territoriale a causa del malfunzionamento dell'algoritmo utilizzato per la gestione della procedura di mobilità.

[153] Nozione di documento amministrativo è rinvenibile dalla lettura dell'art. 22, lett. *d)*, l. n. 241/90 («ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie

Nell'orientamento giurisprudenziale poc'anzi richiamato si evince che l'accesso viene richiesto in quanto "funzionale alla tutela giurisdizionale", ed accordato nonostante mancasse, nel giudizio, la prova di un danno subito dai ricorrenti, del nesso di causalità tra malfunzionamento dell'algoritmo e danno subito, e nonostante fosse stata fornita in atti una spiegazione circa le condizioni di utilizzo della copia del sorgente rilasciata e il regime di diritto d'autore, relativa a quest'ultima, facesse propendere per una diversa soluzione[154].

Non è noto, infatti, se esso sia mai stato nella effettiva disponibilità dell'Amministrazione o se questa lo abbia avuto solo in uso. In quest'ultimo caso il diritto di accesso ai codici sorgenti doveva essere negato a favore della tutela della proprietà intellettuale del *software*, attuando il principio di trasparenza con modalità diverse, maggiormente aderenti al principio di proporzionalità tra i diversi diritti fondamentali rilevanti in fattispecie di siffatto tenore[155].

In modo conforme sul piano dell'apertura si pone anche la sentenza del TAR Lazio, Roma, sez. III-*bis*, del 1°luglio 2020 n. 7526, che, richiamando precedenti pronunce giurisprudenziali emanate nello stesso senso[156], ha riconosciuto ai ricor-

---

del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale») e dell'art. 1, co. 1, lett. *a)*, del D.P.R. n. 445/2000 («ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa»).

[154] Così E. Prosperetti, *Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del TAR Lazio*, in *Dir. inf.*, 2019, 4-5, p. 979 ss.; F. Bravo, *Trasparenza del codice sorgenze e decisioni automatizzate*, cit., p. 693; F. Bravo, *Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional Balancing of Interests?*, in *European Review of Digital Administration & Law (ERDAL),* 2020, vol. 1, Issue 1-2, June-December, pp. 157-165.

[155] Con riferimento alla disciplina sul diritto d'autore relativa alla riproduzione e alla copia dei codici sorgenti del *software* il TAR così argomenta: «in materia di accesso agli atti della p.a., a norma dell'art. 24 della legge n. 241/1990, la natura di opera dell'ingegno dei documenti di cui si chiede l'ostensione non rappresenta una causa di esclusione dall'accesso; in particolare, la disciplina dettata a tutela del diritto di autore e della proprietà intellettuale è, come in precedenza brevemente rappresentato, funzionale a garantire gli interessi economici dell'autore ovvero del titolare dell'opera intellettuale, mentre la normativa sull'accesso agli atti è funzionale a garantire altri interessi e, in questi limiti, deve essere consentita la visione e anche l'estrazione di copia; (…) né il diritto di autore né la proprietà intellettuale precludono la semplice riproduzione, ma precludono, invece, al massimo, soltanto la riproduzione che consenta uno sfruttamento economico e, non essendo l'accesso lesivo di tale diritto all'uso economico esclusivo dell'opera, l'ostensione deve essere consentita nelle forme richieste da parte dell'interessato, ossia della visione e dell'estrazione di copia, fermo restando che delle informazioni ottenute dovrà essere fatto un uso appropriato, ossia esclusivamente un uso funzionale all'interesse fatto valere con l'istanza di accesso; la descrizione della modalità di funzionamento dell'algoritmo assicura una conoscenza assolutamente non paragonabile a quella che deriverebbe dall'acquisizione del richiesto linguaggio sorgente, atteso che, se non altro, la predetta descrizione è, comunque, atto di parte; le valutazioni in ordine alla funzionalità concreta del predetto algoritmo o anche a monte all'esistenza di eventuali errori nella programmazione possono, pertanto, essere effettuate esclusivamente alla luce della piena conoscenza del medesimo che può essere assicurata in modo completo soltanto con il richiesto penetrante accesso ai relativi codici sorgenti».

[156] Cfr. le seguenti sentenze: TAR Lazio, Roma, sez. III-*bis*, n. 733 del 6 giugno 2019, TAR Lazio, Roma, sez. III-*bis*, sent. n. 3769 del 22 marzo 2017 e TAR Lazio, Roma sez.-III *bis*, n. 3742 del 21

renti il diritto di accesso al codice sorgente del *software* utilizzato dalla pubblica amministrazione per la gestione della prova concorsuale informatizzata per il reclutamento dei dirigenti scolastici, evidenziando che l'algoritmo di un software può configurarsi come atto amministrativo cd. informatico ogni qualvolta il ruolo ricoperto dal programma informatico si inquadri in un contesto di indubbia rilevanza pubblicistica, senza che sia di ostacolo il diritto di proprietà intellettuale del *software* in capo al privato appaltatore del programma utilizzato, la regolarità del concorso e di quelli futuri ovvero la riservatezza degli altri candidati[157].

Nella sentenza in commento il Tribunale amministrativo mostra, nuovamente, un chiaro *favor* verso la trasparenza, intesa come accessibilità e piena conoscibilità dei sorgenti a discapito del diritto di proprietà intellettuale, annoverato all'art. 17, par. 2, della Carta dei diritti fondamentali dell'UE.

Secondo il TAR Lazio, con riferimento all'algoritmo, deve tenersi conto della "sostanziale valenza amministrativa del documento, piuttosto che della sua provenienza"[158].

Lo "scontro" tra il diritto d'autore del titolare del *software* fornito e il c.d. *right to know* è risolto dalla giurisprudenza, nel caso di specie, in favore del secondo e ciò crea non pochi dubbi sull'operazione ermeneutica di bilanciamento effettuata dal TAR tra gli interessi in gioco[159]. I richiamati indirizzi giurisprudenziali hanno trovato conferma anche innanzi al Consiglio di Stato, ove il principio di trasparenza, che governa i rapporti con la p.a., viene ancorato anche al principio di trasparenza previsto dalla disciplina in materia di protezione dei dati personali trattati dalla p.a. nell'ambito di procedimenti amministrativi facenti uso di strumenti decisionali automatizzati basati su algoritmi.

---

marzo 2017, Cons. di Stato, sent. n. 881 del 4 febbraio 2020, TAR Sicilia, Catania, sez. IV, sent. n. 22 del 10 gennaio 2019.

[157] Cfr. F. BRAVO, *Trasparenza del codice sorgente e decisioni automatizzate*, cit, pp. 979 ss. Si veda anche F. BRAVO, *Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional Balancing of Interests?*, cit., pp. 157-165.

[158] Secondo E. PROSPERETTI, *Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del TAR Lazio*, cit., p. 979 ss.: «Il Tribunale si pone il problema che l'oggetto a cui viene richiesto accesso è protetto dal diritto d'autore ma non verificherebbe se l'amministrazione abbia o meno i diritti per concederlo a terzi. In mancanza di diritti, suggerisce l'autore, dovrebbe la p.a., limitare l'utilizzo del codice sorgente coperto dal diritto di proprietà intellettuale in virtù di un'eccezione prevista dalla Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione». Sul tema di veda anche F. BRAVO, *Trasparenza del codice sorgente e decisioni automatizzate*, cit., pp. 979 ss. e F. BRAVO, *Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional Balancing of Interests?*, cit., pp. 157 ss.

[159] A tale proposito, preme ricordare, come nei casi di c.d. *proactive disclosure* (pubblicazione obbligatoria e accesso civico semplice) il legislatore risolve in via preliminare e in modo definitivo il problema dell'emersione di eventuali contro-interessi. In questi casi la valutazione dell'amministrazione, relativamente alla proprietà intellettuale, al diritto d'autore e al segreto industriale, avviene *ex ante* e la p.a. dovrà attenersi alla licenza prevista nel contratto o domandarne l'autorizzazione al titolare. Diversamente, nei casi di *reactive disclosure* (istanze di accesso civico generalizzato), come quella nel caso in commento, ai fini della decisione sull'istanza la p.a. dovrà tenere in considerazione i limiti alla conoscenza previsti agli artt. 24 della l. n. 241/90 e 5-*bis*, co. 2, lett. *c)*, del d.lgs. 33/2013.

Come rilevato dal Consiglio di Stato, Sez. VI, con sentenza del 13 dicembre 2019 n. 8473, relativa all'applicazione di algoritmi per procedure di mobilità nazionale straordinaria del personale docente, «tali strumenti sono chiamati ad opera[re] una serie di scelte, le quali dipendono in gran parte dai criteri utilizzati e dai dati di riferimento utilizzati, in merito ai quali è apparso spesso difficile ottenere la necessaria trasparenza. (…) Sul versante della piena conoscibilità, rilievo preminente ha il principio della trasparenza, da intendersi sia per la stessa p.a. titolare del potere per il cui esercizio viene previsto il ricorso allo strumento dell'algoritmo, sia per i soggetti incisi e coinvolti dal potere stesso. (…) Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che i criteri, i presupposti e gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato»[160].

Nella fattispecie esaminata dalla pronuncia in commento, il diritto di accesso regolato dall'art. 15 del GDPR si rivela quale ulteriore tutela ed espressione del principio di trasparenza, in quanto ha «il pregio di prevedere un diritto azionabile dall'interessato e non [solamente, n.d.a.] un obbligo rivolto al titolare del trattamento, e permette inoltre di superare i limiti temporali posti dagli artt. 13 e 14, consentendo al soggetto di acquisire informazioni anche qualora il trattamento abbia avuto inizio, stia trovando esecuzione o abbia addirittura già prodotto una decisione. Ciò, ai fini in esame, conferma ulteriormente la rilevanza della trasparenza per i soggetti coinvolti dall'attività amministrativa informatizzata in termini istruttori e decisori»[161].

[160] Cons. di Stato, sent. 8473/2019, cit.
[161] Cons. di Stato, sent. 8473/2019, cit.

Capitolo V
Il principio di limitazione della finalità

Alice Incerti

SOMMARIO: 1. Inquadramento normativo. – 1.1. L'enunciazione del principio di limitazione delle finalità nell'art. 5 del GDPR. – 1.2. L'embrionale formulazione del principio di limitazione delle finalità nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. – 1.3. Il principio di limitazione della finalità nel Patto internazionale sui diritti civili e politici. – 1.4. Il principio di limitazione della finalità nella Convenzione 108 e nella Convenzione 108+. – 1.5. Il principio di limitazione della finalità nella Direttiva 95/46/CE. – 1.6. Il principio di limitazione delle finalità nella Carta dei diritti fondamentali dell'Unione europea. – 1.7. Il principio di limitazione delle finalità nella l. 31 dicembre 1996, n. 675. – 1.8. Il principio di limitazione delle finalità nel Codice della *privacy* e nel GDPR. – 2. Portata del principio. – 2.1. La *ratio* del principio di limitazione della finalità nel GDPR. – 2.2. Il principio di limitazione della finalità quale fondamento di ulteriori principi in materia di *data protection.* – 2.3. Il ruolo del titolare ed il trattamento dei dati nel rispetto del principio di limitazione della finalità. – 2.4. Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi. – 2.5. Il principio di limitazione della finalità quale presupposto per il rilascio del consenso al trattamento. – 2.6. Le cc.dd. finalità incompatibili e il *compatibility test.* – 3. Applicazione del principio nella casistica. – 3.1. Granularità del consenso, *marketing* diretto, *social spam* e *marketing* virale. – 3.2. Il principio di limitazione della finalità nella giurisprudenza della Corte europea dei diritti dell'uomo. – 3.3. Principio di limitazione della finalità e *big data.* – 3.4. Covid-19 *pandemic*. Limitazione della finalità ed *app* per il tracciamento dei contatti.

1. Inquadramento normativo

1.1. L'enunciazione del principio di limitazione delle finalità nell'art. 5 del GDPR

Il Reg. UE n. 2016/679 (GDPR)[1] prescrive che le attività di trattamento[2] di dati personali[3] siano rispettose di numerosi, importantissimi principi[4]: a stabilirlo è l'art. 5 del summenzionato Regolamento. Fra questi principi, al par. 1, lett. *b)*, del cit. art. 5, di peculiare rilievo è il principio di limitazione della finalità di trattamento, in ragione del quale i dati personali sono «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità». La stessa norma dispone poi che «un ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1, considerato incompatibile con le finalità iniziali»[5].

Tale principio, oggetto d'esame del presente contributo, si configura quale uno fra i più importanti dell'intero Reg. UE n. 2016/679, posto a sua volta a fondamento di altri principi individuati dal summenzionato art. 5, quelli di minimizzazione, di esattezza e di limitazione della conservazione, ed altresì espressivo, a sua volta, del

[1] Si fa riferimento al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 ed entrato in vigore il 25 maggio 2018. È composto da 99 articoli e 173 *considerando* con solo valore interpretativo. A riguardo, V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019; R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della privacy e* data protection, Milano, 2021. Si veda anche F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018.

[2] Si definisce trattamento qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, n. 2, del Reg. UE n. 2016/679). A riguardo, C. del Federico-A.R. Popoli, *Le definizioni*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 63 ss.

[3] Si definisce dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato") ritenendo tale colui che può essere identificato, direttamente o indirettamente, con particolare riferimento a un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, n. 1, del Reg. UE n. 2016/679). A riguardo, C. del Federico-A.R. Popoli, *Le definizioni*, cit., pp. 63 ss.

[4] Si dia lettura al disposto di cui all'art. 5, del Reg. UE n. 2016/679 di definizione dei principi applicabili al trattamento dei dati personali.

[5] Si dia lettura al disposto di cui all'art. 89, par. 1, del Reg. UE n. 2016/679 di definizione di garanzie e deroghe relative al trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

principio di trasparenza[6]. Evidenti connessioni si registrano, altresì, con il principio di liceità del trattamento, in particolare per quelli posti in essere da autorità pubbliche. Si provvederà quindi, nel proseguo, ad una attenta analisi del principio di limitazione della finalità del trattamento dei dati, così come disciplinato dal citato art. 5, al fine di rimarcare non solo le connessioni esistenti con gli altri principi vigenti in materia di *data protection*, ma anche il suo autonomo rilievo[7] ed il suo ambito applicativo teorico e nella casistica[8].

1.2. L'embrionale formulazione del principio di limitazione delle finalità nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali

Già con la firma nel 1950 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (c.d. CEDU)[9], all'art. 8, attraverso una formulazione resa in forma positiva, veniva riconosciuto il diritto alla *privacy* nella sua articolazione in diritto al rispetto della vita privata, della vita famigliare, del domicilio e della corrispondenza[10]. Come la Corte europea dei diritti dell'uomo ha costantemente ritenuto, l'intento è stato indubbiamente quello di assicurare lo sviluppo, senza ingerenze esterne, della personalità di ciascun individuo nei suoi rapporti con gli altri esseri umani[11]. Il concetto di "vita privata" è peraltro ampio e non suscettibile in astratto di una definizione esaustiva, comprendendo altresì aspetti quali l'integrità fisica e psicologica della persona, la sua identità anche di genere, l'orientamento sessuale, il nome, gli elementi relativi al suo diritto all'immagine ed altresì quelle informazioni personali che l'individuo possa legittimamente aspettarsi che non debbano essere pubblicate senza il suo consenso[12].

Lo stesso art. 8, al suo secondo comma – riletto in altra prospettiva messa ben in risalto dallo *UN Human Rights Committee (HRC)* in occasione del commen-

---

[6] G. Malgeri, *Comm. sub. art. 5 GDPR*, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della privacy e* data protection, cit., pp. 183 ss.; P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, I, pp. 445 ss. A riguardo si rinvia al successivo par. 2.2. *Il principio di limitazione della finalità quale fondamento di ulteriori principi in materia di data protection.*

[7] Si rinvia, *infra*, al par. 2 (*Portata del principio*).

[8] Si rinvia, *infra*, al par. 3 (*Applicazione del principio alla casistica*).

[9] La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, sottoscritta in data 4 novembre 1950, è entrata in vigore il 3 settembre 1953.

[10] Al contrario, nell'art. 17 del Patto internazionale sui diritti civili e politici del 1966 (*The International Covenant on Civil and Political Rights*), su cui ci si soffermerà successivamente (v., *infra*, part. 1.3), il diritto in questione appare espresso con una formulazione resa in forma negativa. Cfr., sul punto, anche M.E. Bonfanti, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Dir. um. dir. int*., 2011, n. 5, pp. 437 ss.

[11] C. Giakoumopoulos-G. Buttarelli-M. O'Flaherty, *Manuale sul diritto europeo*, Strasburgo, 2018, p. 25.

[12] CEDU, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo. Diritto al rispetto della vita privata e famigliare, del domicilio e della corrispondenza*, 2019, www.echr.coe.int.

to reso all'analoga formulazione dell'art. 17 dell'*International Covenant on Civil and Political Rights* del 1966[13] – ha introdotto una sorta di clausola di limitazione all'affermato diritto alla *privacy*, con un embrionale principio di limitazione della finalità del trattamento dei dati personali, nella parte in cui è stato previsto un elenco tassativo di ragioni a cui gli Stati nazionali possono ricorrere per giustificare eventuali trattamenti con cui vengono poste delle ingerenze alla *privacy* degli individui[14]. Tali interferenze, da intendersi quali limitazioni nell'esercizio del diritto al rispetto della propria vita privata come più sopra descritta, oltre a dover essere previste dalla legge, si pongono quali misure «che, in una società democratica», risultano necessarie «alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». In più occasioni, la Corte ha peraltro rimarcato la necessità che il rispetto delle finalità individuate nella Convezione debba sussistere in ciascuna delle fasi del trattamento di dati personali, quali la raccolta, la registrazione, la conservazione, la divulgazione o il trasferimento dei dati dell'individuo da parte della pubblica autorità, riconoscendo al contempo il diritto dell'interessato di decidere sul trattamento dei propri dati con la possibilità di accedevi, rettificarli o cancellarli.

È indubbio quindi che così facendo, la citata Convenzione ha riconosciuto, più o meno espressamente, che eventuali ingerenze alla riservatezza degli individui debbano trovare la propria giustificazione in finalità ben precise ed a quella limitarsi[15].

1.3. Il principio di limitazione delle finalità nel Patto internazionale sui diritti civili e politici

Il diritto alla protezione dei dati personali è stato implicitamente riconosciuto anche dall'art. 17 del Patto internazionale delle Nazioni Unite sui diritti civili e politici del 1966[16].

La norma, attraverso una formulazione resa in forma negativa, ha inteso stabilire, al primo paragrafo, il diritto di ogni individuo a non essere sottoposto a interferenze arbitrarie o illegittime nella propria vita privata, casa, famiglia o corrispon-

[13] Si rinvia, *amplius*, al par. 1.3 del presente scritto.

[14] C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 20.

[15] CEDU, *Leander c. Svezia,* ricorso n. 9248/81, 26 marzo 1987; *Uzun c. Germania*, ricorso 35623/05, 2 settembre 2010; *P.G. e J. H. c. Regno Unito*, ricorso n. 44787/98, 25 settembre 2001; *Amann c. Svizzera*, ricorso n. 27798/95, 16 dicembre 2000.

[16] Il Patto internazionale delle Nazioni Unite sui diritti civili e politici (*UN International Covenant on Civil and Political Rights*, in seguito indicato brevemente anche come *"Patto"* o *"Covenant"*), sottoscritto in data 16 dicembre 1966, è entrato in vigore il 23 marzo 1976. Si veda, a riguardo, M. NOVAK, *U.N. Covenant on Civil and Political Right: CCPR Commentary*, Kehl, 2005, pp. 377 ss.; A. CONTE-S. DAVIDSON-R. BURCHILL, *Defining Civil and Political Rights: The Jurisprudence of the United Nations Haman Rights Committee*, Aldershot, 2004, pp. 145 ss.; S. JOSEPH-J. SCHULTZ-P. CASTAN, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary*, Oxford, 2004, pp. 476 ss.

denza, né ad illegittimi attacchi al proprio onore ed alla propria reputazione[17]. Al secondo paragrafo, in termini positivi, l'art. 17 riconosce altresì a ciascun individuo il diritto ad essere tutelato dalla legge contro interferenze o attacchi eventualmente subiti[18]. Emerge, quindi, da una chiara lettura della norma, da un lato, il riconoscimento del diritto alla *privacy* dell'individuo e, dall'altro, il dovere dell'ordinamento d'accordare a tale individuo la necessaria protezione e/o tutela[19]. L'art. 17 in esame, infatti, nello specificare le condizioni necessarie affinché un individuo possa lecitamente subire una restrizione nel godimento del suo diritto alla *privacy* stabiliva il principio secondo cui nessuna ingerenza potesse aver luogo al di fuori dei casi stabiliti dalla legge: le interferenze o gli attacchi alla *privacy* erano quindi legittimi solo quando venivano previsti per legge dall'ordinamento di uno Stato, le cui disposizioni dovevano a loro volta essere conformi a quelle contenute nel *Covenant*, nonché ai fini ed ai principi di quest'ultimo. La valutazione di legittimità doveva perciò avere principalmente quale termine di riferimento la normativa nazionale, ma anche indirettamente gli obblighi internazionali previsti nel patto[20]. La riserva di legge serviva dunque per porre un argine a trattamenti arbitrati e illegittimi, invasivi del diritto alla *privacy*, facendo in modo che gli Stati nazionali andassero ad individuare preventivamente e formalmente le finalità del trattamento.

Seppur legittime, le interferenze nella vita privata, nella famiglia, nella casa e nella corrispondenza o, in altre parole, le finalità perseguite dallo Stato nazionale quale titolare del trattamento, non devono essere «arbitrarie»[21]. La dottrina, esaminata a riguardo, nel considerare quando il trattamento possa presentarsi come arbitrario, richiama i concetti di ingiustizia, imprevedibilità, irragionevolezza nonché l'atteggiamento discriminatorio avuto riguardo al caso di specie, che non sia risultato conforme alle disposizioni, agli obiettivi ed ai fini del *Covenant*[22].

Nell'ambito del presente discorso, giova menzionare anche il significativo commento all'art. 17, del *Covenant*, reso dallo *Human Rights Committee* delle Na-

---

[17] Il testo integrale del *Convenant* è consultabile *online* all'*url* seguente: https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf (consultato da ultimo in data 4 aprile 2022).

[18] Segnatamente, l'art. 17, del *Covenant* stabilisce che «1. *Non one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation*. 2. *Everyone has the right to the protection of the law against such interference or attacks*».

[19] M.E. Bonfanti, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, cit., pp. 437 ss.

[20] *Ibidem.*

[21] Cfr. l'*incipit* dell'art. 17 cit. del *Covenant*: «*Non one shall be subjected to arbitrary or unlawful interference with his privacy (…)*.

[22] M. Novak, *U.N. Covenant on Civil and Political Right: CCPR Commentary*, cit., pp. 377 ss.

zioni Unite[23]. Ci si riferisce, in particolare, al *General Comment n. 16*[24] col quale il Comitato dei diritti umani, in relazione ai principi e diritti in materia di *data protection*, aveva precisato le modalità con le quali poteva essere compiuto, ai sensi dell'art. 17 cit., il trattamento delle informazioni personali dell'individuo. In particolare, secondo il Comitato, la raccolta e la registrazione in archivi elettronici, cartacei o di altro genere di informazioni personali di individui, eseguita deve essere regolata dalla legge sia nel caso in cui il trattamento avvenisse ad opera di soggetti pubblici, sia da soggetti privati[25]. Gli Stati, quindi, nei loro rispettivi ordinamenti, devono prevedere misure di carattere effettivo per garantire che le informazioni relative alla vita privata degli individui venissero trattate, fatte circolare o utilizzate solo dai soggetti autorizzati per legge e, in ogni caso, che *non venissero utilizzate per fini incompatibili* rispetto a quelli previsti dal *Covenant*[26]. Le informazioni raccolte dall'autorità pubblica inoltre possono essere trattate solo qualora la loro conoscenza sia ritenuta essenziale per l'interesse complessivo della società[27]. Per il Comitato, ogni individuo ha inoltre il diritto di conoscere se vi siano dei dati a lui relativi conservati in archivi elettronici, quali siano tali dati, per quali motivi siano stati raccolti e quali siano i soggetti, pubblici o privati, che controllano tali dati[28]. L'individuo conserva inoltre il diritto di ottenere la rettifica o la cancellazione delle informazioni non corrette ovvero raccolte e trattate contrariamente alle disposizioni di legge[29].

Da una disamina quindi del contenuto del *Covenant* del 1966, unitamente ai commenti adottati dal Comitato dei diritti umani nel 1988 (su cui probabilmente molto ha influito la Convenzione di Strasburgo in materia di tutela della persona di fronte al trattamento automatico di dati personali emanata del 1981), è possibile individuare, seppur in forma incompleta o parziale, l'enucleazione di alcuni principi e diritti che stanno alla base della disciplina internazionalistica in materia di *data pro-*

[23] Cfr. UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation*, 8 April 1988, consultabile *online* all'*url* https://www.refworld.org/docid/453883f922.html (consultato da ultimo in data 4 aprile 2022).

[24] COMITATO DEI DIRITTI UMANI, *General Comment No. 16 on The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17),* UN Doc. HRI/GEN/1/Rev.1 dell'8 aprile 1988.

[25] Si dia lettura dei paragrafi 1 e 10 del *General Comment No. 16 on The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17)*, UN Doc. HRI/GEN/1/Rev.1 dell'8 aprile 1988.Nella pate

[26] M.E. BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, cit., pp. 437 ss.

[27] Si dia lettura del paragrafo 7 del *General Comment No. 16 on The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17),* UN Doc. HRI/GEN/1/Rev.1 dell'8 aprile 1988.

[28] Si dia lettura del paragrafo 10 del *General Comment No. 16 on The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17),* UN Doc. HRI/GEN/1/Rev.1 dell'8 aprile 1988.

[29] *Ibidem.*

tection[30]. Tra questi è indubbiamente ravvisabile oltre a quelli di legalità, sicurezza e di proporzionalità, il *principio di finalità* del trattamento, oggetto del presente contributo, in ragione del quale le informazioni degli individui (ora, definiti interessati) non possono essere utilizzate per *fini* incompatibili rispetto a quelli previsti dal *Covenant*, inclusi quelli individuati dai singoli Stati nazionali, nel proprio ordinamento, per contenere le ingerenze arbitrare ed illegittime alla *privacy* degli individui, giusto quanto previsto art. 17, del *Covenant*[31].

Emerge indubbiamente un approccio particolarmente prudente del Comitato che, seppur aveva a disposizione molteplici strumenti giuridici internazionali in materia di *data protection*[32] dai quali prendere ulteriori spunti, ha preferito limitarsi ad un intervento minimo nell'interpretazione di tali principi e diritti dell'individuo, probabilmente in ragione della consapevolezza della difficoltà di definire precise linee guida in materia di protezione dei dati personali che potessero essere universalmente condivise[33].

---

[30] L.A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Right Treaties*, in *International Journal of Law and Information Thechnology*, 1998, pp. 247 ss.

[31] In particolare, il Comitato ha rimarcato che il *Covenant* impone ai singoli Stati di offrire garanzie adeguate sul rispetto dei diritto alla privacy quale diritto ad essere tutelato contro possibili ingerenze illecite ed arbitrarie, poste in essere da parte degli Stati medesimi e di persone fisiche o giuridiche, sicché, preicsa il Comitato «*The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right, In this connection, the Committee wishes to point out that in the reports of States parties to the Covenant the necessary attention is not being given to information concerning the manner in which respect for this right is guaranteed by legislative, administrative or judicial authorities, and in general by the competent organs established in the State. In particular, insufficient attention is paid to the fact that article 17 of the Covenant deals with protection against both unlawful and arbitrary interference. That means that it is precisely in State legislation above all that provision must be made for the protection of the right set forth in that article. At present the reports either say nothing about such legislation or provide insufficient information on the subject. The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant. The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances*» (v. par. 1-4, del Commento *de quo*).

[32] A seguire alcuni esempi: Consiglio d'Europa, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – CETS No. 108 (Convention No. 108)*, adottato a Strasburgo il 28 gennaio 1981, in vigore dal 1° ottobre 1985; *Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* del 23 settembre 1980.

[33] C. Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, in *Computer Law & Security Review*, 2009, pp. 307 ss.

1.4. Il principio di limitazione delle finalità nella Convenzione 108 e nella Convenzione 108+

La Convenzione di Strasburgo del Consiglio d'Europa siglata nel 1981[34] è uno dei più importanti strumenti a protezione delle persone avuto riguardo al trattamento automatizzato dei dati personali. In ragione delle diversità esistenti tra le varie normative nazionali, la Convenzione 108 nasce con l'intento di assicurare un livello minimo di garanzie mediante l'introduzione di una serie di principi cui avrebbero dovuto conformarsi le varie legislazioni nazionali in modo da assicurare il rispetto del diritto alla *privacy* degli individui nei confronti di ogni elaborazione automatizzata di dati concernenti soggetti identificati o identificabili[35]. Oltre a ciò, la Convenzione ha visto le sue origini anche nell'esigenza di tutelare le persone dal proliferare di tecnologie dell'informazione e della comunicazione sempre più diffuse a partire già dagli anni sessanta[36]. Oggi la Convenzione 108 rappresenta l'unico strumento vincolante a livello internazionale in materia di *data protection*, potendo ad essa aderire anche Stati non membri del Consiglio d'Europa[37].

Le norme in essa contenute, che hanno trovato ispirazione nell'art. 8 della Convenzione europea dei diritti dell'uomo[38], sono applicabili a tutti i trattamenti di dati personali, effettuati sia nel settore privato che pubblico, con lo scopo di proteggere i soggetti interessati da eventuali abusi. L'art. 1 sancisce, infatti, che lo «scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ("protezione dei dati")» mentre il successivo art. 5 introduce molteplici

[34] Si fa riferimento alla *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* siglata a Strasburgo il 28 gennaio 1981. È altrimenti nota come *Convenzione 108* del Consiglio d'Europa. La regolamentazione della Convenzione 108 si concentra principalmente sui trattamenti automatizzati (anche se solo parzialmente), ma considera anche i trattamenti manuali come oggetto di tutela, prevedendo la possibilità che i singoli Stati estendano la definizione di trattamento anche a tali trattamenti, purché i dati personali siano contenuti o destinati a figurare in archivi.

[35] A tal proposito l'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) ha emanato varie raccomandazioni "*finalizzate a sollecitare i Paesi membri ad un'uniformità di interventi nel campo della raccolta e diffusione di dati personali*". A riguardo, R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., p. 33.

[36] C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 27.

[37] Tutti gli Stati membri dell'Unione europea hanno ratificato la Convenzione 108 e nel 1999 vi ha provveduto anche la stessa Unione. La Convenzione n. 108 è aperta all'adesione anche di parti non contraenti del Consiglio d'Europa. La portata della Convenzione come norma universale e il suo carattere aperto potrebbero costituire un presupposto per promuovere la protezione dei dati a livello mondiale. Ad oggi, 55 paesi sono parti contraenti della Convenzione 108. L'Uruguay è il primo paese extraeuropeo che via ha aderito, nell'agosto 2013, Maurizio, Senegal e Tunisia vi hanno aderito nel 2016 e nel 2017, Capo Verde e Messico nel 2018, Argentina e Marocco nel 2019. A riguardo, C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 26.

[38] Si dia lettura dall'art. 8, della Convenzione europea dei diritti dell'uomo di disciplina del diritto al rispetto della vita privata e famigliare.

principi in materia di *data protection*, tesi alla disciplina delle attività di trattamento, fra i quali il ben noto principio di finalità[39]. In particolare, è previsto che i dati devono essere raccolti e trattati solo in base a specifiche norme che ne autorizzano il trattamento automatizzato, devono essere trattati inoltre solo per scopi specifici e legittimi e non devono essere destinati ad un uso incompatibile con la finalità di trattamento originaria. Infine, è altresì previsto che i dati personali non devono essere conservati oltre il tempo necessario per raggiungere lo scopo prefissato e devono essere corretti, pertinenti allo scopo e non eccessivi rispetto alla finalità perseguita. Risultano quindi disciplinati tutti i ben noti principi fondamentali che reggono l'intera normativa in materia di protezione dei dati personali.

Il 18 maggio del 2018 il Consiglio ha adottato un protocollo di modifica del testo della Convenzione originario (detto anche Convenzione 108+), teso a modernizzarla, al fine di renderla un quadro giuridico più consono ad un'epoca contrassegnata da un pervasivo sviluppo tecnologico, che impone di soddisfare nuove esigenze, e nella quale le violazioni del diritto alla protezione dei dati sono divenute una importante preoccupazione[40]. Se nulla è cambiato in materia di principi applicabili alle attività di trattamento, le nuove norme avvicinano notevolmente il regime della Convenzione 108 a quello poi introdotto dal Reg. UE n. 2016/679[41]. Nel considerare l'ambito ed i limiti di una particolare finalità, ad esempio, la Convenzione 108+, così come poi il Regolamento UE, ricorrono al concetto di compatibilità: l'utilizzo dei dati per *finalità compatibili* è consentito in ragione della base giuridica iniziale. I dati non possono, pertanto, essere oggetto di un ulteriore trattamento considerato inappropriato, inatteso o contestabile dell'interessato[42]. Così ancora, la Convenzione 108+, al pari del Reg. UE n. 2016/679, dichiara che «l'ulteriore trattamento a fini archivistici, o di ricerca scientifica o storica o a fini statistici» dovrebbe *a priori* essere considerato compatibile con la finalità iniziale. Tuttavia, per l'ulteriore trattamento di dati personali devono essere previste garanzie adeguate, come l'anonimizzazione,

[39] Si di lettura degli artt. 1 e 5, della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale di disciplina, rispettivamente, di «*oggetto e scopo*» della Convenzione oltre che della «*qualità dei dati*».

[40] Il protocollo, inoltre, fornisce un quadro giuridico robusto e flessibile per facilitare il flusso dei dati attraverso le frontiere e fornire garanzie efficaci. Il protocollo introduce innovazioni rilevanti come l'obbligo di comunicare le violazioni dei dati (*data breach*) e il rafforzamento del principio di minimizzazione dei dati, e di trasparenza dell'elaborazione. Principi ritenuti fondamentali per mantenere la fiducia nell'ambiente digitale. Richiede inoltre anche il rispetto del principio di *privacy by design*, introducendo ulteriori tutele nell'ambito dei trattamenti algoritmici, come il diritto di ottenere informazioni sulla logica alla base dell'elaborazione dei dati. La Convenzione 108+ riguarda tutti i tipi di trattamenti, compreso quelli derivanti da sicurezza nazionale e difesa, tranne i trattamenti operati da persone fisiche nell'esercizio di attività puramente personali e domestiche. Il nuovo protocollo, ovviamente, si applica ai soli Stati firmatari, mentre agli Stati firmatari della sola Convenzione originale si applica quest'ultima. Il 5 marzo del 2019 l'Italia ha ratificato la Convenzione 108+.

[41] C. Giakoumopoulos-G. Buttarelli-M. O'Flaherty, *Manuale sul diritto europeo*, cit., p. 138.

[42] Si dia lettura della relazione esplicativa della Convenzione 108+, punto 49. A riguardo, si rinvia al successivo paragrafo *2.6. Le cc.dd. finalità incompatibili e il compatibility test*.

la cifratura con crittografia o la pseudonimizzazione dei dati e la limitazione dell'accesso agli stessi[43].

1.5. Il principio di limitazione delle finalità nella Direttiva 95/46/CE

Il diritto alla protezione dei dati personali fa ingresso nell'ordinamento comunitario con la Direttiva 95/46/CE[44], uno dei punti di riferimento cardine in materia di *privacy*, che si è sin da subito dimostrata uno strumento molto adatto a consentire ai nuovi Paesi, che nel corso degli anni sono entrati a far parte dell'Unione europea, di adempiere all'obbligo di dotarsi di legislazioni di protezione dei dati personali con essa coerenti. L'intento del legislatore comunitario era quello di riuscire a conciliare la necessità di ridurre gli ostacoli esistenti alla circolazione dei dati personali, per agevolare lo sviluppo del mercato economico interno, con l'esigenza di salvaguardare i diritti fondamentali della persona, ben conscio della disparità di tutela del diritto alla vita privata esistente fra i diversi Paesi. Tale Direttiva ha quindi provveduto, da un lato, ad armonizzare le disposizioni vigenti negli Stati membri[45] e, dall'altro, a garantire un livello alto ed equivalente di protezione della persona rispetto al trattamento dei dati[46].

Tali finalità emergono già dalla lettura dell'art. 1, della Direttiva che definisce con precisione l'oggetto della stessa, affermando che «gli Stati membri si impegnano a garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali».

Di rilevo, ai fini del discorso, è altresì l'art. 6 che, nell'introdurre per la prima volta, in maniera ben chiara e dettagliata, i «principi» guida che debbono orientare i diversi Paesi disponeva che «i dati personali devono essere: *a)* trattati lealmente e lecitamente; *b)* rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate; *c)* adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successi-

[43] Si dia lettura della Relazione esplicativa della Convenzione 108+, punto 49. A riguardo, C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 139.

[44] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, adottata in applicazione degli artt. 95 e 251 del Trattato istitutivo della Comunità europea.

[45] Per alcuni degli Stati membri, tra cui l'Italia e la Grecia, l'intento del legislatore unionale è stato quello di sollecitare l'approvazione di una disciplina *ad hoc* in materia di *data protection*.

[46] Si dia lettura del *considerando* n. 8 della Direttiva 95/46/CE ove viene precisato «che, per eliminare gli ostacoli alla circolazione dei dati personali, il livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento di tali dati deve essere equivalente in tutti gli Stati membri; che tale obiettivo, fondamentale per il mercato interno, non può essere conseguito esclusivamente attraverso l'azione degli Stati membri, tenuto conto in particolare dell'ampia divergenza esistente attualmente tra le normative nazionali in materia e della necessità di coordinarle affinché il flusso transfrontaliero di dati personali sia disciplinato in maniera coerente e conforme all'obiettivo del mercato interno ai sensi dell'articolo 7 A del trattato; che risulta pertanto necessario un intervento della Comunità ai fini di un ravvicinamento delle legislazioni».

vamente trattati; *d)* esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati; *e)* conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici». Ancora, al secondo comma, lo stesso art. 6, già in logica *accountability*, attribuiva al "responsabile" del trattamento (che, nella nomenclatura attuale è da intendersi il "titolare" del trattamento) la garanzia del «rispetto delle disposizioni del paragrafo 1».

Per la prima volta, quindi, il legislatore comunitario assegnava la regia delle attività di trattamento all'autore materiale dello stesso (il "titolare" del trattamento, ossia il *data controller*) che doveva, fra gli altri, definirne le *«finalità determinate, esplicite e legittime»* che, sino a quel momento, venivano individuate nei testi normativi con l'enunciazione delle ragioni che potevano giustificare un'ingerenza nella *privacy* degli interessati. L'oggettiva e preventiva individuazione delle finalità del trattamento dei dati personali rappresentava quindi, per la prima volta, dalla vigenza della Direttiva comunitaria, un aspetto fondamentale della disciplina della *data protection*, poiché da essa deriva l'individuazione della cornice entro la quale il titolare del trattamento è legittimato a muoversi[47]. I requisiti richiesti per le finalità perseguite, che alludono al carattere determinato ed esplicito delle stesse, riflettono già, peraltro, il principio di trasparenza, volendo evidenziare sin da subito le modalità del trattamento dei dati e verificarne la legittimità in relazione ai fini per i quali lo stesso è stato avviato. Può ben dirsi quindi che con la Dir. 95/46/CE vede la luce una disciplina che, per molteplici aspetti, porrà le basi per l'attuale normativa contenuta nel Reg. UE n. 2016/679.

1.6. Il principio di limitazione delle finalità nella Carta dei diritti fondamentali dell'Unione europea

Il diritto di controllare il flusso dei propri dati personali ha avuto un importante riconoscimento anche nella Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza il 7 dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione[48]. Essa ha rappresentato un radicale cambio di prospettiva nella politica europea sui diritti fondamentali: mentre nella Direttiva 95/46/CE la loro protezio-

[47] M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 206 ss.

[48] La Carta dei diritti fondamentali dell'Unione europea è stata proclamata il 7 dicembre 2000 ed è stata pubblicata sulla Gazzetta Ufficiale della Comunità Europea n. 2000/C-364/01. A riguardo, cfr. GPDP, Relazione 2000, Roma, Presidenza del Consiglio dei Ministri, 2001, 262. A riguardo, P. Rescigno, *La Carta dei diritti fondamentali dell'Unione europea*, Torino, 2003; A. Barbera, *La Carta europea dei diritti e la Costituzione italiana*, in Aa.Vv., *Le libertà e i diritti nella prospettiva europea*, Padova, 2002, p. 107; M. Cartabia, *Una Carta dei diritti fondamentali per l'Unione europea*, in *Quaderni cost.*, 2, 2000; S. Veca, *A proposito della "Carta dei diritti fondamentali" dell'Unione Europea*, in *Iride*, 1, 2000.

ne era soprattutto funzionale al perseguimento di finalità economiche[49], nella Carta di Nizza i diritti fondamentali sono tutelati in sé e per sé. Si era infatti parlato, in quel mentre, di uno sviluppo della comunità europea da unione economica e monetaria, che poneva al centro la libertà di circolazione europea di persone, capitali, beni e servizi, ad una Europa dei diritti e dei cittadini[50].

Ecco, quindi, che nella Carta trovano riconoscimento, per la prima volta, alcuni nuovi diritti, la cui tutela si era resa necessaria «alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici»[51]. Tra questi diritti inediti, vi era il diritto alla protezione dei dati personali che ha trovato, in tal modo, un autonomo riconoscimento accanto al tradizionale diritto al rispetto della vita privata e famigliare. La sua introduzione rispondeva alla necessità di garantire una specifica tutela della *privacy* nei confronti di attività diffuse e potenzialmente pericolose per alcuni diritti fondamentali. L'utilizzo di mezzi automatizzati nella gestione delle informazioni aveva, infatti, facilitato la possibilità di creare banche dati e di far circolare agevolmente le informazioni in esse contenute, ponendo l'esigenza di una tutela della *privacy* e degli altri diritti della persona rispetto al trattamento dei dati personali. D'altra parte, l'integrazione europea, implicando l'intensificazione dei flussi transfrontalieri di dati, richiedeva che venissero impedite limitazioni della circolazione verso determinati Stati, giustificate dalla mancanza di *standard* minimi di sicurezza.

La disposizione più innovativa nell'ambito della disciplina della *privacy* è indubbiamente l'art. 8 della Carta di Nizza, che recepisce i principi sanciti dalla normativa europea in materia di trattamento dei dati personali[52]. Al primo paragrafo

---

[49] Secondo G.P. CIRILLO, *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004, p. 5, l'obiettivo essenziale della Direttiva n. 95/46/CE «è la armonizzazione delle legislazioni nazionali per evitare effetti negativi sul funzionamento del mercato comune». Inoltre, prosegue l'autore, «è noto che la Corte di Giustizia ha affermato in numerose pronunce che (…) i diritti fondamentali costituiscono, in quest'ottica, non un controlimite assoluto al mercato, ma semmai tendono a stabilizzare lo spazio economico europeo; la loro protezione è necessaria per evitare forme di social dumping tra i paesi aderenti e la possibilità che le imprese facciano lo "shopping" tra le legislazioni, scegliendo, nell'ambito della comunità, i paesi meno garantistici».

[50] S. MELCHIONNA, *I principi generali*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali,* Santarcangelo di Romagna, 2004, p. 32; S. RODOTÀ, *La Carta Europea dei diritti – una vittoria dimezzata*, in *La Repubblica*, 4 ottobre 2000, p. 17.

[51] Si esprime in questi termini il preambolo alla Carta dei diritti fondamentali dell'Unione europea.

[52] Si dia lettura dell'art. 8 della Carta europea dei diritti fondamentali dell'Unione europea disciplinante la «*la protezione dei dati di carattere personale*». Secondo la ricostruzione di F. DONATI, *Commento art. 8*, in R. BIFULCO-M. CARTABIA-A. CELOTTO (a cura di)*, L'Europa dei diritti*, Bologna, 2001, p. 83, i diritti garantiti dall'art. 8 trovano riconoscimento, in ambito comunitario, nella Direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali (poi abrogata e sostituita dal Reg. UE n. 679/2016), nonché nell'art. 286 del Trattato C.E. sulla disciplina applicabile alle istituzioni e agli altri organismi comunitari in materia di *privacy*. Il diritto alla protezione dei dati personali, invece, non viene espressamente menzionato nella C.E.D.U., nella Dichiarazione universale dei diritti dell'uomo, nel Patto internazionale sui diritti civili e politici delle Nazioni Unite e nella dichiarazione congiunta del Parlamento europeo, del Consiglio e della Commissione sui diritti e le libertà fondamentali del 1989. Secondo altra dottrina, il riconoscimento del diritto alla protezione dei dati personali nella Carta si fonda sull'art. 286 T.C.E., sulla Direttiva 95/46/CE (poi abrogata e sostituita dal Reg. UE n.

viene riconosciuto ad ogni individuo il diritto alla protezione dei dati personali che lo riguardano: la tutela è, quindi, limitata alle sole persone fisiche allo stesso modo di quanto era previsto dalla Direttiva comunitaria 95/46/CE. Al secondo paragrafo, avuto riguardo alle condizioni in presenza delle quali è ammesso il trattamento dei dati personali, il legislatore si è limitato a prevedere che i dati devono essere trattati «*secondo il principio di lealtà*» e «*per finalità determinate*»[53]; il trattamento dei dati è ritenuto quindi legittimo solo in presenza del consenso della persona interessata o di un altro fondamento previsto dalla legge, lasciando in tal modo alla discrezionalità del legislatore (prima nazionale, ora europeo) la scelta dei margini di deroga al consenso dell'interessato. In ragione del fatto che la Direttiva 95/46/CE individuava i casi in cui il legislatore nazionale poteva derogare al principio del necessario consenso per il trattamento dei dati personali, si è sempre ritenuto, nel merito, che la Carta offrisse un livello di protezione almeno equivalente a quello riconosciuto dalla direttiva medesima. Va però considerato che la Carta ha assunto, con il Trattato di Lisbona, lo stesso valore giuridico dei trattati dell'UE, sicché è atto normativo posto all'apice delle fonti del diritto europeo (e, conseguentemente, nazionale). Pertanto, il riconoscimento del diritto alla protezione dei dati personali nell'art. 8 della Carta dei diritti fondamentali dell'UE vale anche a rendere non derogabile da altri atti normativi ordinari del diritto europeo (ad es., con successive direttive o regolamenti) i capisaldi della disciplina ora contenuta nel cit. art. 8 della Carta, che, pertanto, in ragione di tale inserimento, godono ora di una tutela rafforzata.

Sempre nel secondo paragrafo dell'art. 8, la Carta riconosce a ciascun individuo «il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica». Anche in tal caso, le garanzie riconosciute dalla norma in esame si aggiungono a quelle già previste dalla normativa comunitaria, ma il valore giuridico delle prime, collocate all'apice delle fonti del diritto europeo, ne garantiscono l'inderogabilità, portando ad una tutela rafforzata rispetto a quella riconosciuta dalla più volte ricordata Direttiva 95/46/CE. L'art. 8 della Carta di Nizza si chiude infine con la previsione di un'autorità indipendente a cui affidare il controllo del rispetto delle regole in materia di protezione dei dati personali, riprendendo così, nuovamente, quanto stabilito dalla Direttiva 95/46/CE, ma rafforzandone la portata.

679/2016), sull'art. 8 della C.E.D.U., nonché sulla Convenzione di Strasburgo del 1981. Sul punto v. G. Alpa, *Prefazione*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., p. XII.

[53] Rispetto alla Direttiva comunitaria 95/46/CE mancano una serie di altre importanti prescrizioni riguardanti l'adeguatezza e la pertinenza dei dati rispetto alla finalità del trattamento, la cancellazione dei dati inseriti e le modalità di conservazione, la riservatezza e la sicurezza dei trattamenti. A riguardo, F. Donati, *Commento art. 8*, cit., p. 87, ritiene che «se da un lato questo è comprensibile, considerando che si tratta di una Carta di diritti che, come tale, non si sofferma sulla disciplina di dettaglio, ma enuncia principi generali di ampia portata, dall'altro, la scelta di inserire solo alcuni dei criteri stabiliti dal legislatore comunitario, lasciandone fuori altri, parimenti importanti, appare criticabile». Nulla, invece, viene detto nell'art. 8 della Carta riguardo la nozione di "*trattamento*"; a tal proposito, dai lavoratori preparatori, sembra emergere che i redattori della Carta abbiano accolto l'ampia accezione di "*trattamento*" adottata dal legislatore comunitario, secondo cui tale attività comprende qualsiasi tipo di operazione svolta con o senza il supporto di mezzi telematici.

Può ben dirsi quindi che il principio di finalità del trattamento, rinvenuto in maniera embrionale nel Patto internazionale sui diritti civili e politici, oltre che nella Convenzione europea dei diritti dell'uomo, è presente quindi, in maniera espressa e rafforzata, anche nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea laddove, nel rimarcare che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano», si precisa che «tali dati devono essere trattati», fra gli altri, «per finalità determinate»[54]. La Carta chiaramente quindi individua il principio di limitazione della finalità del trattamento, collocandolo tra i principi inderogabili dell'ordinamento europeo, posti all'apice della gerarchia delle fonti dell'UE, richiedendo inoltre, quale fondamento dell'attività di trattamento dei dati personali ed al fine di poterlo qualificare come lecito, che lo stesso si svolga «in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge».

La Carta di Nizza dispone, infine, che il diritto alla protezione dei dati personali (art. 8) può essere limitato alle condizioni previste dall'art. 52[55]. Secondo tale disposizione le limitazioni all'esercizio dei diritti garantiti debbono: *a)* essere previste dalla legge; *b)* rispettare il contenuto essenziale dei diritti; *c)* rispettare il principio di proporzionalità; *d)* essere necessarie e rispondenti a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

In conclusione, può ben dirsi che il significato e la portata del diritto alla *privacy* riconosciuto dalla Carta di Nizza, seppur ricalcando *mutatis mutandis* quello della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà personali, ne ha determinato l'innalzamento del livello di protezione fino a considerarlo un diritto fondamentale nell'ambito del diritto dell'Unione.

1.7. Il principio di limitazione delle finalità nella l. 31 dicembre 1996, n. 675

In Italia, uno dei primi interventi legislativi in materia di protezione dei dati personali è riconducibile alla legge n. 675/1996 di recepimento in Italia della Direttiva 95/46/CE, concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali[56].

L'art. 1 di tale legge, seguendo anche i modelli europei, indica l'ambito di applicazione della normativa e ciò che essa mira a garantire, ossia che «il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e

[54] C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 22.

[55] Le stesse limitazioni sono previste dalla Carta di Nizza per il diritto al rispetto della vita privata, riconosciuto dall'art. 7 della Carta. Sull'art. 52 della Carta, in rapporto con l'art. 8 del medesimo testo normativo e, più in generale, con il diritto alla protezione dei dati personali disciplinato dall'intero Reg. UE n. 679/2016, si veda F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., *passim* e, ivi, spec. pp. 205 ss.

[56] Trattasi della legge n. 675 del 31 dicembre 1996 rubricata «*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*», pubblicata sulla Gazzetta Ufficiale n. 5 dell'8 gennaio 1997. La legge è stata abrogata ai sensi dell'art. 183, co. 1, lett. *a)*, del Codice in materia di protezione dei dati personali. A riguardo, G. FINOCCHIARO, *Privacy e protezione dei dati personali*, Bologna, 2016, pp. 21 ss.

all'identità personale»[57]. Quella che si viene a rappresentare è quindi una definizione di diritti, oggetto di disciplina, ben più ampia e completa di quella prospettata dalla direttiva CE, includendo oltre alla tutela della vita privata anche la dignità umana.

Da una disamina del testo di legge, poi confluito con modifiche nel Codice in materia di protezione dei dati personali (d.lgs. 196/2003), il principio di finalità emergeva con riguardo a diversi ambiti. Anzitutto, rilevava nella definizione di titolare del trattamento individuato nella «persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza»[58]. Il titolare era quindi sin da allora individuato quale *controller* dei dati personali e delle attività di trattamento, a cui comunque spettava ogni potere decisionali in ordine sono solo alle modalità del trattamento, ma anche alle sue finalità. Ulteriori riferimenti sono contenuti nell'art. 7 di disciplina della c.d. notificazione, laddove si precisava che «il titolare che intenda procedere ad un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto a darne notificazione al Garante se il trattamento, in ragione delle relative modalità o della natura dei dati personali, sia suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato». La notificazione, sottoscritta dal notificante e dal titolare del trattamento, doveva riportare fra gli altri anche la precisa indicazione delle *finalità* e delle modalità con cui sarebbero state poste in essere le attività di trattamento. La norma peraltro riportava l'obbligo di una notificazione preventiva una sola volta, a mezzo di lettera raccomandata ovvero con altro mezzo idoneo a certificarne la ricezione, a prescindere dal numero delle operazioni da svolgere, nonché dalla durata del trattamento e poteva riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione era richiesta solo in caso di mutamento di taluno degli elementi che in essa dovevano essere riportati[59].

Particolarmente significativa è poi la formulazione dell'art. 9 della l. 675/1996, rubricato «*Modalità di raccolta e requisiti dei dati personali*», ove, accanto ai principi di liceità e correttezza, esattezza, completezza, minimizzazione e di limitazione della conservazione[60], si ha una chiara formulazione del principio di limitazione delle finalità, imponendo non solo che il trattamento possa avvenire solamente «per scopi determinati, espliciti e legittimi» e che i dati possano essere utilizzati solamente «in termini non incompatibili con tali scopi», ma anche che i dati medesimi siano «non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati»[61]

---

[57] Si dia lettura dell'art. 1, della l. n. 675/1996 di individuazione di «*finalità e definizioni*».

[58] Si dia lettura dell'art. 1, co. 1, lettera d) della l. n. 675/1996 di individuazione di «*finalità e definizioni*».

[59] Si dia lettura dell'art. 7 della l. n. 675/1996 di disciplina della «*notificazione*». A riguardo, M. Chiarolla, *L'obbligo di notifica ed i soggetti interessati*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., pp. 323 ss.

[60] Il principio di necessità non era quindi "espressamente" disciplinato dalla l. n. 675/1996. Così G. Finocchiaro, *Privacy e protezione dei dati personali*, cit., pp. 114 ss. Sul punto di veda anche quanto riportato nel Capitolo X del presente volume, dedicato al principio di necessità.

[61] Segnatamente, l'art. 9, co. 1, della l. 675/1996 stabilisce che «I dati personali oggetto di trattamento devono essere: *a)* trattati in modo lecito e secondo correttezza; *b)* raccolti e registrati per *scopi* determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incom-

Seppur in assenza di una precisa enucleazione dei principi da applicarsi all'attività di trattamento di dati personali, che nella cit. legge italiana erano invece considerati alla stregua di «requisiti» dei dati o criteri concernenti le «modalità» della loro raccolta, è comunque ben chiaro che, anche nella vigenza della disciplina italiana *ante* Codice, il principio di finalità s'atteggiava già, sostanzialmente, a guida in materia di *data protection*, rappresentando un elemento cruciale del trattamento, oggetto di definizione da parte del titolare, ben prima dell'avvio delle attività, dovendo per di più essere rappresentato già in sede di notificazione, per i trattamenti allora soggetti a tale obbligo.

1.8. Il principio di limitazione delle finalità nel Codice della *privacy* e nel GDPR

Punto di riferimento centrale in Italia, prima del nuovo Reg. UE n. 2016/679 (GDPR), è stato certamente il Codice in materia di dati personali, emanato con il d.lgs. n. 196 del 30 giugno 2003 che ha provveduto ad una attività di razionalizzazione, semplificazione e coordinamento in una sorta di testo unico, di tutte le precedenti disposizioni in materia di *data protection*[62]. La disciplina ordinata della materia si era resa quanto mai necessaria sia in ragione dell'avvento delle nuove tecnologie, dei *computer*, dei sistemi di raccolta dei dati, quali i *data base*[63], sia per il progressivo stratificarsi di ulteriori norme nazionali in tale settore dell'ordinamento, che hanno richiesto un intervento normativo volto a razionalizzare e ordinare sistematicamente l'intera disciplina.

Più di un decennio dopo l'entrata in vigore del Codice della *privacy*, il legislatore europeo ha provveduto alla scrittura del Reg. UE n. 2016/679 ben consapevole che, sebbene la Direttiva 95/46/CE avesse introdotto validi principi ed obiettivi, non aveva impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né aveva eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni *online* comportino rischi per la protezione delle persone giuridiche. Infatti, oggi, nel pieno dell'era digitale, vi è la diffusa sensazione che i nostri dati personali siano costan-

patibili con tali scopi; *c)* esatti e, se necessario, aggiornati; *d)* pertinenti, completi e non eccedenti rispetto alle *finalità* per le quali sono raccolti o successivamente trattati; *e)* conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli *scopi* per i quali essi sono stati raccolti o successivamente trattati».

[62] Ci si riferisce al d.lgs. n. 196 del 30 giugno 2003 poi integrato dalle modifiche introdotte dal d.lgs. n. 101 del 10 agosto 2018 recante «*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*». Per un commento al testo originario del Codice si veda C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, Padova, 2007, I e II.

[63] Infatti, negli ultimi anni, il potere di controllo dell'individuo sulla circolazione delle informazioni che lo riguardavano si era andata configurando quale questione centrale ed emergente della società, definita società dell'informazione, nella quale ai *mass media* tradizionali, erano andate sovrapponendosi l'informatica e le reti telematiche. Cfr. G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., pp. 21 ss.

temente a rischio e che vi sia una costante ipoteca sull'inviolabilità della propria sfera privata e, soprattutto, sulla controllabilità della circolazione dei propri dati con la conseguente esigenza di assicurare un'applicazione della disciplina sulla *privacy* omogenea su tutto il territorio dell'Unione europea. Tale intento del legislatore è stato ben esplicitato all'interno di articoli e considerando: si è mirato a creare, in materia di protezione dei dati personali, un quadro di maggiore certezza del diritto e di maggiore uniformità tra i vari paesi dell'Unione europea. Al contempo s'è cercato di venire incontro a moderne esigenze, volte a garantire una maggiore circolazione dei dati personali nel contesto dell'UE, senza con ciò privare gli interessati dell'elevato livello di tutela già raggiunto in tema materia nell'ordinamento europeo.

Il legislatore nazionale, con l'entrata in vigore del Reg. UE n. 2016/679, è corso logicamente ai ripari provvedendo a adeguare il Codice della *privacy* alle nuove disposizioni unionali, attraverso la novellazione del codice ad opera del d.lgs. n. 101/2018, contenente norme di coordinamento tra la normativa domestica e quella europea[64].

Il Codice, nella sua versione *ante* Reg. UE n. 2016/679, affrontava il principio limitazione delle finalità in maniera sostanzialmente speculare alle scelte contenute nella legge 675/1996, prevedendo, per un verso, che le finalità del trattamento fossero individuate dal titolare del trattamento, a cui spetta l'esercizio di ogni potere decisionale al riguardo, e, per altro verso, che i dati personali oggetto di trattamento fossero «raccolti e registrati per *scopi determinati, espliciti e legittimi*, ed utilizzati in altre operazioni del trattamento in termini *compatibili con tali scopi*»[65] e che fossero «(…) *non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati*»[66].

Anche nel Codice, così come nella legge 675/1996, il principio di limitazione delle finalità faceva ingresso nel dettato normativo non direttamente, ma attraverso la disciplina delle «modalità del trattamento» e dei «requisiti dei dati», contemplata all'art. 11.

I dati potevano quindi essere raccolti esclusivamente se necessari per le finalità del trattamento e dovevano essere conservati solo per il periodo di tempo a ciò indispensabile, nel rispetto di una disciplina che ha trovato le giuste conferme nel Regolamento UE n. 2016/679.

Da quanto finora illustrato emerge anche una forte connessione tra principio di limitazione delle finalità e «principio di necessità» del trattamento, previsto all'art. 3 del Codice, ora abrogato[67], ai sensi del quale «i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi[68], in modo da escluderne il trattamento quando le finalità perseguite

---

[64] Si dia lettura del d.lgs. n. 101 del 10 agosto 2018 d'adeguamento del Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003) al Regolamento UE n. 2016/679.

[65] Cfr. art. 11, co. 1, lett. *b)*, del Codice in materia di protezione dei dati personali.

[66] Cfr. art. 11, co. 1, lett. *d)*, del Codice in materia di protezione dei dati personali.

[67] Si dia lettura all'art. 3, abrogato del d.lgs. n. 196/2003, rubricato *«Principio di necessità nel trattamento dei dati»*.

[68] Il Codice della *privacy*, all'art. 4, comma 1, lettera *b)*, definiva i dati identificativi come quei *«dati personali che permettono l'identificazione diretta dell'interessato»*. Nel Reg. UE n. 679/2016, l'art.

nei singoli casi possano essere realizzate mediante, rispettivamente dati anonimi[69] o opportune modalità che permettano di essere adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati»[70].

Connesso a principio di necessità è inoltre anche quello di limitazione della conservazione dei dati, che trova ulteriore specificazione, nel Codice, all'interno di altra disposizione dell'art. 11 cit., in tema di modalità del trattamento e requisiti dei dati: si fa qui riferimento al co. 1, lett. *e)* – poi abrogata per le necessità di coordinamento con il Reg. UE 679/2016 – ove si prevedeva che di dati dovessero essere «conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati». Trascorso questo periodo, i dati dovevano essere cancellati o trasformati in forma anonima, garantendo così una sorta di diritto all'oblio dell'interessato[71].

Con l'avvento del Reg. UE 679/2016, i principi in materia di protezione dei dati personali – incluso quello di limitazione delle finalità, che riveste un'importanza centrale anche per altri principi – hanno trovato un più funzionale inquadramento all'intero del provvedimento europeo, con conseguente abrogazione, ad opera del cit. d.lgs. 101/2018, delle relative disposizioni contenute nel Codice, tra le quali gli artt. 3 e 11 cit.[72].

4, par. 1, n. 1), definisce quale «identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

69 Il Codice della *privacy*, all'art. 4, co. 1, lett. *c)*, definiva il dato anonimo come quel «dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile». Nel Reg. UE n. 679/2016 non si rinviene, invece, alcuna definizione di dato anonimo se non da una attenta disamina del *considerando* n. 26 laddove si afferma che «i principi di protezione dei dati non dovrebbero pertanto applicarsi ad informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca».

70 Secondo tale principio, dunque, il trattamento informatizzato dei dati personali doveva essere effettuato in modo tale da ridurre al minimo l'uso dei dati personali e di quelli identificativi, al fine di escluderne il trattamento quando le *finalità* perseguite nei singoli casi potessero essere raggiunte mediante, rispettivamente, dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità. In altri termini, i programmi informatici dovevano essere configurati in modo tale da preferire l'uso di dati anonimi, in luogo di quelli personali, e di quelli che non consentivano un'identificazione diretta dell'interessato, al posto dei dati identificativi (G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., pp. 115 ss.). Così, ad esempio, se il trattamento dei dati poteva essere effettuato mediante l'impiego di un codice, attraverso appositi sistemi informatici, si doveva prevedere di circoscrivere il trattamento solo ai dati codificati, senza identificazione dell'interessato. Quest'ultima poteva essere effettuata solo se divenuta necessaria.

71 *Ibidem*.

72 Sono state oggetto di abrogazione, tra le altre, sia l'art. 3, del Codice, sul «*Principio di necessità nel trattamento dei dati*», sia l'art. 11 sulle «*Modalità del trattamento e requisiti dei dati*»

2. Portata del principio

2.1. La *ratio* del principio di limitazione della finalità nel GDPR

Il principio di limitazione della finalità del trattamento, così come definito dall'art. 5, par. 1, lett. *b)*, del Reg. UE n. 2016/679, prevede dunque che i dati personali debbano essere «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*»[73].

In via generale, il principio di finalità si presenta come uno strumento di controllo della circolazione dell'informazione che lega il dato personale e il trattamento, di cui quello è oggetto, ad un determinato fine[74]. Il principio si fonda sulla natura del conflitto che accompagna il trattamento dei dati personali e sulla particolare attitudine di questo ad interferire con la sfera individuale della persona, con la conseguenza che tale interferenza è tanto più giustificata quanto il trattamento tende ad un fine che l'ordinamento ritiene meritevole di considerazione. La *ratio* di tale principio è da ricercare quindi indubbiamente nell'intento del legislatore di prevenire l'utilizzo di dati personali che possano apparire inaspettati, inappropriati o altrimenti discutibili da parte dell'interessato[75].

Rispondendo a criteri di trasparenza, prevedibilità e certezza giuridica, tale principio, uno dei più importanti dell'intero Reg. UE n. 2016/679, è stato visto dalla dottrina prevalente[76] quale fondamento di principi ulteriori in materia di *data protection*, come quello di minimizzazione, di esattezza o di limitazione della conservazione, e significativo a sua volta del principio di trasparenza[77]. Quello in esame è da intendersi quindi quale principio di portata generale che trova le sue radici nella stretta correlazione tra le ragioni che hanno giustificato la raccolta dei dati personali

[73] Si rinvia al disposto dell'art. 5, del Regolamento UE n. 2016/679 di individuazione dei principi in materia di *data protection*.

[74] P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., pp. 435 ss.

[75] Si definisce «interessato» la persona fisica identificata o identificabile cui si riferiscono i dati personali trattati. Si considera «identificabile» la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, n. 1, del Reg. UE n. 2016/679). A riguardo cfr. C. del Federico-A.R. Popoli, *Le definizioni*, cit., pp. 63 ss.; G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

[76] A riguardo si rinvia al successivo par. 2.2. *Il principio di limitazione della finalità quale fondamento di ulteriori principi in materia di data protection.* G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.; M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., pp. 206 ss.

[77] P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., pp. 441 ss.; M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., pp. 206 ss.

e l'effettivo impiego degli stessi[78]. In tal senso, le finalità perseguite dal titolare del trattamento[79] devono essere sempre determinate, esplicite e legittime.

Per quanto attiene alla determinatezza delle finalità cui è teso il trattamento dei dati, tale requisito impone al titolare di compiere necessariamente una sorta di valutazione interna d'analisi delle finalità del trattamento in questione[80]. Tale valutazione, oltre a dover essere documentata in logica *accountability*[81], dovrà essere compiuta prima che il trattamento abbia inizio[82]: non a caso il legislatore europeo, nella scrittura dell'art. 5 del Reg. UE n. 2016/679 in commento, si riferisce a dati «*raccolti*» avendo bene a mente che la raccolta rappresenta la prima azione che dà avvio al trattamento dei dati[83]. Al titolare del trattamento è richiesto peraltro un livello di dettaglio elevato nel determinare le finalità del trattamento in questione, dovendo individuarle con particolare precisione, a tutto beneficio dell'interessato che potrà in un qualsivoglia frangente avere contezza della tipologia di trattamento che possa dirsi incluso nello scopo determinato inizialmente dal titolare[84]. La finalità, pertanto, non dovrà essere ampia e generica: in presenza di più finalità sarà, ad esempio, opportuno individuarne una generale che colleghi i trattamenti analoghi in esame, così come al contempo sarà bene individuare e determinare anche ogni singola sotto-finalità specifica, definita nel rispetto del principio della c.d. *granularità*[85].

Per quanto attiene all'esplicitezza[86] delle finalità, tale concetto è strettamente connesso al principio di trasparenza[87] e si esplica nell'obbligo di informare[88] il sog-

---

[78] C. DEL FEDERICO-A. R. POPOLI, *Le definizioni*, cit., pp. 63 ss. A riguardo si rinvia al successivo par. 2.3 («*Il ruolo del titolare ed il trattamento dei dati nel rispetto del principio di limitazione della finalità*»).

[79] Si definisce titolare del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4, n. 7, del Reg. UE n. 2016/679). A riguardo, C. DEL FEDERICO-A.R. POPOLI, *Le definizioni*, cit., pp. 63 ss.; L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 321 ss.

[80] G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.; C. DEL FEDERICO-A.R. POPOLI, *Le definizioni*, cit., pp. 63 ss.; L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, cit., pp. 321 ss.

[81] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 1 ss.; G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., pp. 289 ss.

[82] GRUPPO DI LAVORO EX ART. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013.

[83] C. DEL FEDERICO-A.R. POPOLI, *Le definizioni*, cit., pp. 63 ss. A riguardo si rinvia al successivo paragrafo 2.3. *Il ruolo del titolare ed il trattamento dei dati nel rispetto del principio di limitazione della finalità.*

[84] A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 392 ss.; G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., pp. 1 ss.; C. DEL FEDERICO-A.R. POPOLI, *Le definizioni*, cit., pp. 63 ss.; L. GRECO, *L'organigramma privacy: i soggetti del trattamento*, cit., pp. 321 ss.

[85] GRUPPO DI LAVORO EX ART. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013.

[86] Appare rilevante sottolineare che, nelle diverse traduzioni nazionali, il termine «esplicito» è inteso come «comprensibile», piuttosto che semplicemente come «espresso». Si veda G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

[87] Si dia lettura del *considerando* n. 39 GDPR.

[88] A. RICCI, *I diritti dell'interessato,* cit., pp. 392 e ss. A riguardo si rinvia, *infra*, al successivo par. 2.4 (*Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'inte-*

getto interessato in merito alle finalità di trattamento e ad avvisarlo laddove dovessero insorgere finalità nuove[89]. Non è pertanto sufficiente che il titolare del trattamento determini le finalità prima dell'avvio delle attività ed altresì con un elevato grado di dettaglio, ma occorre anche che provveda a comunicarle al soggetto interessato in modo chiaro e comprensibile[90]. Resta inteso che non sempre la forma scritta è l'unica ammissibile, così come nemmeno le sole finalità esplicitate per iscritto risultano essere le sole vincolanti[91]. A fronte di finalità del trattamento solamente dichiarate, occorrerà procedere ad una attenta interpretazione delle stesse, avendo a mente il contesto della fattispecie ed il senso comune. Sarà inoltre sempre opportuna una analisi fattuale sulle reali e concrete finalità del trattamento in questione, a prescindere da quanto solo dichiarato dal titolare del trattamento[92]. Nel caso in cui il titolare ometta di specificare all'interessato le finalità, invece, sarà sempre comunque necessario ricostruirle in concreto per comprenderne il perimetro e valutare la portata di eventuali violazioni poste in essere.

Per quanto attiene invece alla legittimità delle finalità, tale concetto va inteso in senso ampio: la finalità non deve soltanto rispettare la normativa vigente in materia di *data protection*, ma qualsiasi altro settore normativo. Occorre inoltre non soltanto valutare la compatibilità con le norme europee e quelle contenute nelle leggi nazionali vigenti, ma anche con i principi costituzionali ed i provvedimenti amministrativi locali[93]. Possono essere considerati quali validi strumenti d'ausilio, i codici di condotta, i codici etici, gli accordi contrattuali e le specifiche circostanze fattuali, da utilizzarsi con la consapevolezza che il giudizio di legittimità compiuto possa cambiare nel tempo, in ragione di sviluppi tecnologici od al mutare del sentire sociale. In altri termini, come rilevato dalla dottrina predominante[94], il concetto di legittimità delle finalità pare denotare anche un criterio di accettabilità sociale, tale per cui i dati personali dovrebbero essere trattati solo per scopi che non urtino i costumi sociali predominanti e non siano in contrasto con l'ordinamento giuridico.

2.2. Il principio di limitazione della finalità quale fondamento di ulteriori principi in materia di *data protection*

Come si è già avuto modo di precisare, il principio di finalità del trattamento è uno dei principi più importanti dell'intero Reg. UE n. 2016/679 posto, a sua volta, a fondamento di altri principi base per l'attività di *data protection*, quali quello di

ressato e per l'esercizio dei diritti da parte di questi).

89 Si dia lettura del *considerando* n. 50 GDPR.

90 Gruppo di lavoro ex art. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013. A riguardo si rinvia al successivo paragrafo 2.4. *Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi.*

91 G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

92 Gruppo di lavoro ex art. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013.

93 G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss. Gruppo di lavoro ex art. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013.

94 L.A. Bygrave, *Data Protection Law: Approaching ITS Rationale, Logic and Limits*, cit., p. 61.

minimizzazione, di esattezza, di limitazione della conservazione, ed espressivo a sua volta del principio di trasparenza[95].

Anzitutto, il principio di minimizzazione dei dati può considerarsi quale diretta conseguenza del principio di finalità in esame. Esso prevede che i dati raccolti debbano essere «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»[96]. In altri termini, ben più operativi, il titolare del trattamento, una volta determinate le finalità esplicite e legittime del trattamento, potrà concretamente raccogliere dati personali che non risultino superflui, inutili o sovrabbondanti rispetto alle stesse finalità. Per tal ragione, in passato, tenendo conto della giurisprudenza elaborata nel tempo dalle Corti sovranazionali, il principio di minimizzazione dei dati è stato anche denominato quale principio di necessità, principio peraltro presente sia nella Convenzione europea sui diritti dell'uomo che nella Carta dei diritti fondamentali dell'Unione europea[97]. A conferma di ciò, peraltro, il *considerando* n. 39 ben chiarisce che il principio di minimizzazione si concretizza nel giudizio di «*non altri ragionevoli mezzi*», che vuol dire che «*i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi*»[98]. Tale principio obbliga quindi il titolare del trattamen-

[95] G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss. GRUPPO DI LAVORO EX ART. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013; C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 129; G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., pp. 107 ss.; M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., pp. 179 ss.

[96] Si dia lettura dell'art. 5, par. 1, lett. *c)* del Reg. UE n. 2016/679 di definizione del principio di minimizzazione.

[97] Si dia lettura degli artt. 8 della Convenzione europea sui diritti dell'uomo e 7 della Carta dei diritti fondamentali dell'Unione europea. A riguardo di rinvia ai parr. 1.2. (*L'embrionale formulazione del principio di limitazione delle finalità nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali)* e 1.6. *(Il principio di limitazione della finalità nella Carta dei diritti fondamentali dell'Unione europea).*

[98] Si dia lettura del *considerando* n. 39 il quale dispone che «qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o

to a due tipi di valutazioni: una prima in merito all'assenza di altri ragionevoli mezzi per raggiungere le finalità del trattamento ed una seconda, che potremmo indicare quale periodica, tesa alla valutazione sul rispetto del principio di minimizzazione al passare del tempo ed al mutare della realtà fattuale[99].

Tali riflessioni possono ben valere avuto riguardo all'ulteriore principio d'esattezza in ragione del quale i dati trattati debbono essere «*esatti e, se necessario, aggiornati*»[100]. È infatti nell'interesse tanto dell'interessato, quanto del titolare e del responsabile del trattamento, che i dati raccolti, e poi successivamente trattati, siano accurati e non rappresentino falsamente la realtà, ciò in ossequio sì al diritto a non essere falsamente rappresentati del soggetto interessato, ma altresì al raggiungimento delle finalità di trattamento perseguite dal titolare[101]. In altri termini, ben più operativi, il titolare del trattamento, una volta determinate le finalità esplicite e legittime del trattamento, dovrà poter raccogliere e trattare dati personali che risultino esatti ed aggiornati, a beneficio sì dell'interessato, ma anche delle finalità perseguite dal titolare medesimo e da questi individuate. Ecco perché il principio di esattezza è stato spesse volte analizzato criticamente in contrapposizione al principio di opacità, da leggersi quale inaccuratezza dei dati personali. L'interessato molto spesso ha l'interesse a rendere il trattamento dei propri dati personali meno preciso ed accurato al fine di proteggere l'intimità della sua vita privata, ma questa volontà, seppur celata, non può che pregiudicare il raggiungimento e, soprattutto, la chiarezza delle finalità perseguite dal titolare.

Si intuisce quindi come non vada affatto trascurata la stretta connessione che esiste tra il rispetto del principio di finalità e la necessità di stabilire (e rispettare) un periodo di conservazione dei dati quanto più possibile breve, predeterminato e, comunque, anche in questo caso, non eccedente il tempo strettamente necessario per il perseguimento della finalità del trattamento effettuato[102]. Anche questo principio è espresso chiaramente dall'art. 5, par. 1, lett. e), del Reg. UE n. 2016/679, in forza del quale l'arco di tempo in cui le informazioni possono essere conservate va sempre rapportato alle finalità specifiche del singolo trattamento[103]. In altri termini,

---

cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento».

[99] Il principio di minimizzazione è stato definito dalla Corte di Giustizia nel caso *Google Spain* quale intrinsecamente dinamico. Ciò risulta ben evidente nell'esempio dei motori di ricerca *online* laddove può accadere spesso che «i dati risultino inadeguati, non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso». A riguardo, CGUE, Grande Sezione, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sent. 13 maggio 2014; G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

[100] Si dia lettura dell'art. 5, par. 1, lett. *d)*, del Reg. UE n. 2016/679 di definizione del principio d'esattezza dei dati personali.

[101] S. Rodotà, *Dal soggetto alla persona*, Napoli, 1997, p. 588.

[102] E. Navaretta, *Comm. Sub. art. 11 del d.lgs. 30 giugno 2003, n. 196*, in C.M. Bianca-F.D. Busnelli, *La protezione dei dati personali*, cit., pp. 241 ss.; P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., pp. 452 ss.

[103] Si dia lettura dell'art. 5, par. 1, lett. *e)*, del Reg. UE n. 2016/679 il quale dispone che i dati siano «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere

una volta conseguite le finalità del trattamento in questione, i dati vanno eliminati o anonimizzati e da qui appare chiaro dunque come anche questo principio sia una diretta emanazione del principio di finalità, come peraltro ben precisato dal *considerando* n. 39, laddove si rimarca l'esistenza di un «*obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario*»[104]. Il Reg. UE 2016/679 ha comunque voluto circostanziare l'impatto di tale limitazione avuto riguardo alle finalità di ricerca o pubbliche in genere[105]. L'art. 5, par. 1, lett. *e)* chiarisce infatti che «*i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato*»[106], come ad esempio la pseudonimizzazione o la cifratura. È del tutto evidente che, nonostante tale deroga, questo principio è considerato come un probabile ostacolo alle potenzialità scientifiche e tecniche dei *Big Data*[107], di cui si dirà a seguire. A riguardo, giova altresì menzionare l'art. 11, del Reg. UE n. 2016/679[108] in ragione del quale si chiarisce che nel caso in cui «*le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento*».

Infine, il principio di limitazione della finalità risulta essere espressivo del principio di trasparenza, che rappresenta una delle maggiori novità derivanti dall'introduzione del Reg. UE n. 2016/679[109]. A fornire chiare indicazioni sul principio di

conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione")».

[104] G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

[105] Si dia lettura dell'art. 89, del Reg. UE n. 2016/679 di disciplina di «*garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*».

[106] Tale deroga era già presente all'art. 6, paragrafo 1, lettera e) della Direttiva n. 95/46/CE che demandava agli Stati membri la facoltà di regolare la materia. A riguardo, M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., pp. 206 ss.

[107] T. ZARSKY, *Incompatible: The GDPR in the Age of Big Data*, 2017, p. 2011; A. MANTELERO, *La privacy all'epoca dei Big Data*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1181 ss. A riguardo, si rinvia al par. 3.3. (*Principio di limitazione della finalità e big data*).

[108] Si dia lettura dell'art. 11, del Reg. UE n. 2016/679 di disciplina del «*trattamento che non richiede l'identificazione*».

[109] Il principio di trasparenza non era infatti enunciato tra i principi relativi alla qualità dei dati di cui all'art. 6, della Direttiva 95/46/CE. Del resto, tale principio non è neppure presente nell'art. 8, della Carta dei diritti fondamentali dell'Unione europea, che cita soltanto i principi di liceità e lealtà. Tuttavia, la dottrina è concorde nel ritenere tale principio come implicito nel concetto di correttezza e liceità. A riguardo, G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.; P. IAMICELI, *Liceità,*

trasparenza è il *considerando* n. 39. in ragione del quale tale principio «impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro»[110]. Ci si riferisce, in particolare, all'identità del titolare del trattamento ed alle finalità del trattamento stesso, oltre a tutte quelle ulteriori informazioni finalizzate ad assicurare un trattamento corretto e trasparente avuto riguardo alle persone fisiche interessate ed ai loro diritti[111]. Dalla lettura del *considerando* n. 58[112], appare chiaro dunque che il principio di trasparenza è *user-centric*, basandosi invero sulle reali esigenze conoscitive e sulla capacità di comprensione del soggetto interessato al trattamento, assicurandogli una concreta consapevolezza circa le caratteristiche del trattamento dei suoi dati personali.

2.3. Il ruolo del titolare ed il trattamento dei dati nel rispetto del principio di limitazione della finalità

La definizione di titolare del trattamento contenuta nel n. 7, dell'art. 4, del Reg. UE n. 2016/679 si basa sulla nozione di finalità[113]. È titolare colui che «*determina le finalità* ed i mezzi del trattamento di dati personali»: una esplicitazione del concetto di *accountability* su cui si regge l'intero Regolamento UE[114]. È al titolare, quindi, cui viene affidato il compito di decidere autonomamente fini, modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative ed alla luce dei principi definiti dal medesimo Regolamento. Tali funzioni possono essere svolte «singolarmente od assieme ad altri» poiché sussistono ipotesi, sempre più frequenti, in cui il trattamento di dati personali veda interagire più figure che agiscono tutte quali titolari del trattamento in questione[115].

---

correttezza, finalità nel trattamento dei dati personali, cit., pp. 395 ss. Si dia altresì lettura dell'art. 5, par. 1, lett. *a)*, del Reg. UE n. 2016/679.

[110] A riguardo si rinvia al par. 2.4 (*Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi*).

[111] *Ibidem*.

[112] Si dia lettura del *considerando* n. 58 in ragione del quale «Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente».

[113] Si dia lettura dell'art. 4, par. 1, n. 7), del Reg. UE n. 2016/679 sulla definizione della figura del titolare del trattamento.

[114] G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo*, cit., pp. 1 ss.; G. Finocchiaro, *Privacy e protezione dei dati personali*, cit., pp. 289 ss.

[115] Si parla a riguardo di contitolarità del trattamento. A riguardo, C. del Federico-A.R. Popoli, *Le definizioni*, cit., pp. 63 ss.; L. Greco, *L'organigramma privacy: i soggetti del trattamento*, cit., pp. 321 ss.; C. Giakoumopoulos-G. Buttarelli-M. O'Flaherty, *Manuale sul diritto europeo*, cit.,

Il compito di definire le caratteristiche essenziali delle attività di trattamento attribuiti al titolare, è alla base della tenuta del registro delle attività di trattamento. Si tratta di un *quid novi*, uno strumento fondamentale, da redigersi in forma scritta, anche elettronica, destinato allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'azienda o di un soggetto pubblico, indispensabile per ogni valutazione ed analisi del rischio. I contenuti del registro, che possono essere ampliati se il titolare lo riterrà opportuno, proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti, sono individuati dall'art. 30, del Reg. UE n. 2016/679. Vanno annotati nel registro, tra gli altri, il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare, dell'eventuale rappresentante e del responsabile della protezione dei dati[116]; le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali trattati; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, l'eventualità di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale e la documentazione delle garanzie adeguate, i termini ultimi previsti per la cancellazione delle diverse categorie di dati, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate[117].

Alla luce delle disposizioni sino ad ora esaminate, il titolare del trattamento dei dati personali s'atteggia a tutti gli effetti quale *controller* del trattamento stesso. Di fatto, i confini di ciascun trattamento vanno tracciati facendo riferimento ad una serie di elementi strettamente connessi fra loro, tra cui appunto le finalità perseguite, e sostanzialmente riassunti nei principi elencati nell'art. 5, del Reg. UE n. 2016/679, il quale, com'è ben noto, fa espresso riferimento alla necessità di limitare, sotto diversi aspetti volta per volta rilevanti, i dati trattati[118]. Occorrerà quindi incrociare tutti questi elementi per determinare concretamente l'utilizzo dei dati personali che il titolare andrà ad effettuare e poterlo quindi limitare realmente a quanto stretto necessario, volta per volta, per svolgere le attività di trattamento[119].

Sul titolare grava quindi *in primis* l'obbligo di dover generalmente prevedere *ex ante* le finalità per cui i dati verranno raccolti e successivamente trattati, in ragione del ben noto principio di limitazione della finalità del trattamento. Ciò non soltanto al fine permettere agli interessati di essere correttamente informati ai sensi di legge e di compiere, dunque, scelte consapevoli, ma anche e soprattutto per consentire ai titolari stessi di essere in grado di delimitare opportunamente lo scopo delle opera-

p. 114; D. FARACE, *Il titolare e il responsabile del trattamento*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 731 ss.

[116] A. AVITABILE, *Il Responsabile della Protezione dei dati,* in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 355 ss.; C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 195; C. SOLINAS, *La nuova figura del responsabile della protezione dei dati*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 879 ss.

[117] Si dia lettura dell'art. 30, del Reg. UE n. 2016/679 di disciplina del registro delle attività di trattamento. A riguardo, C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 195; G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., pp. 80 ss.

[118] G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

[119] E. NAVARETTA, *Comm. Sub. art. 11 del d.lgs. 30 giugno 2003, n. 196*, cit., pp. 241 ss.; P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., pp. 395 ss.

zioni di trattamento e di determinare, di conseguenza, sia i mezzi che le misure tecniche ed organizzative adeguate rispetto al trattamento dei dati personali in questione.

Una chiara delimitazione delle finalità del trattamento è peraltro necessaria anche per l'effettuazione di una adeguata valutazione d'impatto sulla protezione dei dati[120] e per garantire il rispetto dei principi di *privacy by design* e *privacy by default*[121]. Poiché la finalità perseguita va individuata prima di procedere alla raccolta dei dati personali per le ragioni più sopra esposte (e, qualora i dati siano raccolti presso l'interessato, comunicata a quest'ultimo non più tardi del momento in cui i dati siano ottenuti), l'analisi a cui dovrà procedere ciascun titolare, prima ancora quindi di raccogliere i dati, dovrà essere volta a determinare con precisione quali siano i dati essenziali per lo specifico trattamento che si vuole effettuare, a verificare se quel trattamento sia effettivamente necessario per il raggiungimento di quello scopo particolare ed altresì se la finalità perseguita, a sua volta, non possa essere raggiunta con altri mezzi, ragionevolmente applicabili nel contesto di riferimento. Rileva anzitutto la pertinenza del dato, quale indice oggettivo del principio di finalità riferito alla natura dell'informazione: in molti casi, è il contenuto informativo del dato a riflettere l'inerenza del trattamento ad una certa finalità o comunque sia l'esistenza di un particolare nesso tra quel contenuto e le modalità del trattamento cui il dato è sottoposto[122].

Fondamentale è altresì l'analisi della completezza e della non eccedenza dei dati poiché il principio di finalità opera anche con funzione selettiva rispetto all'ammontare delle informazioni trattate. Occorre infatti assicurarsi che il dato (o il complesso di dati) abbia un contenuto informativo sufficiente al perseguimento del fine, tale da giustificare il trattamento[123]. Parimenti, occorrerà eliminare quella parte del contenuto informativo che, nella generale dinamica del trattamento, non aggiunga nulla di più rispetto al perseguimento del fine proposto, di quanto non sia già assicurato dal trattamento dei dati che possono essere individuati quali non eccedenti e,

[120] La valutazione d'impatto sulla protezione dei dati (DPIA) è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali. L'art. 35, del Reg. UE n. 2016/679 al n. 1 precisa che «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali». La valutazione d'impatto sulla protezione dei dati deve essere effettuata dal titolare del trattamento avvalendosi, se nominato, del responsabile della protezione dei dati. Il principio di carattere generale prevede quindi l'obbligo soltanto se il trattamento è suscettibile di causare un rischio elevato evidenziando come elemento determinante l'uso di nuove tecnologie. Sicuramente una delle funzioni della DPIA è quella di permettere al titolare di realizzare e dimostrare la conformità alla complessa normativa sulla protezione dei dati personali in logica *accountability*. R. Torino, *La valutazione d'impatto* (Data Protection Impact Assessment), in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 855 ss.

[121] Si dia lettura dell'art. 25 del Reg. UE n. 2016/679, rubricato «*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*».

[122] P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., pp. 444 ss.

[123] G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, pp. 261 ss.

anzi, rischi per la sua natura di ampliare la portata del trattamento in direzioni non consentite, perché estranee allo scopo originario così come definito[124].

Compiuta questa analisi, il titolare del trattamento dovrà fare in modo, anche avvalendosi di apposite misure tecniche e organizzative, di ridurre al minimo il trattamento dei dati personali nel suo complesso. Va da sé, infine, che si tratta di una serie di analisi da compiere contestualizzando ciascun trattamento e ciascuna finalità e che dovrà necessariamente essere sottoposta a controlli e revisioni puntuali e periodiche da parte del titolare: i presupposti di liceità e correttezza del trattamento effettuato, e quindi di rispetto anche del principio di limitazione della finalità, infatti, non sono immutabili, ma, anzi, essendo fondati su diversi elementi reciprocamente connessi tra loro, sono esposti a continue modifiche che richiedono costanti verifiche[125].

2.4. Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi

Il principio di limitazione della finalità, ponendosi accanto ai principi di liceità, correttezza e trasparenza, risulta essere strettamente finalizzato a consentire la prevedibilità ed il controllo dell'interessato sui propri dati. Solo se la finalità del trattamento è sufficientemente specifica e chiara, l'interessato può conoscere quali trattamenti aspettarsi sui propri dati ed altresì esercitare i diritti riconosciutigli dal Reg. UE n. 2016/679.

Rileva quindi il disposto di cui agli artt. 13 e 14, del sopraccitato Reg. UE n. 2016/679. Fatte salve alcune eccezioni[126], chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni, ben dettagliate dalla normativa, specie per metterlo nelle giuste condizioni di esercitare i suoi poteri[127]. Qualora i dati siano raccolti presso l'interessato, l'informativa deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati. L'art. 13 precisa che al più tardi deve essere resa nel momento in cui i dati siano ottenuti (tenendo però conto di farla precedere alla corretta acquisizione del consenso, qualora sia questa la base giuridica prevista per il trattamento). Solo nel caso in cui i dati personali non siano stati raccolti direttamente presso l'interessato, l'informativa può essere fornita, *ex* art. 14, del GDPR, entro un termine ragionevole che non può superare il mese dalla raccolta, oppure al momento della comunicazione dei dati a terzi o all'interessato stesso[128].

---

[124] P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., pp. 444 ss.

[125] G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.; C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 110; P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali,* cit., pp. 444 ss.

[126] Si dia lettura dell'art. 13 e dell'art. 14 del Reg. UE n. 2016/679 di disciplina del diritto di informazione dell'interessato.

[127] Ci si riferisce ai diritti, disciplinati dal Reg. UE n. 2016/679, d'accesso (art. 15), di rettifica (art. 16), alla cancellazione ed all'oblio (art. 17), di limitazione di trattamento (art. 18), di notifica in caso di rettifica o cancellazione (art. 19), alla portabilità dei dati (art. 20), di opposizione (art. 21), d'opposizione alla profilazione (art. 22).

[128] C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 225.

I contenuti dell'informativa sono elencati in modo tassativo nei parr. 1 e 2 di entrambi gli artt. 13 e 14, del Regolamento UE. Fra essi, ai nostri fini, è individuata la finalità del trattamento che deve quindi essere definita, come più volte precisato, ben prima della raccolta dei dati personali e resa nota all'interessato. A questa, si aggiungono i dati di contatto del responsabile della protezione dei dati, ove esistente[129], la base giuridica del trattamento, con l'eventuale interesse legittimo perseguito dal titolare, la possibilità di trasferimento, le categorie dei dati personali oggetto di trattamento, l'identità del titolare, quella dell'eventuale rappresentante nel territorio italiano e del responsabile del trattamento, i diritti degli interessati ed i destinatari dei dati. Oltre a ciò, occorre specificare il periodo di conservazione dei dati o i criteri eventualmente definiti per stabilire tale periodo ed il diritto di presentare ricorso all'autorità di controllo, salvo altro.

Il fine perseguito dalle norme in esame è indubbiamente quello di tendere ad un trattamento che sia il più possibile chiaro e trasparente per l'interessato. Anche per questo, il Reg. UE n. 2016/679 richiede che l'informativa sia resa agli interessati in modo ed in forma chiara e semplice, tenendo conto altresì dell'età degli utenti in questione[130]. L'interessato non è infatti un soggetto che passivamente subisce le operazioni di trattamento sui propri dati personali, ma al contrario vanta un ampio potere di controllo e di intervento sugli stessi esercitabili, peraltro senza particolari formalità[131]. Il riconoscimento di questo potere di controllo e di conseguente intervento sui dati personali richiede quindi necessariamente che l'interessato sia informato *in primis*, ma non solo, sulle finalità del trattamento in procinto di avviarsi. Tale principio è profondamento radicato nella teoria del diritto alla *privacy* come controllo informativo (c.d. autodeterminazione informativa), che presuppone che un individuo abbia la piena autorità sulle proprie informazioni personali, esercitando, se del caso i riconosciuti diritti individuali in tema di *data protection*, solo se comprende lo scopo del trattamento di cui trattasi[132].

Resa l'informativa, il titolare dovrà poi agevolare l'eventuale successivo esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica ed organizzativa a ciò idonea, potendo contare peraltro sulla fattiva collaborazione del responsabile del trattamento. Ciò rientra nel più ampio concetto di *accountability* del titolare del trattamento, ossia nell'adozione da parte di questi, di comportamenti anche proattivi e tali da garantire e dimostrare la concreta adozione di misure finalizzate ad

[129] A. Avitabile, *Il Responsabile della Protezione dei dati*, cit., pp. 355 ss.; C. Giakoumopoulos, G. Buttarelli, M. O'Flaherty, *Manuale sul diritto europeo*, cit., p. 195; C. Solinas, *La nuova figura del responsabile della protezione dei dati*, cit., pp. 879 ss.

[130] Gruppo di lavoro ex art. 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679*, 29 novembre 2017.

[131] A. Ricci, *I diritti dell'interessato*, cit., pp. 392 ss.; F. Calisai, *I diritti dell'interessato*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 327 ss.

[132] L. Colonna, *International Data Privacy Law,* 2014, p. 304; G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.; G. Finocchiaro, *Privacy e protezione dei dati personali*, cit., pp. 78 ss.

assicurare l'applicazione del Reg. UE n. 2016/679, anche secondo i ben noti principi sintetizzati dall'espressione inglese «*data protection by default e by design*»[133].

2.5. Il principio di limitazione della finalità quale presupposto per il rilascio del consenso al trattamento

Il Regolamento UE n. 2016/679 prevede che ogni trattamento debba trovare fondamento in un'idonea base giuridica: solo in tal modo viene garantita la liceità del trattamento stesso[134]. Sono individuati quali fondamenti di tale liceità il consenso, l'adempimento degli obblighi contrattuali, gli interessi vitali della persona interessata o di terzi, gli obblighi di legge cui è soggetto il titolare, l'interesse pubblico o l'esercizio di pubblici poteri, l'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati. Particolare attenzione è chiaramente prestata dal legislatore europeo ai dati appartenenti a categorie particolari[135], il cui trattamento è in linea di principio vietato, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate dall'art. 9, par. 2, del Reg. UE n. 2016/679, fra le quali va ricordato, così come per i dati comuni, il consenso esplicito al trattamento per una o più finalità specifiche[136].

Fra le sopraelencate basi giuridiche per il trattamento dei dati personali, il consenso riveste particolare rilievo. L'art. 4, par. 1, al n. 11[137] lo definisce quale «espressione di manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, acché i dati personali che lo riguardano siano oggetto di trattamento». Una tal manifestazione di volontà[138] non può che porsi al seguito di una propedeutica e trasparente informativa. Inquadrando il

[133] Si dia lettura all'art. 25, del Reg. UE n. 2016/679 rubricato «*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*».

[134] Si dia lettura all'art. 6, del Reg. UE n. 2016/679 rubricato «*Liceità del trattamento*».

[135] Si definiscono dati particolari quelli che rivelino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, biometrici, quelli relativi alla salute o alla vita sessuale di una persona o al suo orientamento sessuale. Si definiscono dati genetici i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13, del Reg. UE n. 2016/679). Si definiscono dati biometrici i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (art. 4, n. 14, del Reg. UE n. 2016/679). Si definiscono dati relativi alla salute i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, n. 15, del Reg. UE n. 2016/679).

[136] Si dia lettura all'art. 9, del Reg. UE n. 2016/679 rubricato *«Trattamento di particolari categorie di dati personali»*. A riguardo, F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 110 ss.; C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 126.

[137] Si dia lettura dell'art. 4, par. 1, n. 11), del Reg. UE n. 2016/679 di definizione del consenso.

[138] Il consenso richiama per taluni lo schema del neoformalismo negoziale o comunque dell'agire giuridico. A riguardo, I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Rego-*

consenso quale manifestazione di natura autorizzatoria è infatti fondamentale che lo stesso sia «*informato*», ovvero che siano portate a conoscenza dell'interessato tutte le informazioni contemplate nell'artt. 13 (e 14), del Reg. UE n. 2016/679 con un criterio di completezza, funzionale all'esercizio dell'autodeterminazione informativa in cui si sostanzia il diritto alla protezione dei dati personali[139]. Oltre che informato, il consenso deve altresì dirsi libero, specifico ed inequivocabile in ragione della definizione data dal Regolamento UE[140].

Ai dovuti fini del presente contributo, ciò che rileva è il principio della c.d. *granularità* del consenso, che fa riferimento alla necessità di richiedere distinte manifestazioni di volontà dall'interessato, aventi ad oggetto l'autorizzazione al trattamento dei dati, per ciascuna finalità di trattamento perseguita. Si esprimono in tal senso le linee guida del WP 29[141]: se viene richiesto un unico consenso per diverse finalità di trattamento, tra loro accorpate, il consenso non può ritenersi libero, dato che l'interessato deve potersi esprimere liberamente sulle singole finalità di trattamento ed essere messo in grado di selezionare quali finalità autorizzare e quali eventualmente no[142]. Anche lo *European Data Protection Board* (EDPB) ha adottato in data 4 maggio 2020 la versione 1.0 delle linee guida in materia di consenso, ai sensi del Reg. UE n. 2016/679[143]. In particolare, è chiarito che «se il titolare del trattamento ha *riunito diverse finalità di trattamento* e non ha chiesto il *consenso separato per ciascuna di esse* non c'è libertà»[144]. Un servizio può infatti comportare trattamenti multipli per più finalità ed in tal caso, l'interessato deve essere libero di scegliere quale finalità accettare anziché dover acconsentire ad un insieme eterogeneo di finalità, potendo in tal modo determinarsi la situazione per la quale per l'attivazione di un servizio possano dirsi giustificati più consensi da parte dell'utente interessato.

---

lamento europeo. Analisi giuridica e studi comportamentali, in *Osservatorio del diritto civile e commerciale*, 2018, 1, pp. 67.

[139] F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 110 ss.; F. Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, n. 1, pp. 34-58; A. Ricci, *I diritti dell'interessato*, cit., pp. 392 ss. A riguardo si rinvia, *infra*, al par. 2.4. (*Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi*).

[140] È libero il consenso reso da un interessato che abbia una scelta effettiva nel manifestare la propria volontà autorizzatoria e che abbia anche il controllo sui propri dati. È specifico il consenso reso con riguardo ad elementi di trattamento individuati in maniera puntuale e non generica. È informato il consenso reso dall'interessato al quale siano state portate a conoscenza dell'interessato tutte le informazioni di cui agli artt. 13 e 14, del Reg. UE n. 2016/679. È inequivocabile il consenso reso dall'interessato mediante un atto positivo che non possa essere frainteso nel suo significato, né generare dubbi in ordine alla sua effettiva esistenza. A riguardo, F. Bravo, *Le condizioni di liceità del trattamento di dati* personali, cit., pp. 110 ss.; F. Caggia, *Libertà ed espressione del consenso*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 249 ss.

[141] Gruppo di lavoro ex Art. 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679,* del 28 novembre 2017, modificate il 10 aprile 2018 (WP 259 rev. 01).

[142] F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 110 ss.

[143] EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679,* 4 maggio 2020.

[144] *Ibidem*.

Chiarificatore in tal senso risulta essere altresì il *considerando* n. 32[145], il quale ribadisce che «il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia *più finalità,* il consenso dovrebbe essere prestato per tutte queste».

Il concetto di *granularità* è strettamente correlato alla necessità che il consenso sia *specifico* avuto riguardo per l'appunto alle diverse *finalità* perseguite con quella precisa attività di trattamento. Ciò vale a garanzia per l'interessato avverso la c.d. *function creep* che si concretizza nell'ipotesi in cui le informazioni personali raccolte siano utilizzate per scopi che non erano stati inizialmente palesati[146]. Come più volte rimarcato, ai sensi dell'art. 5, par. 1, lett. *b)*, del Reg. UE n. 2016/679, per ottenere un *consenso valido* occorre sempre prima determinare la *finalità* specifica, esplicita e legittima dell'attività di trattamento prevista[147]. La necessità di un consenso specifico, associata al principio di limitazione delle finalità, mira ad evitare l'ampliamento progressivo, o la commistione, delle finalità di trattamento dei dati dopo che l'interessato ha acconsentito alla loro raccolta iniziale. Questa eventualità rappresenta un evidente rischio per l'interessato, in quanto può comportare l'impiego non previsto di dati personali da parte del titolare del trattamento o di terzi e la conseguente perdita del controllo degli stessi dati da parte del medesimo interessato. Questi dovrà quindi sempre fornire il consenso per una specifica finalità di trattamento: il consenso potrà in astratto coprire trattamenti distinti, ma solo se gli stessi perseguano la medesima finalità. Ciò significa quindi che il titolare del trattamento, che richiede il consenso per finalità diverse, dovrà prevedere una possibilità di adesione distinta per ciascuna finalità, consentendo in tal modo all'utente di esprimere un consenso specifico per finalità altrettanto specifiche[148].

Così, ad esempio, nel contesto della medesima richiesta di consenso, un rivenditore non può chiedere ai propri clienti il consenso ad utilizzare i loro dati per inviare comunicazioni di *marketing* tramite posta elettronica relativi a beni o servizi differenti da quelli per cui è intercorsa la relazione contrattuale e per condividere i

[145] Si dia lettura del *considerando* 32 in ragione del quale «il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

[146] *Ibidem.*

[147] Cfr. il parere 3/2013 del Gruppo di lavoro *ex* Art. 29 sulla limitazione della finalità (WP 203), p. 16: «Per questi motivi, una finalità che sia vaga o generica, come ad esempio "migliorare l'esperienza degli utenti", "finalità di marketing", "finalità di sicurezza informatica" o "ricerca futura", senza ulteriori dettagli, di solito non soddisfa i criteri per essere "specifica"».

[148] EDPB, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679,* 4 maggio 2020.

dati con altre società del gruppo[149]. Tale consenso non si configurerebbe come granulare, in quanto non distinto per le due finalità perseguite dal titolare del trattamento e, pertanto, non potrà dirsi valido. In tale eventualità, risulta quindi necessario un consenso specifico all'invio dei dati di contatto degli interessati ai *partners* commerciali del titolare. Tale consenso specifico sarà ritenuto valido per ciascuno dei *partners*, la cui identità sia stata fornita all'interessato al momento dell'ottenimento del consenso, nella misura in cui i dati vengano inviati per la medesima finalità, quale quella di *marketing*[150]. Così ancora, una rete TV via cavo che ha raccolto i dati personali degli abbonati, sulla base di uno specifico consenso, per fornire loro suggerimenti personali sui nuovi *film* disponibili, in ragione delle loro abitudini di visualizzazione, non potranno inviare ai medesimi interessati pubblicità mirate: in ragione di tale nuova finalità perseguita sarà necessario acquisire dagli abbonati un nuovo consenso[151]. Così ancora, una compagnia aerea che raccoglie i dati dei passeggeri per effettuare le prenotazioni, quali il numero di posto assegnato, le eventuali limitazioni fisiche, le richieste di pasti speciali, non potrà trasmetterli alle autorità preposte al controllo delle immigrazioni all'aeroporto d'arrivo configurandosi, nel caso di specie, un utilizzo di dati per finalità differenti rispetto a quelle perseguire al momento della raccolta dei dati stessi[152].

2.6. Le cc.dd. finalità incompatibili ed il *compatibility test*

Corollario del principio di limitazione della finalità è il divieto di trattare i dati personali raccolti per *finalità secondarie*, differenti da quelle per cui i dati in questione erano stati inizialmente raccolti, con una eccezione significativa e circostanziata, come già chiarito, per la ricerca. Il divieto di finalità incompatibili, già presente nella Direttiva 95/46/CE, è ora rimesso dal legislatore europeo al titolare del trattamento, in attuazione del ben noto principio di *accountability*, su cui grava la comprova d'aver agito nel pieno rispetto del principio di finalità, sulla base di una attenta valutazione in merito alla compatibilità degli scopi ulteriori del trattamento, come richiesto dal combinato disposto degli artt. 5 e 6 del Reg. UE n. 2016/679[153].

Si parla a riguardo di *compatibility test*[154].

---

[149] Com'è noto, non occorre il consenso e si può ricorrere alla condizione di liceità del legittimo interesse, *ex* art. 6, par. 1, lett. *f)*, del Reg. UE n. 679/2016, qualora il *marketing* diretto sia posto in essere per comunicazioni di carattere commerciale rivolte dal titolare del trattamento ai propri clienti per le medesime categorie di beni o servizi già oggetto di fornitura, qualora gli interessati possano ragionevolmente aspettarsi tale trattamento, a cui non si sono opposti. Si veda, in tal senso, il *considerando* n. 47 del GDPR.

[150] *Ibidem.*

[151] *Ibidem.*

[152] C. Giakoumopoulos-G. Buttarelli-M. O'Flaherty, *Manuale sul diritto europeo*, cit., pp. 137 ss.

[153] Si dia lettura degli artt. 5 e 6, del Reg. UE n. 2016/679 di disciplina dei principi in materia di *data protection* e delle condizioni di liceità dei trattamenti di dati personali.

[154] A tal riguardo, un valido strumento di supporto è rappresentato dall'*opinion* n. 03/2013, ove viene affermato che il determinante test di compatibilità debba preferibilmente fondarsi su una valutazione sostanziale, la quale, capace di andare oltre gli aspetti meramente formalistici, si basa sulla valutazione di precisi criteri divenendo così un metodo flessibile, pragmatico e maggiormente efficace. A

La formulazione della lett. *b)*, dell'art. 5 sopraccitato risulta, anche se solo all'apparenza, ambigua e di difficile interpretazione, non risultando, ad una prima lettura, sufficientemente chiaro quando le finalità del trattamento possano dirsi compatibili con quelle sottese alla raccolta dei dati personali trattati[155]. L'ultimo periodo della lett. *b)*, dell'art. 5 deve tuttavia essere letto in combinato disposto con il successivo art. 6 ed altresì con il *considerando* n. 50[156]: i dati personali possono essere trattati per finalità ulteriori, anche incompatibili rispetto a quelle originarie, laddove l'interessato abbia prestato il proprio consenso ovvero nell'ipotesi in cui il trattamento si basi su un atto legislativo dell'Unione europea o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia, in particolare,

riguardo, GRUPPO DI LAVORO EX ART. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013. A riguardo si rinvia, *infra*, al par. 3.1. (*Granularità del consenso,* marketing *diretto,* social spam *e* marketing *virale*).

[155] A. D'OTTAVIO-G. NAVA, *GDPR, il principio di finalità: un equilibrio fra privacy ed innovazione*, 2018, su www.agendadigitale.eu.

[156] Si dia lettura del *considerando* n. 50 in ragione del quale «il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto. Ove l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale, il titolare del trattamento dovrebbe poter sottoporre i dati personali a ulteriore trattamento a prescindere dalla compatibilità delle finalità. In ogni caso, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi. L'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare del trattamento. Tuttavia, tale trasmissione nell'interesse legittimo del titolare del trattamento o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il trattamento non è compatibile con un obbligo vincolante di segretezza, di natura giuridica, professionale o di altro genere».

degli importanti obiettivi di interesse pubblico generale di cui all'art. 23, del Reg. UE n. 679/2016[157].

Qualora non si ricada in una delle due ipotesi sopraccitate, l'art. 6, del Reg. UE n. 2016/679[158] specifica anche che i dati personali possano essere trattati per finalità diverse purché compatibili rispetto a quelle per cui sono stati inizialmente raccolti, prevedendo una serie di parametri, di seguito elencati, di cui il titolare del trattamento deve necessariamente tenere conto nel corso della valutazione sulla compatibilità. Rileva anzitutto ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto: a tale scopo, l'attenzione deve concentrarsi sul rapporto sostanziale tra le due finalità (originaria ed ulteriore) di trattamento, onde così comprendere se sussiste una situazione in cui l'ulteriore trattamento fosse già implicito nella finalità iniziale ovvero assunto come una fase logica successiva del trattamento in ragione alla sua finalità originaria.

Va esaminato altresì il contesto in cui i dati personali sono stati raccolti, con particolare riguardo alle ragionevoli aspettative dell'interessato rispetto all'ulteriore utilizzo dei dati. Al fine di valutare la ragionevole aspettativa del soggetto interessato, è necessario tenere in considerazione la natura del rapporto tra l'interessato ed il relativo titolare del trattamento, lo *status* di quest'ultimo nonché la base giuridica su cui si è fondata la finalità di trattamento originaria, onde così comprendere il grado di sorpresa dell'interessato e l'eventuale squilibrio, ai danni dello stesso, nel relativo rapporto. In particolare, nel valutare il contesto in cui i dati sono stati raccolti e le ragionevoli aspettative dell'interessato in merito al loro utilizzo, deve essere prestata la dovuta attenzione anche alla trasparenza del trattamento nonché se l'ulteriore finalità sia basata su una disposizione di legge; in tal caso, la certezza del diritto e la generale prevedibilità possono suggerire che l'ulteriore utilizzo sia appropriato.

Rileva altresì la natura dei dati personali, e in particolare l'eventualità che siano trattate categorie particolari di dati personali (quali ad esempio, dati relativi alle condizioni fisiche e/o allo stato di salute), ovvero che siano trattati dati relativi a condanne penali e/o reati e le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati. Questo fattore esprime quello che è un approccio comune, giacché la normativa in materia di *data protection* è stata progettata ed è volta a proteggere le persone fisiche contro l'impatto da un uso improprio ovvero eccessivo dei dati personali: in merito, viene, dunque, ricordato che più sensibili sono le informazioni coinvolte, più ristretto è, di conseguenza, l'ambito di un utilizzo compatibile[159].

---

[157] Si dia lettura dell'art. 23, del Reg. UE n. 679/2016 di disciplina delle limitazioni all'applicazione di talune norme contenute nel Regolamento.

[158] Si dia lettura dell'art. 6, del Reg. UE n. 679/2016 ed in particolare dal par. 4 di disciplina delle condizioni li liceità del trattamento dei dati personali.

[159] Si dia lettura del *considerando* n. 75 secondo il quale «i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano

Infine, l'esistenza di garanze e/o di misure tecniche ed organizzative adeguate, come la cifratura o la pseudonimizzazione dei dati personali trattati, concorre a determinare un trattamento corretto e a prevenire un qualsiasi indebito impatto per il soggetto interessato. In merito, nell'opinion n. 03/2013, il WP 29 precisa che «la sussistenza di adeguate misure aggiuntive possono essere idonee, in linea di principio, a compensare l'ulteriore finalità di trattamento ovvero il fatto che essa non sia stata chiaramente specificata all'inizio, così come *ex lege* richiesto: queste possono consistere in misure di sicurezza tecniche e/o organizzative colte a garantire la separazione funzionale (ad es. anonimizzazione, pseudonimizzazione, aggregazione) ovvero a concedere un vantaggio al soggetto interessato (ad es. maggiore trasparenza, agevolare l'esercizio del diritto di opposizione e/o di revoca del consenso)»[160].

In ragione dell'indagine compiuta, il WP 29 ha evidenziato che, in via potenziale, possono sussistere *tre differenti scenari*: (i) la *compatibilità* è la prima ipotesi *ovvia*. Un ulteriore trattamento può essere ritenuto compatibile, quando i dati sono trattati per raggiungere, in un modo consueto, le finalità specificate al momento della raccolta; (ii) quando la *compatibilità non è ovvia* si necessita di un'ulteriore analisi, che riguarda l'ipotesi in cui potrebbe esserci una connessione tra lo scopo specificato ed il modo in cui i dati vengono successivamente elaborati. Sussiste correlazione, ma gli scopi non sono completamente corrispondenti; (iii) infine, quando l'*incompatibilità* è *ovvia*, lo è poiché i dati vengono elaborati in un modo o per *scopi aggiuntivi* che una persona ragionevole riterrebbe inaspettato, inappropriato o altrimenti discutibile, e il trattamento non soddisfa senz'altro, le aspettative dell'interessato.

Solo nella prima ipotesi non può dirsi richiesta una base giuridica *ad hoc*, diversa ed ulteriore rispetto a quella legittima che ha consentito la raccolta dei dati. Ciò nonostante, il titolare dovrà in ogni caso fornire sempre una informativa su tale nuovo trattamento all'interessato, sia nel caso in cui i dati siano stati raccolti direttamente presso di lui[161], sia laddove i dati siano invece stati raccolti presso terzi[162].

---

l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati».

[160] In alcuni casi, la richiesta di uno specifico consenso separato, in ragione del principio di granularità del consenso, per il nuovo trattamento può aiutare a compensare il cambio di finalità.

[161] Si dia lettura dell'art. 13, del Reg. UE n. 679/2016 di disciplina dell'informativa da rendersi all'interessato a fronte del trattamento da eseguirsi su dati personali raccolti presso l'interessato stesso. A. RICCI, *I diritti dell'interessato*, cit., pp. 392 ss. A riguardo si rinvia al paragrafo 2.4. (*Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi*).

[162] Si dia lettura dell'art. 14, del Reg. UE n. 679/2016 di disciplina dell'informativa da rendersi all'interessato a fronte del trattamento da eseguirsi su dati personali raccolti presso terzi. A. RICCI, *I diritti dell'interessato*, pp. 392 ss. A riguardo si rinvia al paragrafo 2.4. (*Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi*).

In conclusione, può ben dirsi che il Reg. UE n. 2016/679 apre alla possibilità di ampliare le finalità iniziali del trattamento rimettendo al titolare ed a lui soltanto la valutazione in merito alla loro non incompatibilità delle stesse, rientrando nella sua *accountability* l'esser in grado o meno di dimostrare che il trattamento sia in ogni caso avvenuto nel pieno rispetto della normativa applicabile in materia di protezione dei dati personali[163].

3. Applicazione del principio nella casistica

3.1. Granularità del consenso, *marketing* diretto, *social spam* e *marketing* virale

Nella casistica posta innanzi all'autorità di controllo, il principio di limitazione delle finalità trova applicazione frequente. Tra i casi più significativi si riscontrano quelli in tema di *marketing* diretto, su cui si rende opportuno formare l'attenzione.

La Raccomandazione del Consiglio d'Europa N.R. (85) 20[164] definisce *marketing* diretto il «complesso delle attività e dei servizi ausiliari a quelli che permettono di offrire prodotti e servizi, di trasmettere una serie di messaggi pubblicitari a segmenti di popolazione per mezzo della posta, del telefono o di altri mezzi, diretti a fornire informazione o al fine di sollecitare una reazione da parte della persona interessata». Rientrano in tale nozione, le ricerche di mercato, l'invio di messaggi pubblicitari, l'offerta commerciale e la vendita diretta a prescindere dalle modalità e dagli strumenti utilizzati.

Tale attività ha suscitato l'interesse del legislatore europeo che, nel Reg. UE n. 2016/679, ha volutamente inserito all'art. 21 il diritto di opposizione al trattamento di dati personali effettuato per finalità di *marketing* diretto, che può essere esercitato dall'interessato in un qualsiasi momento e senza la necessità di motivarne le ragioni[165].

Parimenti, il legislatore italiano, nel dare attuazione alla Direttiva 2002/58/CE[166] ha introdotto nel Codice in materia di protezione dei dati personali l'art. 130, mantenuto in essere nonostante il *restyling* compiuto con d.lgs. n. 101/2018, rubricato «*comunicazioni indesiderate*»[167]. Tale norma detta regole differenti a seconda dei metodi impiegati per l'attività di *marketing*. In particolare, viene richiesto il consen-

[163] A. D'Ottavio-G. Nava, *Gdpr, il principio di finalità: un equilibrio fra privacy ed innovazione*, cit.; G. Finocchiaro, *Privacy e protezione dei dati personali*, cit., pp. 289 ss.

[164] Raccomandazione del Consiglio d'Europa N.R. (85) 20, relativa alla protezione dei dati a carattere personale utilizzati al fine di *direct marketing*, adottata dal Comitato dei Ministri il 25 ottobre 1985.

[165] Si dia lettura dell'art. 21, del Reg. UE n. 2016/679 di disciplina del diritto di opposizione al trattamento.

[166] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita provata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). Tale Direttiva è stata successivamente modificata dalla Direttiva 2009/136/CE.

[167] Si dia lettura dell'art. 130, del Codice della privacy di disciplina delle cc.dd. comunicazioni indesiderate.

so dell'interessato (c.d. *opt-in*)[168] per l'uso dei sistemi automatizzati di chiamata o di comunicazioni di chiamata senza l'intervento di un operatore, per le comunicazioni elettroniche, per le comunicazioni effettuate mediante posta elettronica, *telefax*, messaggi del tipo MMS (*multimedia messaging service*) o SMS (*short messaging service*) o di altro tipo, per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazioni commerciali. Se tuttavia il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e sempre che l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni (c.d. *soft spam*). È comunque vietato in ogni caso l'invio di comunicazioni a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato può esercitare i diritti riconosciutigli dalla legge[169]. Ciò è del resto compatibile con le innovazioni apportate dal Reg. UE n. 679/2016, nella parte in cui si trova precisato che il trattamento per *marketing* diretto possa eventualmente rientrare, nei limiti evidenziati dal *considerando* n. 47, tra i trattamenti per i quali non sia richiesto il consenso al trattamento, ma sulla base del legittimo interesse di cui all'art. 6, par. 1, lett. *f)*, del GDPR, nel rispetto ovviamente del principio di limitazione delle finalità.

In più occasioni il Garante per la protezione dei dati personali ha avuto modo di analizzare i trattamenti dei dati personali svolti per finalità di *marketing* diretto, rimarcando che «la manifestazione del consenso da parte del soggetto interessato costituisce uno dei principi cardine del trattamento dei dati personali nel settore privato». Tra i numerosi provvedimenti adottati dal Garante, particolare rilievo assumono le linee guida in materia di attività promozionale e di contrasto allo *spam*, adottate nel luglio 2013[170]. In quell'occasione l'autorità ha evidenziato come il requisito del consenso debba intendersi in termini selettivi, ovvero nel senso della necessità di un consenso specifico per ogni finalità perseguita dal titolare del trattamento, distinguendo espressamente, ad esempio, tra profilazione[171] e *marketing*[172]. La regola è peraltro di stringente interpretazione, con la conseguenza che, senza il consenso

[168] Il regime "*opt-in*" che, ai fini della legittimità del trattamento, richiede il preventivo consenso dell'interessato, si contrappone al regime "*opt-out*", su cui si basa il diritto di opposizione, che consente di iniziare liberamente il trattamento, riconoscendo all'interessato il diritto di interromperlo successivamente.

[169] A. RICCI, *I diritti dell'interessato*, cit., pp. 392 ss.

[170] GPDP, linee guida in materia di attività promozionale e contrasto allo *spam*, 4 luglio 2013, pubblicate sulla Gazzetta Ufficiale n. 174 del 26 luglio 2013, doc. web. n. 2542348, www.gpdp.it.

[171] Per profilazione si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4, par. 1, n. 4, del Reg. UE n. 2016/679).

[172] GPDP, *Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto"*, 15 maggio 2013, doc. web. n. 2543820, www.gpdp.it.

preventivo dell'interessato non è possibile inviare comunicazioni promozionali con strumenti automatizzati neppure nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti *web*, atti o documenti conosciuti o conoscibili da chiunque[173]. Come evidenziato in diverse occasioni dallo stesso Garante, la circostanza che le numerazioni telefoniche o gli indirizzi di posta elettronica utilizzati siano conoscibili da una pluralità di soggetti in quanto presenti in *Internet*, non implica che le stesse informazioni possano essere legittimamente trattate per qualsivoglia finalità da parte di terzi: l'eventuale disponibilità in *Internet* di indirizzi di posta elettronica, anche se resi conoscibili dagli interessati per certi scopi (ad esempio su un sito istituzionale o anche aziendale) attraverso siti *web* o altri strumenti, va «*rapportata alle finalità per cui essi sono pubblicati sulla rete*»[174]. Questi interessati, in ragione del ben noto principio della finalità del trattamento, debbono infatti essere messi nella condizione di conoscere tali finalità per poter esprimere il proprio specifico consenso al trattamento dei propri dati per il caso di specie. Per gli stessi motivi, senza il consenso preventivo, rese note le precise finalità perseguite, non è lecito utilizzare, ai fini dell'invio di *e-mail* promozionali, gli indirizzi di posta elettronica certificata contenuti nell'indice nazionale degli indirizzi P.E.C. delle imprese e dei professionisti[175]. È invece possibile e consentito contattare telefonicamente mediante operatore, al fine di richiedere il consenso a ricevere comunicazioni promozionali, i numeri presenti in elenchi telefonici e non iscritti nel registro pubblico delle opposizioni[176].

In tutti i casi, come ribadisce il Garante, il consenso dell'interessato a cui sono state palesate le finalità di *marketing* diretto, che, si badi bene, possono coesistere con finalità ulteriori e differenti, in ragione del ben noto concetto della granularità, deve essere libero, informato, specifico, nonché documentato per iscritto. In particolare, il consenso per l'attività promozionale, precisa il Garante, può dirsi libero quando non è preimpostato e non risulta, anche solo implicitamente in via di fatto, obbligatorio per poter fruire del prodotto o del servizio fornito dal titolare del trattamento[177]. In tale ipotesi, il consenso per quella specifica finalità non potrà certo dirsi libero.

Il principio di limitazione della finalità, unitamente al concetto di granularità del consenso, rileva altresì avuto riguardo al c.d. *social spam* che consiste in un insieme di attività attraverso cui lo *spammer* veicola messaggi promozionali, utilizzando i dati personali degli utenti iscritti ai *social network* o ad altri servizi. Elevato è, in tali ipotesi, il rischio di compromissione della libertà dell'utente nella scelta e nella fruizione dei servizi della società dell'informazione o, in altri termini, la libertà

[173] GPDP, Provv. dell'11 febbraio 2001, doc. *web* n. 480823; Provv. del 5 dicembre 2003, doc. *web* n. 1053809; Provv. del 15 gennaio 2004, doc. *web* n. 1086456; Provv. del 12 gennaio 2017, doc. *web* n. 5986406.

[174] GPDP, Newsletter n. 158 del 20 febbraio 2003.

[175] Ci si riferisce all'indice istituito con il d.l. 18 ottobre 2012, n. 179 convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, che ha introdotto l'art. 6-*bis* del d.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione digitale).

[176] Il registro è stato istituito con il d.l. 25 settembre 2009, n. 135, convertito con modificazioni dalla l. 20 novembre 2009, n. 166.

[177] GPDP, Provv. del 15 luglio 2010, doc. *web* n. 1741998; Provv. del 22 febbraio 2007, doc. *web* n. 1388590; Provv. del 3 novembre 2005, doc. *web* n. 1195215.

dell'utente di rendere il consenso al trattamento dei propri dati in ragione di precise finalità. Ecco perché, nell'ipotesi in cui l'utente riceve in privato, sulla bacheca o tramite e-mail inviata all'indirizzo di posta elettronica collegato al proprio profilo *social*, un messaggio promozionale da un'impresa che abbia tratto i suoi dati personali dal profilo al quale l'interessato è iscritto, il trattamento dei dati è da ritenersi illecito, salvo che lo spammer non dimostri di aver acquisito un consenso preventivo, specifico, libero e documentato avuto riguardo alla perseguita finalità di *social spam*[178]. Infatti, il consenso reso dall'utente *social*, in occasione dell'iscrizione al *network*, non potrà in alcun modo dirsi riferito a finalità ulteriori di *marketing*, perseguite peraltro da titolari differenti, essendo unicamente stato rilasciato avuto riguardo al trattamento dei propri dati personali finalizzato all'iscrizione alla piattaforma. L'ulteriore finalità di marketing diretto dovrà costituire oggetto di un ulteriore consenso specifico, secondo il ben noto concetto della granularità.

Particolarmente simile alla finalità di *marketing* diretto è quella di *marketing* virale, una modalità di attività promozionale mediante la quale un soggetto promotore sfrutta la capacità comunicativa di pochi soggetti, destinatari diretti delle comunicazioni promozionali, per trasmettere il messaggio ad un numero elevato di soggetti finali, incentivati in tal senso dal titolare del trattamento. In tal caso, il trattamento dei dati personali posto in essere per tale finalità dovrà reggersi sul consenso nel momento in cui i dati di contatto dei destinatari sono stati reperiti in elenchi pubblici o dal *web*; consenso che non sarà necessario nell'ipotesi in cui il passaparola sia stato effettuato a titolo personale ad amici e/o conoscenti[179]. Come più sopra ribadito, il fatto che l'interessato abbia reso pubblico il proprio indirizzo in una pagina *web* o in un *newsgroup*[180], non significa, in ragione del principio di finalità qui in esame, che esso sia utilizzabile per scopi diversi da quelli per i quali è stato pubblicato. La circostanza che l'indirizzo *e-mail* sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti non lo rende, infatti, liberamente utilizzabile e non autorizza comunque l'invio di informazioni, di qualunque genere, anche se non specificamente a carattere commerciale o promozionale, senza un preventivo consenso legato a quella specifica finalità o senza altra specifica base giuridica del trattamento, anche diversa dal consenso.

3.2. Il principio di limitazione della finalità nella giurisprudenza della Corte europea dei diritti dell'uomo

Come più volte rimarcato, la finalità perseguita dal titolare del trattamento deve essere ben nota ed esplicitata all'interessato nell'informativa di cui si è ampiamente trattato[181]. Il principio di limitazione della finalità, se ben conosciuta, consente

[178] A. RICCI, *I diritti dell'interessato*, cit., pp. 392 ss.

[179] *Ibidem.*

[180] Un *newsgroup* è uno degli spazi virtuali creato su una rete di *server* interconnessi per discutere di un argomento (*topic*) ben determinato. In italiano, a volte viene utilizzata l'espressione «gruppo di discussione» o *forum*.

[181] A riguardo si rinvia, *infra*, al par. 2.4. (*Il principio di limitazione della finalità quale presupposto per il rilascio dell'informativa all'interessato e per l'esercizio dei diritti da parte di questi*).

all'interessato di porre precisi limiti all'utilizzo dei dati personali da parte del titolare, così che il soggetto possa prevedere e valutare il pericolo di fornire una determinata informazione o di consentirne il trattamento[182].

Proprio per tale ragione, la dottrina[183] relaziona strettamente il principio della limitazione della finalità del trattamento al diritto fondamentale alla vita privata e famigliare. Tale nozione, elaborata dalla giurisprudenza della Corte di Strasburgo, risulta particolarmente ampia, tanto da comprende l'integrità fisica e morale della persona e numerosi aspetti dell'identità dell'individuo, tra i quali il nome e gli elementi che si riferiscono al diritto all'immagine, includendo i coniugi, nonché i figli legittimi, dal momento della loro nascita ed a prescindere dal requisito della coabitazione, così come i figli naturali[184]. In ragione di ciò, un individuo può quindi legittimamente aspettarsi che non vengano pubblicate informazioni personali senza il suo consenso[185], così come la pubblicazione di una foto, può ben invadere la vita privata di una persona anche se si tratta di una persona pubblica[186].

Con la sentenza *Peck c. United Kingdom*[187], ad esempio, la Corte europea dei diritti dell'uomo si è pronunciata sulla compatibilità del diritto alla *privacy*, così come disciplinato dall'art. 8 della Convenzione europea dei diritti dell'uomo, di una fattispecie avente ad oggetto il trattamento consistente in raccolta, conservazione ed ulteriore utilizzo di dati personali acquisiti a fini di *police intelligence*. In quell'occasione, la Corte ha avuto modo di precisare che il concetto di vita privata è particolarmente ampio e non suscettibile di una definizione esaustiva, ritenendo quindi che la videosorveglianza di luoghi pubblici, nell'ipotesi in cui i dati visivi siano registrati, conservati e successivamente resi pubblici, rientri nell'ambito d'applicazione dell'art. 8 della Carta europea dei diritti dell'uomo. In particolare, la Corte ha ritenuto che la trasmissione ai *media*, a fini di diffusione, di sequenze video del tentativo di suicidio del ricorrente, ripreso dalle telecamere di sorveglianza, costituisse una grave ingerenza nella vita privata del ricorrente stesso, nonostante il fatto che egli si trovasse in quel momento in un luogo pubblico. La conservazione di quei dati, peraltro, non si era dimostrata assolutamente necessaria ai fini, ad esempio, di una indagine particolare di polizia. Per quel caso di specie, la Corte ha concluso, all'unanimità riconoscendo una violazione dell'art. 8 della Carta europea ed un dovuto risarcimento alla parte lesa. I dati raccolti nel caso di specie lo erano per finalità di sicurezza e ad esse, in ragione del ben noto principio di limitazione della finalità, dovevano essere necessariamente circoscritte le operazioni di trattamento a tutto vantaggio dell'interessato e del suo diritto alla protezione dei dati personali, ma anche della sua vita privata e famigliare[188].

---

[182] A riguardo si rinvia, *infra*, al par. 2.5. (*Il principio di limitazione della finalità quale presupposto per il rilascio del consenso al trattamento*).

[183] G. Malgeri, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss.

[184] CEDU, quinta sezione, *Case of Henry Kismoun v. France*, 5 dicembre 2013.

[185] CEDU, grande camera, *Case of Von Hannover v. Germany*, 7 febbraio 2012.

[186] *Ibidem.*

[187] CEDU, quarta sezione, *Case of Peck v. The United Kingdom*, 28 aprile 2003.

[188] CEDU, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo, diritto al rispetto della vita privata e famigliare, del domicilio e della corrispondenza*, 31 agosto 2019, www.echr.coe.int.

3.3. Principio di limitazione della finalità e *big data*

Giusto corollario del principio di limitazione della finalità del trattamento è il divieto di trattare i dati personali per finalità cc.dd. secondarie, diverse quindi da quelle per le quali i dati personali erano stati raccolti. Tale divieto appare particolarmente problematico nel mondo dei *big data*, laddove il grande potenziale predittivo – ed i relativi possibili usi – dei dati personali non è ancora noto al momento della raccolta[189]. Questo è un tema che impone una dovuta riflessione. Se infatti è vero che l'utilizzo di una simile quantità di informazioni potrebbe portare grandi benefici agli individui ed alla società nel suo complesso, altrettanto vero è che questa ulteriore attività di trattamento debba necessariamente costituire oggetto di una attenta analisi preliminare in merito alla compatibilità delle finalità ulteriori del trattamento, rispetto alle finalità per i cui i dati personali sono stati inizialmente raccolti e/o resi pubblici[190].

Fino ad oggi il metodo tradizionale di studiare ed utilizzare i dati ha ricalcato il metodo scientifico tradizionale: viene formulata un'ipotesi, elaborata una teoria e successivamente collezionati, analizzati e messi in correlazione i dati a riprova o a smentita di quanto ipotizzato. Ora invece si sta assistendo ad un mutamento di paradigma, nel quale lo studio e l'utilizzo dei dati segue il percorso contrario: si inizia dall'analisi dell'enorme quantità di informazioni disponibili alla ricerca di collegamento e/o correlazioni, sia tramite l'analisi manuale, ma sempre più attraverso algoritmi e/o procedimenti automatizzati, con implicazioni scientifiche, etiche, politiche e legali che, seppur estremamente importanti, ricadono ben al di fuori di quanto consentito dall'art. 5, par. 1, lett. *b)*, del Reg. UE n. 2016/679.

Questo attuale metodo d'indagine risulta infatti completamente e radicalmente incompatibile con il principio di limitazione della finalità. Al momento della raccolta originaria dei dati, infatti, sarà possibile informare il soggetto solo sulle finalità perseguite in quel momento, con quel trattamento, ma non per quelle ulteriori rese possibile dalla disponibilità dell'ingente mole di dati raccolta. Rimane impossibile identificare, in questa prima fase, come un *software* (ad esempio, di intelligenza artificiale) interagirà con quelle informazioni e con quali conseguenze. L'utilizzo di nuovi algoritmi può portare – e di fatto questo è lo scopo delle nuove tecniche di *big data analytics* – alla scoperta di correlazioni inaspettate e quindi all'utilizzo dei dati per scopi anche diversi da quelli originariamente stabiliti.

Il problema si è posto *in primis* nel riutilizzo (c.d. *secondary use*) delle informazioni per la ricerca medica, ma oggi si possono trovare esempi applicati ad ogni settore commerciale, come per esempio il calcolo della solvibilità di un mutuatario o del premio assicurativo, basati solamente su dati raccolti per altre finalità, come avviene nel caso di analisi della banale navigazione *online* o delle più complesse attività di interazione con gli "assistenti vocali" o, ancora, con il monitoraggio capillare dei comportamenti resi possibili da dispositivi mobili, dispositivi *wearable* o tecnologie IoT.

---

[189] C. GIAKOUMOPOULOS-G. BUTTARELLI-M. O'FLAHERTY, *Manuale sul diritto europeo*, cit., p. 389.

[190] A. MANTELERO, *La privacy all'epoca dei Big Data*, cit., pp. 1181 ss.; M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., pp. 206 ss.

Il WP 29 nell'*Opinion* n. 03/2013 relativa alla limitazione di finalità[191], seppur antecedente al Reg. UE n. 2016/679, analizza due scenari possibili. Nel primo, il titolare del trattamento riutilizza i dati raccolti per ricavarne tendenze e correlazioni generiche. In questo caso, vi è solo la necessità di garantire, oltre la sicurezza e accuratezza dei dati, una *separazione funzionale*, ossia che le informazioni utilizzate per statistica non abbiano ricadute sui soggetti. Il secondo caso invece è quello che sta vedendo il maggiore sviluppo grazie ai *big data,* che si realizza quando «una organizzazione vuole specificatamente analizzare o prevedere le preferenze personali, i comportamenti e le abitudini di clienti individuali». Due casi esemplari sono l'adattamento del prezzo di un servizio o prodotto in base al sistema operativo utilizzato per la navigazione sul sito *internet* di una società commerciale fornitrice (ove ad esempio venisse rilevato quale sia il sistema operativo utilizzato degli utenti, al fine di applicare una politica di *pricing* più conveniente solamente per chi utilizza un dato sistema operativo, a discapito di altri utenti che ricorrono a sistemi operativi differenti) o il calcolo del rischio creditizio in base ai contenuti condivisi sui *social network.* Per queste situazioni, sempre più all'ordine del giorno, è richiesto il consenso informato (*opt-in*) del soggetto cui i dati si riferiscono, che deve essere acquisito, secondo i principi del GDPR, dopo che siano state illustrate adeguatamente le finalità specifiche e determinate del trattamento.

Alla luce di quanto visto finora, non è errato assumere che l'applicazione pratica, volta a valorizzare i big data nei trattamenti dei dati personali, muove in direzione totalmente opposta rispetto a quella perseguita dal legislatore europeo con il Reg. UE n. 2016/679 e con il principio di limitazione della finalità di cui all'art. 5, par. 1, lett. *b)*, ivi contemplato. Molteplici sono state, invero, le critiche mosse in dottrina a tale principio[192], soprattutto per quanto attiene alla sua efficacia rispetto alle esigenze della prassi e dell'economia[193]. Per questi motivi, si è spesso proposto di spostare l'attenzione dalle finalità agli interessi delle parti: solo una valutazione di legittimità sui secondi e non sulle prime garantirebbero una adeguata tutela ai soggetti interessati del trattamento[194].

Giova poi rimarcare, come prima illustrato, che, per ovviare alle critiche in merito alla mancanza di efficacia del principio di limitazione della finalità o ai rischi di limitare lo sviluppo scientifico e tecnologico, l'art. 6, del Reg. UE n. 2016/679[195] permette gli "usi secondari" dei dati, nella misura in cui questi siano compatibili con le finalità iniziali, in relazione ad una serie di indici quali il nesso tra la finalità

[191] Gruppo di lavoro ex art. 29, *Parere 03/2013 sulla limitazione della finalità*, 2 aprile 2013.

[192] H.T. Tavani, *Informational privacy, data mining, and the internet*, Londra, 1999, p. 197; L. Colonna, *International Data Privacy Law*, Oxford, 2014, p. 304.

[193] T. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, cit., p. 1005.

[194] L. Moerel-C. Prins, *Privacy for* the homo digitalis*: proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things*, Tilburg, 2016, p. 12.

[195] Si dia lettura dell'art. 6, del Reg. UE n. 2016/679 di disciplina delle condizioni di liceità del trattamento.

iniziale e quella secondaria, il contesto, la natura dei dati, le possibili conseguenze di usi secondati e eventuali garanzie adeguatamente prestate[196].

3.4. Covid-19 *pandemic*. Limitazione della finalità ed *app* per il tracciamento dei contatti

Tra le innumerevoli sfide che hanno interessato il quadro giuridico dell'Unione europea in ragione della pandemia da Covid-19, una delle più significative è senza dubbio quella che riguarda la *data protection*[197]. In particolare, la dottrina si è interrogata più volte su quali siano le condizioni ricavabili dal Reg. UE n. 2016/679 per le applicazioni nazionali di tracciamento dei contatti che ha mostrato un indubbio valore aggiunto nell'ottica del contenimento dei contagi[198].

Tra gli Stati dell'Unione europea che hanno deciso di avvalersi di simili applicazioni è possibile citare anzitutto l'Italia, sul cui territorio nazionale, dallo scorso 15 giugno 2020, è stata attivata l'app *Immuni*[199]. Trattasi di una *app* su base volontaria che associa ad ogni dispositivo un codice casuale, consentendone lo scambio quando si verifica un contatto fra utenti. Quando uno di questi dovesse risultare positivo al Covid-19, quest'ultimo potrà mettere a disposizione le informazioni circa i suoi recenti incontri così da poter avvertire chi ha avuto un contatto a rischio con la persona infetta, indicandogli altresì la procedura da seguire[200].

In primis, occorre precisare che il quadro normativo esistente non osta alla predisposizione di simili applicazioni. Ciò è confermato sia dal dato testuale del Reg. UE n. 2016/679 sia dai recenti pronunciamenti del Comitato europeo per la protezione dei dati che, sin dal mese di marzo 2020, si è espresso in più di una occasione sulle problematiche relative al trattamento dei dati personali nell'attuale contesto emergenziale[201].

Avuto riguardo all'*app Immuni*, per giustificare il trattamento dei dati in ragione della necessità di tracciare i contatti di soggetti positivi al *coronavirus*, la disposizione invocata è quella contenuta nell'art. 9, par. 2, lett. *i)*, del Reg. UE. Tale disposizione riguarda l'ipotesi della necessità del trattamento per motivi di interesse

---

[196] G. MALGERI, *Comm. sub. art. 5 GDPR*, cit., pp. 183 ss. A riguardo si rinvia, *infra*, al par. 2.6. *(Le cc.dd. finalità incompatibili e il* compatibility test*).*

[197] G. RUGANI, *Le condizioni ricavabili dal Regolamento generale sulla protezione per le applicazioni nazionali di tracciamento dei contatti: alcune considerazioni*, in *European Papers*, 1, 2020, pp. 633 ss.

[198] D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, in *Persona e Mercato*, 2020, 2, pp. 65-76; D. POLETTI, *"Contact tracing" e "app" Immuni: atto secondo*, in *Persona e Mercato*, 2021, 1, pp. 92-101; F. PIZZETTI, *Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti*, in *Rivista di diritto dei media*, 2020, 2, pp. 11-33.

[199] www.immuni.italia.it.

[200] A riguardo, GOVERNO ITALIANO, PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Al via Immuni, l'app per il contact tracing*, 2020, www.governo.it.

[201] EDPB, *Satement of 19 March 2020 on the processing of personal data in the context of the COVID-19 outbreak*; *Guidelines 04/2020 of 21 April 2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,* www.edpb.europa.eu.

pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero[202].

Il trattamento dei dati deve poi rispettare numerosi, importanti principi, e fra questi il ben noto principio di limitazione della finalità, secondo cui, come ampiamente chiarito, i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tale finalità». In ossequio a tale principio, le finalità devono essere sufficientemente specifiche così da escludere trattamenti ulteriori per scopi non correlati alla gestione della crisi sanitaria in essere: ad esempio, trattamenti per fini commerciali o per le attività di contrasto di matrice giudiziaria o di polizia[203]. È dunque necessario ed essenziale definire con chiarezza la finalità del trattamento, e successivamente, garantire che l'uso dei dati personali sia necessario e proporzionato rispetto alla stessa. A riguardo, il d.l. 30 aprile 2020, n. 28[204] ha disposto che «gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli artt. 13 e 14 del Regolamento UE n. 2016/679, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati», ribadendo poi che «i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento UE n. 2016/679 possano essere esercitati anche con modalità semplificate».

In conclusione, può quindi dirsi che il Reg. UE n. 2016/679, operando un bilanciamento tra le esigenze di interesse pubblico nel settore della sanità e quelle di protezione dei dati, secondo un criterio di gradualità[205] e tramite il ricorso costante al principio di limitazione delle finalità, si è mostrato uno strumento sensibile alle moderne ed emergenziali esigenze, permettendo agli Stati membri di avvalersi di tali applicazioni, seppur imponendo svariate condizioni di utilizzo e funzionalità al fine di proteggere i dati personali degli utenti[206].

---

[202] www.immuni.italia.it, *Informativa Privacy*, par. 3.

[203] G. Rugani, *Le condizioni ricavabili dal Regolamento generale sulla protezione per le applicazioni nazionali di tracciamento dei contatti: alcune considerazioni*, cit., pp. 633 ss.

[204] Si dia lettura del d.l. 30 aprile 2020, n. 28 recante «*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché' disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*», pubblicato sulla G.U. n. 111 del 30 aprile 2020 ed entrato in vigore in data 1° maggio 2020.

[205] O. Pollicino-F. Resta, *Data tracing, no a deleghe in bianco all'algoritmo*, in *CorCom*, 24 marzo 2020, www.corrierecomunicazioni.it.

[206] E.M. Kuskonmaz-E. Guild, *A New Struggle over Privacy, Data Protection and Human Rights?*, in *European Law Blog*, 4 marzo 2020, www.europeanlawblog.eu.

Capitolo VI
Il principio di minimizzazione dei dati

*Silvia Giulia Battistini - Lucrezia Matarazzo - Lara Zanetti**

SOMMARIO: 1. Inquadramento normativo. – 1.1. L'enunciazione del principio di minimizzazione dei dati nel GDPR. – 1.2. Minimizzazione e "qualità dei dati" nella Convenzione n. 108 del 1981. – 1.3. Minimizzazione e "qualità dei dati" nella Direttiva 95/46/CE. – 1.4. La normativa italiana di recepimento. – 1.5. Il principio di «minimizzazione dei dati» nel GDPR. – 1.6. Il principio di minimizzazione dei dati nella Convenzione di Strasburgo n. 108, aggiornata a seguito del Protocollo di modifica del 2018 (c.d. Convenzione n. 108+). – 2. Portata del principio. – 2.1. Il principio di minimizzazione dei dati e i tre criteri in cui si declina. – 2.2. Il rapporto con altri principi complementari (con particolare riferimento al principio di necessità e di proporzionalità). – 2.3. Principio di minimizzazione dei dati ed approccio "olistico" di tipo "quali-quantitativo". – 2.4. (*segue*): connessioni con la *privacy by design* e *by default*. – 3. Applicazione del principio nella casistica – 3.1. Il principio di minimizzazione dei dati nella casistica del Garante per la protezione dei dati personali. – 3.2. Il principio di minimizzazione dei dati nella casistica delle Autorità di controllo degli altri Paesi membri dell'UE. – 3.3. Il principio di minimizzazione dei dati nella giurisprudenza della Corte di giustizia dell'UE. – 3.4. Il principio di minimizzazione dei dati nella giurisprudenza nazionale italiana e straniera. – 3.4.1. Il principio di minimizzazione dei dati nella giurisprudenza della Corte di Cassazione. – 3.4.2. Il principio di minimizzazione dei dati nella giurisprudenza della Corte Regionale di Bonn. – 3.5. Riflessioni conclusive.

1. Inquadramento normativo

1.1. L'enunciazione del principio di minimizzazione dei dati nel GDPR

Il principio di minimizzazione è uno dei principi generali in materia di protezione dei dati personali. È sancito dall'art. 5, par. 1, lett. *c)* del GDPR, in forza del quale «i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Esprime la necessità che la raccolta di dati personali e le ulteriori operazioni avvengano sempre nei limiti di quanto necessario per il raggiungimento dello scopo che anima il trattamento, determinato dal titolare.

Nell'impianto europeo esso si pone quale principio cardine che non può essere in alcun modo limitato senza fondate giustificazioni[1]; un "vettore" che deve indirizzare ogni titolare del trattamento nella scelta selettiva di quali informazioni,

---

* Pur essendo lo scritto frutto di riflessione comune, i par. 1 e 2 sono da attribuire a Lara Zanetti, i par. 3.1, 3.2, 3.3, 3.4.2 e 3.5 sono da attribuire a Lucrezia Matarazzo, il par. 3.4.1 è da attribuire a Silvia Giulia Battistini.

[1] Così M. SINISI, *Uso dei big data e principio di proporzionalità*, in *federalismi.it*, 2020, 8, pp. 358-378.

riguardanti una persona identificata o identificabile, acquisire per il raggiungimento delle finalità legittime del trattamento[2].

1.2. Minimizzazione e "qualità dei dati" nella Convenzione n. 108 del 1981

Nella seconda metà del XX secolo le informazioni sono raccolte – e in generale, "trattate" – per la gran parte in formato analogico, oltre che in formato elettronico, e non sono necessariamente pronte per essere oggetto di analisi sofisticate, oggi possibili con lo straordinario progresso tecnologico dell'ultimo ventennio: i *personal computer*, pur diffusi negli ambienti domestici e nelle realtà organizzative pubbliche e private, erano spesso disconnessi dalla rete Internet; i dati personali, "transitando" in connessioni per lo più cablate, hanno iniziato progressivamente ad essere oggetto di trattamenti via via più complessi, trascendendo la mera archiviazione dei dati.

L'affermarsi della gestione automatizzata dei dati ha determinato da un lato l'aumento della quantità di informazioni disponibili e dall'altro la necessità di rivedere il concetto di diritto alla *privacy*, da intendersi sempre più quale diritto al controllo e alla protezione dei dati personali, legato alla loro gestione automatizzata, con profondo scostamento dall'iniziale inquadramento operato nel celebre saggio di Warren e Brandeies in cui la *privacy* era percepita come *the right to be let alone*, ovvero uno *jus excludendi alios*.

In tale prospettiva si pone la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108 del 1981, primo strumento internazionale giuridicamente vincolante in materia di protezione dei dati[3].

Dalla lettura dell'art. 1 emerge che la Convenzione si riferisce solo alle informazioni oggetto di elaborazione automatica, ignorando i dati trattati con procedure manuali o comunque analogiche[4]. Secondo un'autorevole dottrina tale carenza si ritrova nella maggior parte dei provvedimenti normativi dell'epoca, «i quali presen-

---

[2] Per l'analisi giuridica del principio in esame nella sua collocazione all'interno del GDPR si rimanda, per esigenze di economia di trattazione dedicata alla collocazione del principio nell'ambito dell'evoluzione normativa in materia di protezione dei dati personali, a quanto precisato al par. 1.5 del presente scritto.

[3] La Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale è stata adottata dal Consiglio d'Europa a Strasburgo il 28 gennaio 1981 ed è stata ratifica da parte di tutti gli Stai membri dell'UE nel 1999. L'Italia ha provveduto a ratificare la Convenzione di Strasburgo con notevole ritardo mediante la legge 21 febbraio 1989, n. 98, in G.U. n. 66 del 20 marzo 1989. La Convenzione di Strasburgo, a differenza di altre convenzioni del Consiglio d'Europa, ha carattere aperto, nel senso che, una volta entrata in vigore, è accessibile a qualsiasi altro Stato non membro del Consiglio che tuttavia sia stato invitato ad aderirvi da parte del Comitato dei ministri: cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 3 ss.

[4] L'art. 1 della Convenzione 108 sancisce che «Scopo della presente Convenzione è quello di garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano ("protezione dei dati")».

tano il dato comune di mirare alla sola protezione delle notizie personali inserite in raccolte automatizzate»[5].

Il trattamento automatizzato veniva percepito come potenzialmente rischioso, sicché la disciplina normativa era mossa da un approccio essenzialmente difensivo rispetto all'incidenza che le nuove tecnologie potessero avere sui diritti della persona.

Dal testo del provvedimento si possono cogliere importanti principi in materia di protezione dei dati. Un embrionale concetto di "minimizzazione", limitato a «i dati a carattere personale oggetto di elaborazione automatica» si ravvisa nell'art. 5, lett. *c)*, della Convenzione citata in cui si richiedono dati «adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati»[6].

In questo primo provvedimento, si può osservare altresì una "limitata estensione applicativa" del principio di minimizzazione, da ravvisarsi in rapporto a finalità qui individuate con riguardo al solo momento della registrazione, ovvero solamente a una delle diciassette attività che rientrano nell'attuale definizione di trattamento[7].

1.3. Minimizzazione e "qualità dei dati" nella Direttiva 95/46/CE

Dopo quattordici anni dalla Convenzione di Strasburgo le esigenze di regolamentazione in materia di dati personali sono state avvertite anche in seno all'allora Comunità europea, che ha provveduto ad emanare la Direttiva 95/46/CE[8]. Seppur

---

[5] Così R. Pardolesi, *Dalla riservatezza alla protezione dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, I, p. 34. L'A. parla al riguardo di una vera e propria «sindrome da elaboratore».

[6] Nella Convenzione 108, l'art. 5 rubricato «*Qualità dei dati*» si trova nel capitolo II («*Principi fondamentali per la protezione dei dati*») e descrive le caratteristiche e le modalità affinché i dati personali possano ritenersi di qualità adeguata: «I dati a carattere personale oggetto di elaborazione automatica devono essere: *a)* ottenuti ed elaborati lealmente e legalmente; *b)* registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini; *c)* adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati; *d)* esatti e, se necessario, aggiornati; e conservati sotto una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati».

[7] Nel corso del tempo, la diffusione e lo sviluppo della tecnologia digitale e il riconoscimento di un autonomo diritto di protezione dei dati personali ha determinato un'inevitabile evoluzione anche del concetto di trattamento che oggi è, pertanto, più complesso e articolato rispetto al passato. Ben potrebbe poi verificarsi l'ipotesi in cui i dati, registrati per una finalità, vengano poi utilizzati per finalità ulteriori: a differenza di quanto riscontrabile in atti normativi più recenti (come ad esempio, oggi, nel GDPR) la Convenzione non sembra cogliere adeguatamente tale aspetto.

[8] Il Parlamento europeo e il Consiglio dell'Unione europea, in applicazione degli artt. 95 e 251 del Trattato istitutivo della Comunità Europea, hanno emanato la Direttiva comunitaria 95/46/CE il 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in G.U.C.E. n. L. 281 del 23 novembre 1995. Tale Direttiva viene anche definita "Direttiva madre", proprio in quanto costituisce il testo di riferimento – a livello europeo – in materia di protezione dei dati personali. Cfr. le considerazioni espresse nel Documento di lavoro «*Tutela della vita privata su Internet. Un approccio integrato dell'EU alla protezione dei dati on-line*», adottato il 21 novembre 2000 dal Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito ai sensi dell'art. 29 della Direttiva 95/46/CE, p. 22 ss., secondo cui la Direttiva si applica «a qualsiasi trattamento di dati personali che rientra nel relativo ambito di applicazione, indipendentemente dai mezzi tecnici utilizzati».

figlia del suo tempo, tale direttiva rivela un legislatore europeo visionario e lungimirante, capace di anticipare e prevedere quella "rivoluzione" che, negli anni a venire, a seguito dell'introduzione di tecnologie digitali sempre più sofisticate[9], si sarebbe realizzata nell'elaborazione e nello scambio di dati informativi e delle comunicazioni interpersonali[10].

Inoltre, per rimediare alla lacuna lasciata dalla Convenzione di Strasburgo, la c.d. "Direttiva madre", sopra citata, nel *considerando* n. 27, ad esplicitazione del dettato normativo in essa contenuto, afferma espressamente che «la tutela delle persone fisiche deve essere applicata al trattamento dei dati sia automatizzato che manuale», così da evitare «gravi rischi di elusione delle disposizioni».

Il provvedimento dedica l'art. 6, rubricato «Principi relativi alla qualità dei dati», all'elencazione dei principi da applicarsi ad ogni trattamento di dati personali e alla lett. *c)* specifica che i dati personali devono essere «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati».

Si assiste pertanto ad una sostanziale differenza applicativa e concettuale del principio in esame rispetto a quanto previsto nella Convenzione 108: i dati devono presentare le caratteristiche di adeguatezza, pertinenza e non eccedenza nei trattamenti interamente o parzialmente automatizzati nonché nei trattamenti non automatizzati contenuti o destinati a figurare negli archivi[11], valutando la minimizzazione dei dati in riferimento a quelle finalità che sono da individuare non solo con riguardo al momento iniziale del trattamento (la registrazione dei dati), ma anche con riferimento alle operazioni successive di trattamento (ossia al trattamento nel suo insieme, considerato unitariamente, così come nelle sue singole operazioni)[12].

---

[9] Si legga diffusamente S. RODOTÀ, *Intervista su privacy e libertà*, a cura di CONTI, Roma-Bari, 2005.

[10] La consapevolezza del legislatore della centralità in futuro del ruolo della tecnologia e della conseguente sempre maggiore necessità di tutela dei dati personali si deduce dalla lettura combinata di alcuni considerando della Direttiva 95/46/CE: «(4) considerando che nella Comunità si ricorre sempre più frequentemente al trattamento di dati personali nei vari settori delle attività economiche e sociali; che i progressi registrati dalle tecnologie dell'informazione facilitano notevolmente il trattamento e lo scambio di tali dati»; «(14) considerando che la presente direttiva dovrebbe applicarsi al trattamento dei dati in forma di suoni e immagini relativi a persone fisiche, vista la notevole evoluzione in corso nella società dell'informazione delle tecniche per captare, trasmettere, manipolare, registrare, conservare o comunicare siffatti dati»; e dall'art. 33, ai sensi del quale «(…) La Commissione esaminerà in particolare l'applicazione della presente direttiva al trattamento dei dati sotto forma di suoni o immagini relativi a persone fisiche e presenterà le eventuali proposte necessarie, tenuto conto dell'evoluzione della tecnologia dell'informazione e alla luce dei progressi della società dell'informazione».

[11] Cfr. art. 3 («*Campo di applicazione*»), par. 1, della Direttiva 95/46/CE.

[12] L'art. 2, lett. *b)* della Direttiva 95/46/CE definisce il trattamento dei dati personali come «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione».

1.4. La normativa italiana di recepimento

In Italia, il Parlamento aveva provveduto a recepire i dettami internazionali e comunitari tramite la l. n. 675 del 31 dicembre 1996[13], che ha rappresentato la prima normativa organica di settore[14], attuando un intervento di ampio respiro in materia di diritto alla riservatezza e di diritto all'identità personale[15]. Analogamente a quanto previsto nella direttiva europea, la l. n. 675/1996, «ha valorizzato solennemente il diritto alla riservatezza e il diritto all'identità personale, e si è poi articolata in una disciplina dell'attività di raccolta e di elaborazione delle informazioni che, in varia forma, attengono alla persona»[16].

La *privacy* e la sicurezza delle informazioni, strumentale per assicurare la prima, assumono grande rilevanza anche là dove il trattamento non riguardi la sfera intima dell'interessato[17] e il legislatore italiano, nel disciplinare la «Modalità di raccolta e requisiti dei dati personali», enunciava, all'art. 9, lett. *d)*, che «i dati oggetto

[13] Il Parlamento nello stesso giorno aveva approvato, oltre alla l. n. 675/1996, («Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»), la l. n. 676/1996 con cui delegava il governo ad emanare (per i diciotto mesi successivi all'entrata in vigore) decreti legislativi al fine di adattare la l. n. 675/1996 alle concrete esigenze del contesto italiano. La scelta di regolamentare la materia non era derivata tuttavia dalla particolare sensibilità del legislatore, quanto dalla necessità di provvedervi al fine di poter aderire all'Accordo di Schengen sui controlli alle frontiere. In merito si ricorda che fino ad allora, l'Italia unitamente alla Grecia erano gli unici Stati appartenenti all'Unione Europea privi di una disciplina del trattamento dei dati personali. Cfr. M. Bin, *Privacy e trattamento dei dati personali: entriamo in Europa*, in *Contr. Impr./Europa*, 1997, p. 459. Il lungo corso di proposte di legge sulla regolamentazione delle banche iniziato negli anni Ottanta viene così a concludersi. In riferimento al primo disegno di legge in materia risalente al 1984, Cfr. *Atti parlamentari (Camera),* n. 1675/C, IX Legislatura e il c.d. "Progetto Mirabelli" in Aa.Vv., *"Banche di dati" e diritti della persona*, Padova, 1985, pp. 205 ss.

[14] In tal senso, cfr. C. Castronovo, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Eur. dir. priv.*, 1998, pp. 653 ss. Nella stessa direzione s'è espressamente ritenuto che la l. n. 675/1996 debba essere considerata «l'atto di nascita della legislazione in materia di protezione dei dati personali». Così A. Biasiotti, *Il nuovo regolamento europeo sulla protezione dei dati. Una guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679 aggiornata alle più recenti interpretazioni e disposizioni normative,* Roma, 2017, p. 31. Per un commento in dottrina cfr., tra gli altri, M. Granieri, *Il sistema della tutela dei diritti nella legge 675/1996*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, II, p. 437 ss.; E. Giannantonio-M.G. Losano-V. Zeno Zencovich (a cura di), *La tutela dei dati personali. Commentario alla L. 675/96*, Padova, 1999; M.G. Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Roma-Bari, 2001.

[15] Così il Garante della Privacy che in *La tutela dei dati personali: una novità nella legislazione italiana,* Relazione 1997, 30 aprile 1998, sottolinea come «Gli interventi normativi del 1996 si sono articolati in una pluralità di innovazioni e sono destinati ad incidere in maniera significativa sull'assetto dei diritti garantiti costituzionalmente, favorendone un corretto bilanciamento».

[16] *Ibidem*.

[17] Nelle prime righe della Relazione annuale del 1997, il Garante per la protezione dei dati personali specificava che «l'approccio normativo ha posto come oggetto della nuova disciplina, il "trattamento" di qualunque informazione di carattere personale, anche se non riguardante la sfera più intima della persona». Il testo completo, disponibile all'url https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1343305, è stato consultato, da ultimo, in data 14 novembre 2023.

di trattamento devono essere (…) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati»[18].

Entrava dunque nel nostro ordinamento interno il principio di minimizzazione fissato nella Direttiva 95/46/CE e, prima ancora, dalla Convenzione n. 108 del 1981. In nessun caso il titolare può utilizzare i dati oltre il confine impresso dallo scopo, il quale costituisce pertanto sugli stessi un "vincolo di destinazione".

Alla l. n. 675/96 fecero seguito, nel nostro ordinamento, ulteriori provvedimenti normativi in materia di protezione dei dati personali, tanto da richiedere, agli inizi del nuovo millennio, un'opera di coordinamento e razionalizzazione con l'emanazione di un testo unico in materia. Ha così visto la luce il Codice in materia di protezione di dati personali, adottato con d.lgs. 30 giugno 2003 n. 196 (c.d. Codice privacy)[19] che ha provveduto ad abrogare formalmente la l. n. 675/1996 pur recependone principi e norme. Il nuovo Codice elevava per la prima volta il «diritto alla tutela dei dati personali» a posizione giuridica autonoma riconosciuta esplicitamente in capo a «chiunque»[20].

La materia del trattamento dei dati personali, con il Codice del 2003, era stata dettagliatamente regolamentata in maniera organica, con un sostanziale adeguamento ai principi comunitari. L'art 3 del Codice introduceva, per la prima volta, il principio di necessità nel trattamento dei dati che si riferiva ai contesti informatici e telematici che «sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi»[21]. Rappresenta una vera rivoluzione nell'approccio alla protezione dei dati trattati con sistemi automatizzati[22] in quanto dispone che i sistemi informatici e i *software* siano configurati in modo da minimizzare il ricorso a dati personali e identificativi nei trattamenti, prevedendo in loro sostituzione l'utilizzo di dati anonimi o pseudonimi quando le finalità non ne risentano e prescrivendo l'identificazione dell'interessato solo in caso di necessità.

Il "principio di necessità", scolpito nell'art. 3, non va però confuso con quello di "minimizzazione", che nell'impianto del Codice trovava la sua collocazione in altra disposizione normativa. L'art. 11, infatti, rubricato «*Modalità di trattamento e requisiti dei dati*», riproponeva alla lett. *d)* la necessità che i dati abbiano requisiti di pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono rac-

---

[18] Nella l. n. 675/1996, l'art. 9 era il primo articolo del Capo III («*Trattamento dei dati personali*»), Sezione I («*Raccolta e requisiti dei dati*»).

[19] Il d.lgs. n. 196/2003 ha istituito il Codice in materia di protezione dei dati personali (anche detto «Codice della *privacy*»), semplificando e coordinando in un unico testo tutte le precedenti disposizioni in Italia relative alla protezione dei dati personali sorte successivamente all'adozione della l. 675/1996.

[20] L'art. 1 del d.lgs. 196/2003, rubricato significativamente «*Diritto alla protezione dei dati personali*», nella sua originaria formulazione, enunciava testualmente che «Chiunque ha diritto alla protezione dei dati personali che lo riguardano».

[21] L'art. 3 del d.lgs. n. 196/2003, rubricato «*Principio di necessità dei dati*», stabiliva che «I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità».

[22] Questo principio non era previsto né nella Direttiva 95/46/CE né nella l. 675/1996.

colti o successivamente trattati, ricalcando quanto già previsto nella l. n. 675/1996[23]. In base a tale norma, poi abrogata, l'utilizzo di dati personali, incluso quelli identificativi, doveva dunque avvenire solo nei casi in cui questi fossero indispensabili per il raggiungimento delle finalità del trattamento [art. 11, lett. *d)*], che dovevano essere determinate, legittime ed esplicite [art. 11, lett. *b)*] e per il periodo necessario a tale scopo [art. 11, lett. *e)*].

Dalla lettura dell'11, lett. *d)*, del Codice – nelle sue evidenti connessioni con le restanti lettere del medesimo articolo e con l'art. 3 – si possono trarre gli elementi sostanziali che costituiranno il «principio di minimizzazione», come attualmente delineato nel Reg. UE n. 679/2016 (GDPR).

1.5. Il principio di «minimizzazione dei dati» nel GDPR

Negli ultimi decenni, a seguito dell'evoluzione di Internet e della diffusione dei *social media*, il contesto sociale ed economico ha subito profondi mutamenti. Oggi le informazioni sono prodotte in grande quantità in formato digitale (c.d. *big data analytics*), con un conseguente aumento a dismisura delle possibilità di raccolta, indicizzazione, organizzazione, comprensione e analisi, anche al fine di porre in essere processi decisionali automatizzati, basati o no su sistemi di intelligenza artificiale. L'uso di dati personali è frequentemente alla base di *business models* volti ad ottenere forme di remunerazione elevate. La circolazione stessa dei dati è incoraggiata dalla normativa europea nella prospettiva di favorire la creazione del mercato unico digitale e di accelerare i processi di integrazione all'interno dell'Unione.

Sono sorte pertanto nuove esigenze nel trattamento dei dati personali e il Reg. UE 2016/679 (GDPR) – dopo il riconoscimento espresso, da parte della Carta dei diritti fondamentali dell'Unione europea, del diritto alla protezione dei dati quale diritto fondamentale della persona – ha posto in essere una disciplina uniforme per tutti i Paesi dell'Unione europea, rafforzando e ammodernando le disposizioni di tutela contenute nella previgente disciplina comunitaria.

Particolarmente significativa, nel nuovo testo normativo, è la disposizione con cui vengono elencati e "codificati" i «*Principi applicabili al trattamento di dati personali*». Si tratta dell'art. 5 del Regolamento, nel quale si stabilisce, al par. 1, lett. *c)*, che i dati debbano essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati», ravvisando espressamente in ciò il principio di «minimizzazione dei dati»[24].

---

[23] L'art. 11, co. 1, del Codice, testualmente, prevedeva che «I dati personali oggetto di trattamento sono: *a)* trattati in modo lecito e secondo correttezza; *b)* raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; *c)* esatti e, se necessario, aggiornati; *d)* pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; *e)* conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati».

[24] Più precisamente, l'art. 5 GDPR, rubricato «*Principi applicabili al trattamento di dati personali*», stabilisce, al par. 1, che: «I dati personali sono: *a)* trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("*liceità, correttezza e trasparenza*"); *b)* raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

Com'è noto, l'emanazione del GDPR ha comportato l'esigenza di coordinare le norme di diritto interno dei singoli Paesi membri dell'UE con quelle, di rango superiore, contenute nel predetto Regolamento europeo. Nel diritto italiano il coordinamento normativo si è avuto con il d.lgs. n. 101/2018[25], che, non senza ritardo e con un iter alquanto tribolato, ha novellato il Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003 e ss.mm.ii.), le cui disposizioni, risultanti a seguito dell'intervento di adeguamento della normativa interna a quella europea, devono ora essere interpretate e applicate in conformità al Regolamento. Sicché l'art. 3 (in cui si trovava disciplinato il principio di necessità nel trattamento dei dati) e l'11, lett. *d)*, del predetto Codice (in cui trovava collocazione il principio di minimizzazione dei dati) sono stati formalmente abrogati dal d.lgs. 101/2018, dovendosi ora rinvenire l'attuale riferimento normativo direttamente nell'art. 5 del GDPR.

1.6. Il principio di minimizzazione dei dati nella Convenzione di Strasburgo n. 108, aggiornata a seguito del Protocollo di modifica del 2018 (c.d. Convenzione n. 108+)

Il 18 maggio 2018 il Consiglio ha approvato un Protocollo di modifica del testo della Convenzione (noto anche come Convenzione 108+) volto a modernizzare e migliorare il testo originario della Convenzione, ad affrontare i problemi relativi al rispetto della vita privata derivanti dall'uso delle nuove tecnologie relative all'*Information and Communication Technology*, tenendo conto delle nuove sfide emerse negli ultimi quarant'anni, e a rafforzare in generale il meccanismo della Convenzione, anche al fine di garantirne l'effettiva applicazione così da riuscire ad affrontare le nuove sfide digitali e i nuovi pericoli che si presentano quotidianamente a livello globale. Nel Preambolo si precisa infatti che «*it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual*

un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("*limitazione della finalità*"); *c)* adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("*minimizzazione dei dati*"); *d)* esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("*esattezza*"); *e)* conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("*limitazione della conservazione*"); *f)* trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("*integrità e riservatezza*")».

[25] D.lgs. 10 agosto 2018, n. 101 recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)».

and, given the diversification, intensification and globalisation of data *processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data*» ed ancora, nella medesima direzione, si rimancarca che «*it is necessary to promote* at the global level *the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people*»[26].

Il Protocollo, nella prospettiva enunciata, istituisce un quadro giuridico multilaterale robusto e flessibile, destinato a facilitare il flusso transfrontaliero dei dati e ad offrire nel contempo garanzie efficaci in caso di uso di dati personali. L'esigenza di rivedere il testo originario della Convenzione n. 108 è duplice: per un verso è stata avvertita la necessità di modernizzarne i contenuti, al cospetto dei grandi cambiamenti che hanno interessato la società, l'economia, il progresso tecnologico; per altro verso si è voluto allineare la Convenzione di Strasburgo alle importanti novità introdotte nell'ordinamento europeo con il GDPR.

A tal fine, il Protocollo contiene, rispetto al testo originario della Convenzione, rilevanti innovazioni, tra cui l'obbligo di notifica delle violazioni dei dati (*data breach*), il richiamo pervasivo al principio di proporzionalità e al principio di *accountability*, specifiche previsioni in materia di *privacy by design* e *privacy by default*.

Riceve invece conferma il principio di minimizzazione dei dati, ribadito all'art. 5, par. 4, lett. *c)*, ove si prevede – con una riformulazione rimasta sostanzialmente inalterata rispetto al testo del 1981, fatta eccezione per l'ambito di applicazione della disciplina, riferibile ora a tutti i trattamenti di dati personali e non solamente a quelli automatizzati – che «*Personal data undergoing processing shall be (…) adequate, relevant and not excessive in relation to the purposes for which they are processed*»[27]. Tali scelte normative sono da considerarsi oggi fondamentali

[26] Il testo integrale dell'*Explanatory Report to the Protocol amending the Conventionfor the Protection of Individual with regard to Automatic Processing of Personal Dat*a, reso dal Consiglio d'Europa a Strasburgo il 10 ottobre 2019, è consultabile al seguente link https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (consultato da ultimo in data 14 novembre 2023). Il testo consolidato della Convenzione n. 108+ (*Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*) del 18 maggio 2018 è invece consultabile all'indirizzo https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (consultato anch'esso, da ultimo, in data 14 novembre 2023).

[27] L'art. 5 del testo consolidato della Convenzione n. 108+, rubricato «*Legitimacy of data processing and quality of data*», è del seguente tenore: «1. *Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.*
2. *Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.*
3. *Personal data undergoing processing shall be processed lawfully.*
4. *Personal data undergoing processing shall be*: a) *processed fairly and in a transparent manner*; b) *collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes*; c) *adequate, relevant and not excessive in relation to the purposes for which*

per mantenere la fiducia nell'ambiente digitale ed assicurare un regime omogeneo di protezione tra gli Stati aderenti al Consiglio d'Europa, siano essi appartenenti o meno all'UE.

Le nuove norme avvicinano dunque il regime della Convenzione di Strasburgo, così come aggiornata nel 2018, al regime stabilito dal Regolamento europeo (GDPR)[28]. In esse il principio di minimizzazione, già previsto nel testo originario del 1981, viene confermato come caposaldo della disciplina in materia di protezione dei dati personali.

2. PORTATA DEL PRINCIPIO

2.1. Il principio di minimizzazione dei dati e i tre criteri in cui si declina

Nel corso degli ultimi anni si è assistito al progressivo affermarsi della digitalizzazione, caratterizzata da una vera e propria «esplosione del volume di dati personali raccolti e il loro utilizzo per scopi personali»[29]. In questo contesto già nel 2009 Meglena Kuneva, Commissario europeo per la tutela dei consumatori, ha affermato che «[*p*]*ersonal data is the new oil of the internet and the new currency of the digital world*»[30]: i dati sono il nuovo petrolio, una ricchezza non contenibile la cui tutela richiede un costante equilibrio tra sicurezza e libertà[31], a dire il vero non sempre

they are processed; d) *accurate and, where necessary, kept up to date*; e) *preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed*».

Il testo originario dell'art. 5, coerentemente con l'ambito di applicazione della Convenzione 108 del 1981, stabiliva invece che «*Personal data undergoing* automatic *processing shall be (…)* c) *adequate, relevant and not ecessive in relation to the purpose for which they are stored*».

[28] Anche l'ambito di applicazione della Convenzione di Strasburgo è mutato in sintonia con le previsioni del GDPR), riferendosi ora non solo al trattamento automatizzato di dati, ma ad ogni trattamento di dati personali: l'art. 2, lett. *b)* e *c)*, della Convenzione 108+ prevede infatti che « *"data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data; Where automated processing is not used, "data processing" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria*». Nel teso originario della Convenzione 108 del 1981, invece, la disciplina trovava applicazione unicamente ai trattamenti in tutto o in parte automatizzati, come ben si evince dalla lettura dell'art. 1 e dell'art. 2, lett. *c)*.

[29] Discorso pronunciato il 31 marzo 2009 a Bruxelles, nell'ambito di una *Roundtable on Online Data Collection, Targeting and Profiling*, da Meglena Kuneva, Commissario europeo per la tutela dei consumatori, ove ha sostenuto che «*Internet is an advertisement supported service and the development of marketing based on profiling and personal data is what makes it go round. Personal data is the new oil of the internet and the new currency of the digital world*». Il testo completo è disponibile *online* all'url https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (consultato da ultimo il 7 ottobre 2020).

[30] *Ibidem*.

[31] Benjamin Franklin nel 1775, in riferimento all'equilibrio inteso in termini di esigenze apparentemente contrapposte, sosteneva che «chi è pronto a dar via le proprie libertà fondamentali per

raggiunto in maniera soddisfacente poiché «allo stesso modo in cui internet è senza confini, anche le domande relative alla raccolta dei dati sono globali»[32].

L'avvento e il progresso della società digitale ha rinnovato il concetto di diritto alla protezione dei dati presentando all'interprete nuovi scenari che hanno aperto molti interrogativi, *in primis* l'impatto sui diritti e valori fondamentali dell'uomo in materia di trattamento di dati personali.

La stessa giurisprudenza della Corte di giustizia[33] ha avuto sempre più spesso ad oggetto le innovazioni tecnologiche e il trattamento dei dati nelle comunicazioni elettroniche – si pensi a titolo esemplificativo alle pronunce *Digital Rights Ireland*[34] e *Tele2 Sverige*[35] – e, nel tentativo di risolvere questi moderni aspetti in relazione alla tutela dei dati delle persone fisiche, ha ribadito con forza la difesa della libertà e della dignità della persona, passando definitivamente da una «configurazione [della tutela] prevalentemente *market-driven* a una *fundamental rights-oriented*»[36].

Nell'epoca dell'interconnessione globale, rileva il sostanziale cambio di paradigma del legislatore[37], che già da tempo è passato da una concezione sostanzialmente *statica* del diritto, espressione di una pretesa di essere lasciati soli con sé stessi (che per certi aspetti richiamava ancora il *the right to be let alone*[38] di statunitense

comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza». (B. Franklin, *Pennsylvania Assembly: Reply to the Governor*, November 11, 1755 in *The Papers of Benjamin Franklin*, ed. Leonard W. Labaree, 6, 1963, p. 242).

[32] Così M. Kuneva, *Roundtable on Online Data Collection, Targeting and Profiling*, cit. («*In much the same way that the internet is borderless, the questions pertaining to online data collection are also global*»).

[33] Cfr. G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. inf.*, 2015, pp. 779 ss.; F. Pizzetti, *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya"*, in *Dir. inf.*, 2014, pp. 805 ss.

[34] CGUE, 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland*, con cui è stata dichiarata l'invalidità dell'intera direttiva 2006/24/CE sulla conservazione dei dati di traffico telefonico e telematico, dei dati relativi all'ubicazione dell'abbonato e quelli necessari alla sua identificazione (*data retention*), poiché lesiva del principio di proporzionalità.

[35] CGUE, 21 dicembre 2016, C-203/15 e C-698/15, in cui la Corte ha inibito ai fornitori di servizi di comunicazione elettronica «una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica».

[36] M. Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quad. cost.*, 2016, 3, p. 588.

[37] Cfr. G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati personali*, in *Nuove leggi civ. comm.*, 2017, 1, pp. 1-18; F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, 2, pp. 369 s. Quest'ultimo A. esclude che il nuovo Regolamento rappresenti una sorta di riaffermazione della previgente tutela in materia di *privacy*, dal momento che il legislatore ora presenta essenzialmente una disciplina che pone una maggiore enfasi sulla circolazione dei dati personali, piuttosto che sulla protezione della persona, con un vistoso arretramento su questo terreno.

[38] Il noto "*right to be let alone*" di cui parlavano S.D. Warren e L.D. Brandeis nel loro articolo *The right to privacy*, in *Harward Law Review*, 15 dicembre 1890.

memoria), ad un approccio di tipo "dinamico"[39], favorito dalla circolazione dei dati attraverso il diffuso utilizzo di comunicazioni elettroniche[40].

In risposta alla reticolare affermazione della società dell'informazione e della comunicazione[41], si è profilata pertanto una nuova dimensione sostanziale di *privacy*[42] che va oltre i problemi legati alla tutela della riservatezza individuale e che pone l'accento sulla "protezione dei dati" anche da archiviazioni e trattamenti non necessari.

Tra gli obiettivi del GDPR vi è sicuramente anche quello di «garantire un elevato livello di protezione dei dati personali»[43] da perseguire nel rispetto di quei principi che il legislatore ha da tempo individuato quali focali elementi per la tutela delle persone rispetto al trattamento dei dati personali.

Sebbene la totalità dei principi abbia una valenza che copre ogni aspetto della disciplina, particolare attenzione merita il già citato principio di minimizzazione dei dati – contemplato all'art. 5, lett. *c)*, GDPR –, che costituisce il «cardine della normativa europea»[44] e fissa, a vantaggio dell'interessato, un limite "interno" al trattamento[45]. Come già rimarcato, rappresenta un "vettore" che deve indirizzare ogni ti-

---

[39] L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in *Federalismi.it*, 14 febbraio 2018, p. 23.

[40] Cfr. S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari 2012, pp. 397 s.

[41] L'espressione "società dell'informazione" è stata usata per la prima volta nel 1973 da Daniel Bell, ordinario di sociologia a Harvard, per indicare una società moderna che essendo giunta al culmine del processo di industrializzazione, per continuare a crescere, deve concentrare i propri sforzi verso la produzione di beni immateriali. Nel 2001 l'ONU ha decretato la nascita di una sede di confronto internazionale (denominata WSIS – *World Summit on the Information Society*) per affrontare gli aspetti generali e i problemi specifici inerenti a tale fenomeno qualificato come «un processo dinamico che promette una trasformazione profonda in ogni aspetto della nostra vita: (…). Siamo infatti nel pieno di una rivoluzione, forse la maggiore che l'umanità abbia mai sperimentato (...)». Così in *La governance di internet*, *Quaderni di documentazione n. 43*, a cura di SERVIZI GIURIDICI, Senato della Repubblica, Roma, 2006, pp. 9-10.

[42] Così M. MENSI-P. FALLETTA, *Il diritto del web. Casi e materiali*, Padova, 2015, p. 308, cit. («l'avvento di Internet e le innovazioni tecnologiche che ne hanno accompagnato il successo da un lato hanno intensificato lo scambio di informazioni tra cittadini, aumentando la conoscenza, le possibilità di comunicazione, la libertà di espressione e opinione, incentivando il dialogo e lo scambio culturale, dall'altro hanno ridefinito il confine tra spazio pubblico e privato, riducendo entro limiti certamente più angusti rispetto al passato quell'area di riservato dominio qualificabile come privacy»).

[43] *Considerando* n. 6, GDPR.

[44] Così M. SINISI, *Uso dei big data e principio di proporzionalità*, in *federalismi.it*, 2020, 8, pp. 358-378.

[45] Cfr. E. NAVARRETTA, *Comm. art. 11 d.lgs. 196/2003*, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, Padova, 2007, I, p. 266, ove rileva che, per il principio di minimizzazione, le finalità fissate dal titolare del trattamento assolvono la funzione di limitare la libertà di trattamento in maniera «non predeterminata *in toto* dal legislatore, ma affidata anche alla scelta del titolare del trattamento. Sul presupposto di un'opzione normativa che esclude una generica libertà di trattamento dei dati, il titolare è chiamato a definire, entro le coordinate della legittimità dello scopo, una finalità specifica della sua attività che, a partire da quella scelta, configura un limite invalicabile per l'esercizio della situazione soggettiva, a tutto vantaggio dell'interessato, la cui posizione viene a contrapporsi ad una libertà specificata rispetto ad un interesse puntuale». Il discorso, riferito al principio di minimizzazione contenuto nell'art. 11 del Codice in materia di protezione dei dati personali, conserva

tolare del trattamento nella scelta selettiva in ordine a quali informazioni concernenti una persona fisica identificata o identificabile possa trattare per il raggiungimento delle proprie finalità legittime.

Il principio di minimizzazione dei dati parte dall'idea che, salvo poche eccezioni, un titolare deve trattare i dati raccolti solo nei limiti del raggiungimento delle finalità per le quali sono stati richiesti[46].

Esso si declina in tre profili (o criteri):

(i) *adeguatezza* dei dati, ossia proporzionalità dei dati rispetto alle finalità per le quali sono raccolti;

(ii) *pertinenza* dei dati rispetto alle finalità, nel senso che non vanno raccolti o comunque trattati dati che non abbiano corrispondenza con la finalità del trattamento;

(iii) *limitazione* del trattamento dei dati a quelli realmente necessari, escludendo dati raccolti o comunque trattati in misura maggiore a quella strettamente necessaria per il raggiungimento della finalità del trattamento.

Rispetto alle declinazioni precedenti del principio di minimizzazione, il legislatore ha finito per abbandonare la logica della "completezza" del dato – riscontrabile nell'art. 11, co. 1, lett. *d)*, del Codice in materia di protezione dei dati personali –, a favore di una logica di "adeguatezza" del dato, con un approccio decisamente "minimalista", offrendo una prudente soluzione alle complesse questioni in materia di protezione dei dati personali sottese soprattutto all'immane diffusione di comunicazioni elettroniche. In tali termini, "completezza" e "adeguatezza" sono da intendersi quali concetti disgiunti e non necessariamente coesistenti: un dato, infatti, ben potrebbe essere adeguato alle finalità pur non essendo completo. Variazioni lessicali, queste, in cui viene veicolata l'innovazione sostanziale della tutela del diritto alla protezione dei dati personali, che da statica e negativa è divenuta dinamica e positiva[47].

L'adeguatezza e pertinenza del dato sono criteri che richiedono di selezionare i dati nella fase di raccolta, in previsione anche delle successive operazioni, in relazione agli scopi del trattamento. Ciò comporta un intervento selettivo già in fase di progettazione del trattamento e per impostazione predefinita (*privacy by design* e *by default*), ponendo particolare attenzione proprio all'analisi dei dati, che devono mantenersi strettamente funzionali al raggiungimento delle finalità predeterminate. Tale analisi, propedeutica ad un intervento selettivo sui dati medesimi, va però condotta non solamente nel momento iniziale del trattamento, con un approccio statico, ma anche nel suo divenire e dunque secondo un approccio dinamico, che segue l'intero ciclo di vita del trattamento[48].

---

ovviamente la sua attualità anche al cospetto del nuovo assetto normativo e, segnatamente, dell'art. 5, par. 1, lett. *c)*, del GDPR.

[46] E. Navarretta, *op. cit.*, pp. 266 ss.

[47] Si veda, tra gli altri, S. Calzolaio, voce *Protezione dei dati personali,* in *Dig. disc. pubbl.*, Torino, 2017, p. 53.

[48] Significative a tal riguardo sono le parole di chi ha rimarcato che, «Stando alle regole generali dell'economia, per ogni dato che viene successivamente raccolto, cresce l'utilità che si ricava dalla lettura complessiva dei dati, tuttavia detta utilità cresce in misura meno che proporzionale rispetto

A tale conclusione si giunge anche osservando il terzo profilo, che si traduce nell'analisi della "non eccedenza" dei dati personali, avendo sempre riguardo alle finalità legittime del trattamento individuate dal titolare. Infatti, come ben rimarcato in dottrina, la «non eccedenza dei dati comporta la necessità che il titolare compia periodiche e sistematiche verifiche dirette ad assicurare la strumentalità delle operazioni di trattamento rispetto alle finalità perseguite. I dati raccolti o detenuti non necessari al perseguimento delle finalità dichiarate e perseguite dal titolare del trattamento costituiscono dati eccedenti e pertanto vanno distrutti o resi anonimi»[49].

In tal modo si giunge ad ampliare il livello di tutela dell'interessato, riducendo a monte i rischi di esposizione a pregiudizi che potrebbero derivargli dal trattamento di dati relativi alla sua persona. In queste logiche il legislatore ha effettuato una trasposizione del principio di precauzione, il quale opera in via preventiva rispetto all'insorgenza del rischio, analogamente a quanto avviene con il principio di minimizzazione dei dati, che opera sin dal momento antecedente al trattamento, imponendo al titolare una valutazione, *ex ante*, di pertinenza del dato rispetto al fine. Nel principio di minimizzazione, tuttavia, la valutazione di adeguatezza, pertinenza e limitazione dei dati rispetto alle finalità legittime del trattamento, come già rimarcato, prosegue anche nell'intero ciclo di vita del trattamento medesimo[50].

2.2. Il rapporto con altri principi complementari (con particolare riferimento al principio di necessità e di proporzionalità)

La corretta definizione del principio di minimizzazione, come oggi concepito, non può prescindere dall'accostamento con altri principi ad esso complementari, che mirano a rafforzare la tutela dell'interessato, con particolare riferimento a: (i) la necessità di raccolta di dati per finalità determinate, esplicite, lecite e la necessità che siano successivamente trattati in modo compatibile con tali finalità (principio di limitazione delle finalità); (ii) la necessità che i dati siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di limitazione della conservazione).

Si tratta di una costellazione di principi che trova la sintesi nei principi di necessità e di proporzionalità, di portata ancora più ampia[51]. In altre parole i dati utilizzati devono essere limitati a quelli strettamente necessari rispetto allo scopo per cui

ad ogni dato addizionale. In altri termini i dati successivamente raccolti, che si riferiscono allo stesso oggetto, soddisfano un interesse alla conoscenza sempre meno importante, cioè aggiungono sempre meno utilità, sì da far ritenere inutile e ingiustificato il sacrificio della riservatezza dell'individuo con un'aggiunta di dati superflui rispetto a quella sufficiente per raggiungere lo scopo». Così A. Paravani, *Qualità e sicurezza dei dati personali*, in *InterLex*, 24 maggio 2000.

[49] G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, p. 118.

[50] In virtù di quanto detto, il principio in esame trova dunque attuazione in qualunque momento del trattamento, estendendosi in maniera ancora più incisiva alla fase antecedente l'inizio dello stesso, ma senza limitarsi ad essa, in modo da ridurre al minimo l'uso dei dati personali.

[51] Sui principi di necessità e di proporzionalità si vedano, rispettivamente, i Capitoli X e XI nel presente volume.

gli stessi sono raccolti, nel rispetto del principio di necessità, in generale, e di proporzionalità, che pertanto diventano parte integrante della struttura del Regolamento ed accompagnano qualsivoglia attività di elaborazione dei dati personali rientrante nell'applicazione del GDPR. Ebbene, il controllo di necessità è un momento focale per vagliare l'effettiva minimizzazione dei dati; esso indaga, in negativo, che il mezzo sia il meno dannoso possibile per la realizzazione di un determinato fine[52]. Allo stesso tempo, il principio di necessità è espressione di quel più generale principio di proporzionalità[53] che assurge a «canone ermeneutico» dell'intera disciplina (europea e nazionale) in materia di protezione dei dati personali. L'importante connessione emerge peraltro anche dalla lettura del *considerando* n. 39, per cui «i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi»[54], tenendo ben presente, per di più, «l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario»[55].

Il Regolamento, all'art. 5, non parla esplicitamente di principio di necessità, ma di minimizzazione del trattamento, che ne costituisce una sottocategoria e richiede che i dati personali debbano sempre essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»[56].

2.3. Principio di minimizzazione dei dati ed approccio "olistico" di tipo "quali-quantitativo"

Nell'insieme, il vaglio di adeguatezza, pertinenza e limitazione a quanto necessario rispetto alle finalità del trattamento si traduce nell'osservanza di un «limite di contenuto dell'attività di trattamento, sotto il duplice profilo quantitativo e qualitativo»[57]. Si può pertanto sostenere che il principio di minimizzazione sottende sempre una valutazione quantitativa e qualitativa dei dati rispetto allo scopo che il titolare persegue nel porre in essere un determinato trattamento[58].

L'espressione "*less is more*" esprime bene la portata di questo principio, poiché oggi il principio di minimizzazione richiede di adottare un *approccio olistico* relativo non solo alla qualità, ma anche alla «quantità dei dati personali raccolti, (…) [alla] portata del trattamento, (…) [al] periodo di conservazione e (…) [all']

---

[52] Cfr. N. Miniscalco, *Uno, nessuno o centomila? Minimizzazione e privacy by default nel primo provvedimento del Garante dopo il GDPR*, in *Dir. inf.*, 2018, 4-5, pp. 782-797.

[53] Si veda A. Sandulli, *Proporzionalità*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, V, Milano, 2006, pp. 4643 ss.

[54] V. *considerando* n. 39 GDPR.

[55] *Ibidem.*

[56] Un riferimento esplicito alla «necessità e proporzionalità dei trattamenti in relazione alle finalità» è comunque contenuto, in maniera esplicita, all'art. 35, par. 7, lett. *b)*, GDPR, in tema di valutazione di impatto.

[57] M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 210.

[58] Per un approfondimento, si veda S. De Nitto, *A proposito della proporzionalità come criterio giuridico*, in *Riv. trim. dir. pubbl.*, 2017, p. 1035.

accessibilità»[59]. Non si tratta solo di raccogliere una minima quantità di dati, ma anche di adottare un "approccio qualitativo" attraverso l'applicazione di specifiche misure tecniche di sicurezza (come la pseudonimizzazione o la cifratura dei dati)[60] che possano realizzare una minimizzazione "qualitativa" dei dati stessi. Ancora, è altresì necessario minimizzare l'estensione delle operazioni di trattamento in relazione alle specifiche finalità, diminuendo in tal modo i rischi per i diritti e le libertà dell'interessato; occorre altresì minimizzare il periodo di conservazione dei dati per ogni finalità, che potrebbe determinare anche la scelta di non conservare alcun dato oppure di anonimizzare o cancellare i dati quanto prima nel momento in cui si è esaurita la loro utilità; infine il titolare deve garantire la minima accessibilità ai dati, definendo i diritti di accesso agli stessi.

In tali termini, il principio di minimizzazione ha trovato espresso riconoscimento anche nel parere n. 1/14 del Gruppo di Lavoro WP29, per cui «*The information registered from the on going monitoring, as well as the information that is shown to the employer,* should be minimized as much as possible. *Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances. Solutions that for example track vehicles can be designed to register the position data without presenting it to the employer. Employers must take the* principle of data minimization *into account when deciding on the deployment of new technologies. The information should be stored for the minimum amount of time needed with a retention period specified. Whenever information is no longer needed it should be deleted*».

Operativamente, il principio di minimizzazione richiede «che, nell'ambito delle relative finalità (esplicitamente predeterminate), il titolare uniformi il compimento delle proprie attività ad una misura idonea a ridurre al minimo le possibili interferenze con la sfera dell'interessato»[61].

2.4. (*segue*): connessioni con la *privacy by design* e *by default*

A tal fine, è necessario che il titolare del trattamento si avvalga di apposite misure tecniche e organizzative in grado di ridurre al minimo il trattamento dei dati personali, nella fattispecie concreta.

Rispetto all'impostazione iniziale della disciplina in materia di protezione dei dati personali, come emergente negli anni '80 del secolo scorso, ove l'approccio

---

[59] D. STEFANELLO, Data protection by default*: trattare solo i dati personali necessari per ogni specifica finalità*, in *iusinitinere*, 7 luglio 2019.

[60] Per approfondire la pseudonimizzazione e la cifratura dei dati: D. STEFANELLO, *Come proteggere i dati personali? Anonimizzazione, pseudonimizzazione e cifratura a confronto*, https://www.iusinitinere.it/come-proteggere-i-dati-personali-anonimizzazione-pseudonimizzazione-e-cifratura-a-confronto-17616.

[61] M. DELL'UTRI, *op. cit.*, p. 210. L'A. precisa poi che «i parametri della misure di minima incidenza del trattamento in rapporto agli scopi (…) rifuggono dalla rigorosa assunzione di valori oggettivamente predeterminabili, limitandosi a rivestire il ruolo di criteri sostanzialmente regolativi cui al giudice [e all'Autorità di controllo] è consentito ricorrere, una volta tematizzato l'ambito dei confini del trattamento così come tracciati dai suoi stessi protagonisti nella concreta dimensione dialettica del conflitto» (*Ibidem*, p. 211).

nei confronti della tecnologia era essenzialmente difensivo, è maturata progressivamente la consapevolezza di poter usare gli strumenti tecnologici anche al fine di incrementare i livelli di tutela per l'interessato.

Si è così assistito ad un graduale rafforzamento dell'importanza del principio di minimizzazione che viene richiamato anche dall'art. 25 del GDPR, intitolato «*Protezione dei dati fin dalla progettazione e per impostazione predefinita*».

Il primo paragrafo di tale articolo, in tema di *privacy by design*, espressamente prevede che «(…) sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati». Il principio di minimizzazione è dunque intimamente collegato con l'obbligo di approntare misure tecniche e organizzative adeguate che diano concreta ed efficace attuazione al principio medesimo[62], a prescindere dalle modalità e dai mezzi con cui viene effettuato il trattamento[63].

Va guardato con interesse, ai fini del nostro discorso, anche a quanto previsto nel secondo paragrafo dell'art. 25, il quale, in tema di *privacy by default*, enuncia espressamente che «il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento di persone fisiche».

Anche la *data protection by default* si basa dunque sul principio di minimizzazione dei dati, accostato inscindibilmente ai principi di limitazione della conservazione e di limitazione delle finalità, i quali concorrono, in uno con il principio di necessità, alla determinazione dei dati personali che possono divenire oggetto di

---

[62] A ragione si può sostenere che il principio di minimizzazione costituisce il presupposto della c.d. *privacy by default* che ne rappresenta una forma di applicazione concreta. Del resto già l'art. 3 del d.lgs. 196/2003, contenente la definizione delle PET (*Privacy Enhancing Technologies*), ha certamente anticipato i concetti di *privacy by default e privacy by design*. Per un approfondimento si veda F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 775-854.

[63] Questa visione derivava dall'interpretazione estensiva che parte della dottrina ha fatto dell'art. 3 del d.lgs. 196/2003 (il c.d. principio di necessità), «come riferito non soltanto ai meri sistemi informatici, ma piuttosto a qualunque strumento e/o procedura, anche non informatizzata». Così N. Miniscalco, *op. cit.,* che ricorda come, secondo F.D. Busnelli, *Commento all'art. 3*, in M. Bianca-F. D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, cit., spec. p. 33, «l'art. 3 parla di "sistemi informativi" in senso generale, anziché di sistemi informatici. Il suo terreno elettivo di applicazione è quello dei contesti informatici e telematici, nei quali opera con evidenza, ma la norma non schiude la porta alla sua applicazione fuori nel mondo dell'elettronica. Deve anzi ritenersi che, per un titolare di trattamento, risponde ai criteri di diligenza e di correttezza nel trattamento dare spontanea attuazione al principio di necessità anche in caso di trattamento non automatizzato di dati».

ogni specifico trattamento. Rispetto alla declamazione del principio di minimizzazione di cui all'art. 5, par. 1, lett. *c)*, tuttavia, l'art. 25, par. 2, si colloca nella fase applicativa, imponendo, come già riscontrato anche per la *data protection by design*, quelle misure tecniche ed organizzative indispensabili per assicurare l'applicazione pratica ed operativa della minimizzazione nella fattispecie concreta di trattamento.

A conferma del rilievo ad esse riconosciuto, giova ricordare il richiamo contenuto nell'art. 83, par. 2, lett. *d)*, del Regolamento che dispone la comminazione di sanzioni amministrative da parte delle Autorità di controllo «tenendo conto delle misure tecniche e organizzative da essi messi in atto ai sensi degli artt. 25 e 32»[64].

Il discorso ben si ricollega all'impatto delle nuove tecnologie e all'impiego delle c.d. PET (*Privacy Enhancing Technologies*), ossia quelle tecnologie "aggiuntive" in grado di mitigare gli effetti indesiderati – attraverso per es. i sistemi di crittografia[65], nonché gli strumenti tecnologici di gestione della *privacy*[66] – la cui produzione è agevolata dal fenomeno dei c.d. «*Big data*»[67], ossia dall'infinita mole di dati prodotti quotidianamente dalla vita digitale delle imprese, delle persone fisiche, delle amministrazioni, dagli oggetti (*Internet of Things*)[68] e trattati nei "non luoghi" detti *cloud*.

Anche a prescindere dai contesti tecnologici più avanzati, il principio di minimizzazione deve connotare in maniera sistematica ogni trattamento di dati personali. Per coglierne meglio la portata applicativa diviene fondamentale il confronto con la

---

[64] Cfr. A.D. Cortesi, *L'art. 25 del GDPR: dalla privacy by default al principio di minimizzazione o necessità nel trattamento dei dati personali*, in *Interlex*, 4 settembre 2017 (da ultimo consultato in data 11 dicembre 2020). L'A. suggerisce di abbandonare il riferimento alla "*privacy by default*", che ritiene potersi contenere nella "*privacy by design*" e di riferirsi in via esclusiva al principio di minimizzazione. Per un approfondimento dei principio di *privacy by design* e *by default* si veda, nel presente volume, il Capitolo XII.

[65] L'idea di utilizzare le tecnologie per disciplinare la tecnologia stessa e, in particolar modo, gli aspetti concernenti la tutela dei dati personali, risale all'art. 17 della dir. 95/46/CE, attraverso l'introduzione delle misure tecniche e organizzative che il responsabile del trattamento doveva attuare per tutelare i dati personali. Proprio in quegli anni, infatti, si sviluppano le *Privacy Enhancing Technologies* (PET), ossia tutte quelle tecnologie nell'ambito dell'*Information and Communications Technology* (ICT) che hanno lo scopo di aumentare la protezione dei dati personali. Il termine *privacy by design*, invece, è stato coniato nel 2010 da Ann Cavoukian, *Privacy Commissioner* dell'Ontario, nel corso della 32ª Conferenza mondiale dei Garanti privacy. Cfr. G. Pascuzzi, *Il diritto nell'era digitale*, 3ª ed., pp. 79 ss.; *32ª Conferenza internazionale delle autorità di protezione dei dati*, Gerusalemme, 27-29 ottobre 2010, in www.icdppc.org.

[66] Si pensi ai c.d. *privacy patterns*, in ordine ai quali si rimanda a F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 800 ss.

[67] Cfr. S. Calzolaio, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *federalismi.it*, 2017, 24, p. 6. Per una spiegazione del fenomeno dei *Big Data* e della possibilità tecnica – molto contestata nel dibattito internazionale – di una sua compatibilità con gli strumenti a tutela della protezione dei dati personali cfr. G. D'Acquisto-J. Domingo Ferrer-P. Kikiras, V. Torra-Y.A. de Montjoye-A. Bourka, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, *European Union Agency for network and information security*, december 2015, in http://www.enisa.europa.eu. In tema si vedano anche D. D'Acquisto-M. Naldi, *Big data e privacy by design*, Torino, 2017, p. 27; M. Bogni-A. Defant, *Big data: diritti IP e problemi della privacy*, in *Riv. dir. ind.*, 2015, pp. 117 ss.

[68] Sull'IoT si veda P. Paganini, *Verso l'internet delle Cose*, in *Dir. ind.* 2015, pp. 107 ss.

casistica concreta, quale emergente dall'analisi dei provvedimenti resi dall'Autorità di controllo.

3. Applicazione del principio nella casistica

3.1. Il principio di minimizzazione dei dati nella casistica del Garante per la protezione dei dati personali

Il Garante per la protezione dei dati personali ha fatto ricorso al principio di minimizzazione dei dati in molteplici fattispecie, talvolta attribuendogli rilevanza maggiormente autonoma, talaltra, invece, facendone applicazione in più stretta relazione con l'operatività di altri principi ad esso intimamente collegati.

In materia di *e-commerce* si segnala, sotto tale ultimo profilo, il provvedimento n. 324 del 20 luglio 2017[69], in cui il Garante ha censurato il trattamento di dati personali nella parte in cui veniva acquisito il consenso dell'interessato al trattamento dei propri dati personali mediante raccolta di un'unica manifestazione di volontà, sia per finalità di acquisto tramite il canale *online*, sia per finalità di *marketing*.

La decisione è stata presa a seguito della segnalazione di alcuni utenti raggiunti da pubblicità indesiderata da parte di una società di *shopping online*, i quali contestavano altresì il mancato rispetto del diritto di opposizione al trattamento dei loro dati dagli stessi esercitato.

Nella specie, veniva prevista la registrazione sul sito e la conseguente accettazione, con un *flag*, delle condizioni contrattuali e della *privacy policy* del sito quale *condicio sine qua non* per accedere ad alcune sezioni del sito medesimo ed eventualmente acquistare i prodotti in vetrina. Così facendo però l'utente, con un solo *click*, finiva per prestare il proprio consenso affinché i propri dati venissero utilizzati non solo per le finalità connesse ai servizi di vendita *online*, ma anche per finalità di *marketing* da parte della società titolare del trattamento e dei suoi *partner* commerciali.

Tale pratica comportava, quale conseguenza, la raccolta e la registrazione in una banca dati di numerosi indirizzi e-mail e dati personali che, successivamente, venivano utilizzati per l'invio di diverse tipologie di pubblicità.

Nel Provvedimento il Garante non si è però limitato ad affermare la violazione del principio di liceità del trattamento, in relazione alle modalità di acquisizione del consenso, ma ha argomentato anche sulla violazione del principio di minimizzazio-

[69] Con il Provv. n. 324 del 20 luglio 2017, doc. *web* n. 6955363, il Garante per la protezione dei dati personali si è pronunciato sulle richieste di tre utenti del sito aziendale della società "Dalani s.r.l.", i quali, nonostante l'esercizio del diritto di opposizione (art. 7 ss. del Codice), hanno continuato a ricevere *email* promozionali. I segnalanti, infatti, sostenevano di aver presentato più volte, alla società titolare del trattamento, formale richiesta di cancellazione dalla *mailing list*. Inoltre, uno di loro lamentava la mancata correttezza di funzionamento dell'indirizzo *e-mail* aziendale inserito nel sito *web* e un altro contestava le modalità di acquisizione del consenso per finalità di *marketing*. La società, a sua difesa, aveva dichiarato di aver provveduto alla cancellazione da loro richiesta e, nel caso della persona che non aveva manifestato il consenso al trattamento, aveva confermato che la stessa non si era registrata al sito ma aveva comunque dato il consenso a società terze per attività di *marketing*.

ne dei dati. Per un verso, infatti, ha sostenuto che obbligare un utente a conferire il consenso per navigare su un sito è un atto che viola la disciplina della protezione dei dati in quanto il consenso deve essere libero e specifico[70]: «il consenso per il trattamento dei dati personali, per essere valido, non deve essere condizionato, ma libero e specifico, oltre che acquisito prima dell'invio di comunicazioni promozionali. Non si può quindi obbligare una persona a ricevere pubblicità solo per avere accesso alla "vetrina *online*" di un sito»; per altro verso, però, il Garante ha ribadito anche la violazione del principio di minimizzazione[71], stante la quantità di dati raccolti dalla società in fase di registrazione al sito, i quali non erano necessari né per la sua navigazione né per l'acquisto dei prodotti in esso reclamizzati. In altre parole, nel caso di specie le informazioni raccolte sono state ritenute eccessive e irrilevanti per le finalità indicate.

In altre occasioni il Garante ha avuto modo di esprimersi sulla necessità del rispetto del principio di minimizzazione a seguito delle numerose violazioni di informazioni e dati personali, contenuti in referti e/o cartelle cliniche di aziende e strutture sanitarie, comunicati per errore, anche attraverso l'utilizzo di *email*, non agli specifici interessati ma a terzi.

In tal senso si veda l'ordinanza ingiunzione resa nei confronti dell'ASL n. 2 Savonese, n. 210 del 14 novembre 2019[72]. Il caso di specie aveva tratto origine da una segnalazione, giunta all'attenzione dell'Autorità, con cui si lamentava una violazione della disciplina rilevante in materia di protezione di dati personali in merito ad una procedura amministrativa effettuata dall'ASL e per ottenere, da una società fornitrice di presidi ortopedici, la presentazione di preventivi per la fornitura di alcune protesi. Assieme alla richiesta di preventivo, tuttavia, l'ASL aveva allegato anche alcuni moduli contenenti dati personali dei pazienti per i quali erano necessari i dispositivi ortopedici, inclusi i dati identificativi e quelli relativi alla loro salute.

Il Garante ha rappresentato che la comunicazione è stata fatta in violazione non solo dei principi di liceità, correttezza e trasparenza, ma anche del principio di minimizzazione, precisando che «il titolare del trattamento è tenuto, in ogni caso, a rispettare i principi in materia di protezione dei dati, fra i quali quello di "liceità, correttezza e trasparenza" nonché di "minimizzazione", in base ai quali i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" e devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. *a)* e *c)*, del RGPD)», «(…) e devono essere trattati, solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi (principi di liceità, correttezza, trasparenza e minimizzazione; cfr. anche Cons. n. 39)».

Le medesime finalità si sarebbero potute perseguire, nel rispetto del principio di minimizzazione, anonimizzando i dati dei pazienti e veicolando alla società

[70] Cfr. art. 130, co. 1 e 2, del Codice (punti 3.1 e 3.2).

[71] Nel Provv. cit. il Garante ha fatto riferimento ai principi di minimizzazione dei dati personali, necessità e correttezza di cui agli artt. 3 e 11, co. 1, lett. *d)* ed *a)*, del Codice.

[72] GPDP, ordinanza ingiunzione nei confronti di ASL n. 2 Savonese n. 210 del 14 novembre 2019, doc. *web* n. 9269852.

fornitrice solamente quelli indispensabili per la formulazione del preventivo, senza pregiudizio per i diritti dell'interessato.

Sul principio di minimizzazione l'Autorità garante ha avuto modo di pronunciarsi anche in tema di diffusione *online* di dati personali da parte di soggetti pubblici, in mancanza di un corretto presupposto normativo.

Con l'ordinanza di ingiunzione n. 209, datata 7 novembre 2019[73], il Garante ha censurato il comportamento del Comune di Tivoli che aveva pubblicato sull'albo pretorio *online* del sito *web* istituzionale del Comune una deliberazione della Giunta Comunale contenente dati e informazioni personali di un dipendente comunale «riguardanti anche la notizia della pendenza di un procedimento penale nei suoi confronti (poi archiviato)», la cui pubblicazione si è protratta per un periodo superiore ai quindici giorni previsti dalla normativa di settore[74].

La necessità del rispetto del principio di minimizzazione ai sensi dell'art. 5, par. 1, lett. *c)*, GDPR[75], viene rimarcata dal Garante ricordando quanto previsto nel provvedimento n. 243 del 15 maggio 2014[76] recante le «*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*» secondo cui «anche in presenza di un obbligo di pubblicazione, i soggetti chiamati a darvi attuazione non possono comunque diffondere i dati personali eccedenti o non pertinenti (…)».

Ne consegue che «fin dalla fase di redazione degli atti e dei documenti oggetto di pubblicazione, nel rispetto del principio di adeguata motivazione, non dovrebbero essere inseriti dati personali "eccedenti", "non pertinenti", "non indispensabili" (e, tantomeno, "vietati"). In caso contrario, occorre provvedere, comunque, al relativo oscuramento (…)»[77].

È inoltre previsto che «una volta trascorso il periodo di pubblicazione previsto dalle singole discipline di riferimento [es.: art. 124 del d. lgs. n. 267/2000] se gli enti locali vogliono continuare a mantenere nel proprio sito *web* istituzionale gli atti e i documenti pubblicati, ad esempio nelle sezioni dedicate agli archivi degli atti e/o della normativa dell'ente, devono apportare gli opportuni accorgimenti per la tutela dei dati personali. In tali casi, quindi, è necessario provvedere a oscurare nella docu-

---

[73] Per una lettura completa dell'ordinanza di ingiunzione nei confronti di Comune di Tivoli n. 209 del 7 novembre 2019 si v. doc. *web* n. 9269824.

[74] Il riferimento è all'art. 124, co. 1, d.lgs. 18 agosto 2000, n. 267 *(«Testo unico delle leggi sull'ordinamento degli enti locali»)*, ai sensi del quale «Tutte le deliberazioni del Comune e della Provincia sono pubblicate mediante affissione all'albo pretorio, nella sede dell'ente, per quindici giorni consecutivi, salvo specifiche disposizioni di legge».

[75] Il Garante nell'ordinanza lamenta la violazione del principio di liceità e di minimizzazione del trattamento [ai sensi dell'art. 5, par. 1, lett. *a)* e *c)*, del GDPR, nonché dell'art. 6, par. 1, lett. *c)* ed *e)*, par. 2 e par. 3, lett. *b)*, del GDPR], in quanto sono stati diffusi dati personali in assenza di un idoneo presupposto normativo (per il periodo eccedente i tempi di pubblicazione previsti dall'art. 124, comma 1, d.lgs. n. 267/2000) in violazione dell'art. 19, comma 3, del Codice al tempo in vigore.

[76] GPDP, Provv. n. 243 del 15 maggio 2014, doc. *web* n. 3134436.

[77] V. l'ordinanza di ingiunzione n. 209, datata 7 novembre 2019.

mentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati (…)»[78].

Il Garante è intervenuto anche in merito a trattamenti effettuati con dispositivi che permettono la geolocalizzazione di veicoli dati in dotazione ai dipendenti per l'esecuzione dell'attività lavorativa, ove il principio di minimizzazione ha trovato larga applicazione soprattutto sotto la vigenza del GDPR. Significativo è, a tal riguardo, il provvedimento del 28 giugno 2018, n. 396[79], reso a seguito di una segnalazione da parte di un dipendente di una società di "distribuzione e commercializzazione di impianti per saldatura e macchine per saldare" e della relativa assistenza ai clienti. Questi lamentava «un trattamento di dati personali a sé riferiti attraverso l'installazione da parte della società di un dispositivo GPS sull'autovettura aziendale, in assenza di una informativa o della comunicazione di una *policy* aziendale in merito all'esistenza ed alle caratteristiche essenziali del sistema di geolocalizzazione».

Il sistema di geolocalizzazione avrebbe permesso al datore di lavoro di raccogliere e trattare molteplici dati relativi alla posizione geografica del dipendente sia in orario di lavoro che fuori orario (trattandosi di veicoli aziendali affidati per un utilizzo promiscuo), oltre ai dati relativi alla velocità, alle ore di guida, alle pause effettuate, ecc.

Tali informazioni inoltre potevano essere consultate per un periodo complessivo di 365 giorni dalla loro raccolta.

All'esito dell'esame delle dichiarazioni rese dalla società all'Autorità nel corso del procedimento[80] e della documentazione acquisita, il Garante ha quindi ritenuto che «tali modalità del trattamento e, segnatamente, la raccolta di informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti cui i veicoli sono affidati, quali la ricostruzione su mappa dei percorsi effettuati sia in tempo reale che giornalmente, con ulteriore distinta ricostruzione anche per ciascuna tratta dei percorsi effettuati e delle relative modalità, comprese le pause, con una periodicità della rilevazione estremamente ravvicinata (ogni 120 secondi), non sono proporzionate con gli scopi rappresentati dalla società (v. artt. 11, comma 1, lett. *d)* del Codice e 5, par. 1, lett. *c)* del Reg. UE n. 679/2016) che potrebbero essere utilmente e legittimamente perseguiti con la raccolta di informazioni assai più limitate »[81].

---

[78] *Ibidem.*

[79] GPDP, Provv. n. 396 del 28 giugno 2018, doc. *web* n. 9023246.

[80] L'azienda, a sua difesa, ha dichiarato: *«a)* nello svolgimento della propria attività, (…) ha installato su furgoni aziendali, "atteso l'elevato valore dei macchinari trasportati", dispositivi di geolocalizzazione mediante sistema GPS; *b)* i furgoni aziendali dotati di tali dispositivi (…) rientrano ogni sera presso la sede (…) pertanto nessun controllo tramite sistemi di localizzazione avviene al di fuori dell'orario di lavoro"(…); *d)* le finalità perseguite sono logistiche ed organizzative (…), nonché volte a "garantire la sicurezza e l'incolumità dei lavoratori ed infine [a] prevenire e contrastare eventi criminosi ai danni dei beni aziendali" (…); *g)* i dati trattati "sono automaticamente registrati sul server del fornitore del servizio e cancellati decorsi 365 giorni mediante sovrascrittura dei dati più recenti"».

[81] *Ibidem.*

In sostanza, la società stessa, titolare del trattamento, avrebbe ben potuto perseguire le medesime finalità effettuando una minore raccolta di dati e garantendo un periodo di conservazione più breve.

L'utilizzo del sistema di geolocalizzazione in modalità standard, senza richiedere al fornitore l'aggiunta di alcuna modifica, è risultato essere in violazione dei principi di necessità, pertinenza e non eccedenza di cui al Codice in materia di protezione dei dati personali, nel testo antecedente alla riforma del 2018 [in relazione agli artt. 3 e 11, co. 1, lett. *d)* ed *e)*] e del principio di minimizzazione dei dati e di limitazione della conservazione di cui al GDPR [con riferimento all'art. 5, par. 1, lett. *c)* ed *e)*].

In applicazione dei principi e delle disposizioni del Regolamento, il sistema tecnologico avrebbe dovuto avere una configurazione tale da garantire il trattamento dei soli dati personali necessari con impostazione predefinita, per ogni specifica finalità del trattamento, giusto quanto richiesto anche dall'art. 25 GDPR.

Com'è evidente, il progresso tecnologico ha determinato una profonda connessione tra principio di minimizzazione e *data protection by design* e *by default*, così come emerge dal provvedimento in esame, che ha sancito la violazione contestuale dei principi di minimizzazione dei dati e della disposizione resa in materia di *privacy by default* [ai sensi degli artt. 5, par. 1, lett. *c)*, e 25 del GDPR] [82].

La sussistenza della citata correlazione è stata ribadita dal Garante anche in relazione a molti atti regolamentari e amministrativi di enti pubblici. Un interessante esempio è costituito dal parere n. 151 del 24 luglio 2019 in tema di videolotterie, con cui il Garante si è espresso in modo favorevole su «uno schema di decreto del Direttore dell'Agenzia delle dogane e dei monopoli in tema di regole tecniche per la produzione dei sistemi di gioco VLT»[83].

Si ricorda che in Italia l'accesso ai giochi d'azzardo è consentito solo ai giocatori maggiorenni e i terminali VLT[84], per procedere a questa iniziale verifica inerente l'età ed evitare così che i minorenni vi accedano illecitamente, richiedono sempre l'utilizzo della tessera sanitaria, documento che contiene tuttavia molte altre informazioni personali[85].

---

[82] Nel Provv. n. 396 del 28 giugno 2018, doc. *web* n. 9023246, il Garante ha ingiunto al titolare del trattamento di «configurare – in base al principio di *privacy by design* e *by default* – la versione *standard* dei servizi offerti attraverso il sistema di localizzazione con modalità proporzionate rispetto al diritto alla riservatezza degli interessati, in particolare con riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati ed alla messa a disposizione delle mappe dei percorsi effettuati».

[83] GPDP, parere n. 151 del 24 luglio 2019, doc. *web* n. 9126407.

[84] L'acronimo indica una nuova tipologia di apparecchi, le Videolotterie o *Videolottery* (VLT), nel settore dei giochi da divertimento e intrattenimento legali che sono connessi ad un sistema di gioco centrale e privi di "scheda di gioco" al loro interno. Tali sistemi utilizzano una tecnologia avanzata che consente migliori performance, più sicurezza per tracciabilità dei flussi, nonché un'offerta multipla di gioco, i principali sono giochi a rullo, e possibilità di vincite più elevate. Sono di fatto dei terminali di gioco, rientranti nel concetto di *Served Based Gaming* (SBG), collegati ad una rete e ad un sistema centrale (informazioni tratte dal sito www.sistemagiocoitalia.it).

[85] Tale previsione è stata disposta dall'art. 9-*quater* (rubricato «*Misure a tutela dei minori*»), del d.l. 12 luglio 2018, n. 87, conv. con mod. dalla l. 9 agosto 2018, n. 96, ai sensi del quale «1. L'accesso agli

L'Agenzia, durante le varie comunicazioni intercorse con il Garante, ha individuato nello schema misure rispettose sia del principio di minimizzazione che del principio di *privacy by design* e *by default*, prevedendo che le modalità di accertamento della maggiore età avvenga per mezzo dell'estrazione delle sole informazioni registrate nelle prime due tracce della banda magnetica della tessera sanitaria (codice fiscale ed identificativo della tessera) senza procedere alla successiva loro memorizzazione nelle banche dati del sistema di gioco VLT.

La memorizzazione dei dati non sarebbe infatti lecita in quanto eccedente rispetto alla finalità prefissata, che deve essere unicamente quella di verificare la maggiore età del giocatore ed impedire il gioco ai minorenni. Le modalità di trattamento individuate nello schema di decreto, nel perseguire le finalità indicate, erano tuttavia tali da rispettare il principio di minimizzazione dei dati.

3.2. Il principio di minimizzazione dei dati nella casistica delle Autorità di controllo degli altri Paesi membri dell'UE

In ambito europeo, anche le altre Autorità di controllo si sono pronunciate in materia di protezione dei dati e, nello specifico, nel rispetto del principio di minimizzazione.

Limitando l'analisi ad alcuni provvedimenti successivi al Regolamento UE n. 679/2016, si ricorda *in primis*, in riferimento alla tutela del principio di minimizzazione, la Delibera SAN-2020-003 resa dal Garante francese (CNIL, *Commission Nationale de l'Informatique et des Libertés*) il 28 luglio 2020, relativamente all'attività svolta dall'azienda Spartoo, rivenditore *online* in diversi territori europei con sede in Francia.

La procedura contestata, avendo quale oggetto il trattamento transfrontaliero dei dati personali, ha richiesto l'avvio della cooperazione europea, coordinata dalla CNIL in qualità di capofila.

L'azienda in esame aveva registrato e conservato, in modo integrale e permanente, le conversazioni telefoniche ricevute dai dipendenti del servizio clienti e i dati personali di questi ultimi, come indirizzi e coordinate bancarie. Nel memorizzare le coordinate bancarie dei clienti, aveva provveduto a criptarle solo parzialmente.

---

apparecchi di intrattenimento, di cui all'articolo 110, comma 6, lettere *a)* e *b)*, del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, è consentito esclusivamente mediante l'utilizzo della tessera sanitaria al fine di impedire l'accesso ai giochi da parte dei minori. Dal 1° gennaio 2020 gli apparecchi di cui al presente comma privi di meccanismi idonei a impedire ai minori di età l'accesso al gioco devono essere rimossi dagli esercizi. La violazione della prescrizione di cui al secondo periodo è punita con la sanzione amministrativa di euro 10.000 per ciascun apparecchio».

Successivamente, con l'art. 27, co. 4, del d.l. 28 gennaio 2019, n. 4, conv. con mod. dalla l. 28 marzo 2019, n. 26, è stato disposto che «In considerazione della previsione di cui all'articolo 1, commi 569, lettera *b)*, e 1098, della legge 30 dicembre 2018, n. 145, l'introduzione della tessera sanitaria prevista dall'articolo 9-*quater* del decreto-legge 12 luglio 2018, n. 87, convertito, con modificazioni, dalla legge 9 agosto 2018, n. 96, sugli apparecchi di cui all'articolo 110, comma 6, lettera *a)*, del Testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, deve intendersi riferita agli apparecchi che consentono il gioco pubblico da ambiente remoto».

Inoltre, per contrastare efficacemente i fenomeni dell'evasione e delle frodi telematiche, la società aveva raccolto e conservato copia della carta d'identità e della tessera sanitaria (quest'ultima soprattutto dei clienti italiani).

La CNIL, dopo un controllo effettuato presso la società titolare del trattamento[86], ha accertato che, nel caso di specie, v'è stata la violazione del principio di minimizzazione dei dati in quanto ha ritenuto eccessiva sia la registrazione completa e permanente delle telefonate ricevute dai dipendenti del servizio clienti, non necessaria per la finalità perseguita (la formazione dei dipendenti), sia la registrazione e la conservazione delle coordinate bancarie del cliente e, nell'ambito della lotta alle frodi telematiche, la raccolta in Italia di copie delle "tessere sanitarie" dei clienti.

L'Autorità francese ha contestato, unitamente ad altre violazioni, il venir meno del principio di minimizzazione, irrigando una sanzione complessiva di 250.000 euro[87].

Non meno attento a tale principio è stato il Garante rumeno che ha sanzionato Unicredit Bank per un importo di circa 130.000 euro all'esito di un'indagine iniziata nel mese di novembre 2018 e conclusasi alla fine del mese di giugno 2019[88]. La sanzione è stata applicata in quanto l'Autorità nazione di controllo avrebbe accertato che i dati relativi al CNP e all'indirizzo delle persone che effettuano i pagamenti a Unicredit Bank SA, tramite transazioni *online*, venivano comunicati al beneficiario dell'operazione, tramite moduli di estratto conto[89].

---

[86] Cfr. Deliberazione del collegio ristretto n. SAN-2020-003 del 28 luglio 2020: «*La formation restreinte relève, tout d'abord, que si certains clients s'opposent à l'enregistrement de l'appel téléphonique passé, la société met en en œuvre un traitement permettant d'enregistrer toutes les conversations téléphoniques de ses salariés, sans que ceux-ci aient la possibilité de s'y opposer. Ensuite, elle considère que la société ne justifie pas de la nécessité d'enregistrer l'intégralité des conversations téléphoniques passées par le service client, au regard de la finalité du traitement, à savoir la formation des salariés. La formation restreinte relève que la société indiquait, lors de l'audition du 19 juin 2019, que la personne chargée de cette formation n'écoute généralement qu'un enregistrement par semaine et par salarié. Par ailleurs, si la société a affirmé, lors de la séance du 28 novembre 2019, que le taux d'enregistrement des conversations téléphoniques est passé de 100% à 30%, elle ne produit sur ce point aucune pièce justificative. Si le nombre d'enregistrements peut varier en fonction de chaque salarié et des circonstances, en particulier des besoins de formation de celui-ci, la formation restreinte considère que la société ne démontre pas avoir mis en place, pour le passé et l'avenir, un enregistrement des conversations téléphoniques des salariés limité à ce qui est nécessaire au regard de la finalité poursuivie. Or, un responsable de traitement ne peut mettre en place un traitement de données à caractère personnel sans s'assurer que celui-ci est nécessaire à ses besoins, a fortiori lorsqu'il repose sur un dispositif particulièrement intrusif pour les salariés. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 5-1-c) du RGPD est constitué*».
Per un approfondimento consultare il testo completo in https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042203965/.

[87] L'Autorità francese, oltre alla violazione del principio di minimizzazione, ha ritenuto sussistere anche (i) una violazione dell'obbligo di limitare il periodo di conservazione dei dati [art. 5, lett. *e)*, del GDPR], (ii) una violazione degli obblighi di informazione ai sensi dell'art. 13 GDPR, poiché le informazioni sulla protezione dei dati dell'impresa non erano coerenti , infine, (iii) una violazione dell'obbligo di garantire la sicurezza dei dati personali e prevenire l'accesso di soggetti terzi non autorizzati ai sensi dell'art. 32 GDPR.

[88] Cfr. EDPB*, First fine by the Romanian Supervisory Authority*, 26 giugno 2019, https://edpb.europa.eu/news/national-news/2019/first-fine-romanian-supervisory-authority_it.

[89] Cfr. nota precedente.

All'Istituto bancario è stata contestata la mancata applicazione delle misure tecniche e organizzative di sicurezza volte ad attuare efficacemente i principi di protezione dei dati, quali la minimizzazione dei dati, e ad integrare le garanzie atte a soddisfare i requisiti del Regolamento e a tutelare i diritti degli interessati. L'Autorità di controllo ha sostenuto che l'attività di Unicredit ha violato gli art. 25 e 5 del GDPR e il *considerando* n. 78 dello stesso Regolamento[90].

Ancora, il Garante lituano ha sanzionato un istituto bancario[91] per le violazioni degli artt. 5, 32 e 33[92] del GDPR, ossia la violazione dei dati personali nel sistema del servizio di disposizione di ordine di pagamento. In riferimento all'art. 5 GDPR è stato accertato che MisterTango UAB aveva trattato (con operazioni di accesso e raccolta) più dati personali di quanto avesse indicato come necessari per l'effettuazione del pagamento avviato dal pagatore stesso.

Inoltre, la possibilità di visionare nel sito dell'istituto l'elenco dei pagamenti elaborati per più di due giorni, ha evidenziato un'inadeguata applicazione di misure tecniche e organizzative che consentirebbero di garantire un livello di sicurezza adeguato al rischio, inclusa la protezione contro il trattamento illecito, la divulgazione, quindi, in violazione degli artt. 5 e 32 del GDPR[93].

Una violazione del principio di minimizzazione è stata rilevata anche dall'Autorità danese per la protezione dei dati, che nell'ottobre del 2018 ha sanzionato la società Taxa 4×35 che offre un servizio di trasporti simile ad Uber[94].

La società, nel momento in cui un utente chiamava un "taxi", raccoglieva un'elevata quantità di dati (ad esempio il nominativo degli utenti, il numero di telefono, la data e l'ora di inizio e di fine del viaggio, i chilometri percorsi, il pagamen-

---

[90] A titolo meramente informativo si ricorda che a tale sanzione ne è seguita una seconda pari a 15.000 euro a seguito dell'istruttoria apertasi *post* notifica di *data breach* dell'ente bancario, che ha rilevato un accesso non autorizzato. Nello specifico, i dati personali dei clienti che si trovavano in formato analogico presso l'istituto bancario sono stati oggetto di violazione ad opera di terzi, in particolare sono stati fotografati da persone non autorizzate ad averne accesso e successivamente diffusi sulla rete, con ogni conseguente danno per gli interessati coinvolti.

[91] Le sanzioni sono state irrogate a MisterTango UAB, una società che opera a livello internazionale e fornisce servizi di pagamento ai residenti e alle società della Lituania, nonché ai residenti e alle società straniere. Tale società ha stabilito una filiale in Lettonia e ha fornito servizi in altri Paesi. Il testo del comunicato relativo al provvedimento, datato 21 maggio 2019, è consultabile al sito https://edpb.europa.eu/news/national-news/2019/first-significant-fine-was-imposed-breaches-general-data-protection_en.

[92] La violazione dell'art. 33 deriva dalla mancata notifica all'Autorità di controllo della violazione dei dati derivante dall'accesso non autorizzato ai dati visibili sul sito per più di due giorni (9-10 luglio 2018).

[93] Cfr. il testo del comunicato relativo al Provvedimento, datato 21 maggio 2019, consultabile *online* all'indirizzo https://edpb.europa.eu/news/national-news/2019/first-significant-fine-was-imposed-breaches-general-data-protection_en, ove si trova precisato che «*Thus, MisterTango UAB has failed to choose the appropriate technical or organisational measures which would help to ensure a level of security appropriate to the risk, including protection against unlawful processing, disclosure, thus, breaching Articles 5 and 32 of the GDPR*».

[94] Il testo del comunicato relativo al provvedimento («*The Danish Data Protection Agency proposes a DKK 1,2 million fine for Danish taxi company*») è consultabile al sito dell'EDPB all'indirizzo https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_it.

to, i dati di geolocalizzazione tramite GPS) che collegava alle relative informazioni fiscali dell'utente per determinare l'importo chiesto quale corrispettivo del servizio.

Nel corso dell'istruttoria è stato accertato, inoltre, che Taxa 4×35 conservava i dati personali dei clienti ben oltre il periodo di conservazione previsto dalla normativa in quanto i nomi e gli indirizzi dei clienti venivano cancellati dopo due anni di conservazione, secondo il periodo fissato per la *data retention*, ma i numeri di telefono dei clienti venivano mantenuti per altri tre anni, per un periodo complessivo di ben cinque anni.

A sua difesa Taxa 4×35 ha sostenuto l'impossibilità di eliminare i numeri di telefono dopo i due anni previsti dalle norme in quanto parti essenziali del proprio database informatico e di non violare tali principi perché tutti i dati venivano anonimizzati.

L'Autorità di controllo però non ha reputato fondata la giustificazione fornita dalla società, ritenendo che la difficoltà del sistema informatico di un'impresa non possa giustificare la grave violazione della riservatezza dei dati.

Insufficiente è stato ritenuto anche il processo di anonimizzazione dei dati adottato dall'azienda, che consisteva nel cancellare solo i nominativi degli utenti, in quanto tale tecnica avrebbe dovuto rendere impossibile la successiva identificazione degli interessati, resa invece possibile collegando le persone ai loro numeri di telefono conservati.

L'Autorità ha rimarcato l'importanza della violazione dell'art. 5, par. 1, lett. *c)* ed *e)* del Regolamento (rispettivamente principio di minimizzazione dei dati e di limitazione della conservazione) a causa della grande quantità e della qualità dei dati personali dei clienti (tra cui i numeri di telefono) che la società continuava a trattare senza averne effettivamente necessità.

Considerevole, pertanto, è stata la conseguente sanzione comminata di 1,2 milioni di corone, pari a circa 160 mila euro, equivalente a circa il 2,8% del fatturato annuale della società.

Il provvedimento del Garante danese costituisce anche un importante precedente sulla "debolezza" del tentativo di giustificare lunghi periodi di conservazione dei dati dovuti alle limitazioni organizzative delle infrastrutture IT dell'azienda, ormai non più giustificabile neanche alla luce dell'art. 25 GDPR in tema di *data protection by design* e *by default*.

3.3. Il principio di minimizzazione dei dati nella giurisprudenza della Corte di giustizia dell'UE

Anche la Corte di giustizia dell'UE, nel suo ruolo di «*human rights adjudicator*»[95], si è sofferma sul principio di minimizzazione dei dati.

Con la sentenza *Digital Rights Ireland* del 2014 [96], la Corte di giustizia ha dichiarato invalida la direttiva 2006/24/CE volta a realizzare l'armonizzazione delle

[95] De Búrca, *After The EU Charter of Fundamental Rights: The Court Of Justice As A Human Rights Adjudicator?*, in *Masst. J. Eur. & Comp. L.*, 2013.

[96] CGUE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*

disposizioni degli Stati membri in tema di conservazione di determinati dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione. La direttiva era dunque volta a garantire la disponibilità di tali dati per l'espletamento delle attività di indagine, accertamento e perseguimento di reati gravi, come in particolare i quelli relativi alla criminalità organizzata e al terrorismo. A tali fini, la direttiva prevedeva che i fornitori dei servizi di comunicazione elettronica dovessero conservare i dati relativi al traffico, i dati relativi all'ubicazione ed i dati necessari all'identificazione dell'abbonato o dell'utente.

La direttiva prevedeva dunque un obbligo generalizzato di conservazione dei predetti dati, con facoltà di accesso per finalità di repressione dei reati, considerato però dalla Corte eccessivamente in contrasto con i diritti fondamentali del rispetto della vita privata e della protezione dei dati personali[97].

La Corte infatti ha ritenuto che, «pur mirando a contribuire alla lotta contro la criminalità grave, la suddetta Direttiva non impone alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica e, in particolare, non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi»[98].

I dati devono pertanto essere «adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati»[99].

Un'altra significativa sentenza resa dalla Corte di giustizia e sul tema della *data retention* è quella relativa al caso Tele2 Sverige[100].

La Corte ha stabilito che è incompatibile con l'ordinamento europeo una norma dell'ordinamento nazionale di un Paese membro che preveda, «per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica» oppure che disciplini «la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso

[97] *Ibidem*, par. 65.
[98] *Ibidem*, par. 59.
[99] Cfr. art. 5, par. 4, lett. *c)*, della Convenzione n. 108+, nonché l'art. 5, par. 1, lett. *c)*, del GDPR.
[100] CGUE, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, Tele2 Sverige AB e a. Per un approfondimento si vedano L. Scaffardi, *Data retention e diritti della persona*, in *Costituzionalismo.it*, 2/2017; G. Tiberi, *Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla Data retention*, in *Quaderni Costituzionali*, 2, 2017, pp. 434 ss.; O. Pollicino-G.E. Vigevani, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza Tele2 Sverige della Corte di giustizia UE*, in *Forum di Quaderni Costituzionali*, 1, 2017.

ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione»[101].

Agli stessi Stati è consentito solamente una conservazione limitata – e non generalizzata – dei dati degli utenti, con lo scopo di contrastare atti di criminalità. È possibile effettuare una conservazione in casi circostanziati e limitatamente a quanto sia strettamente necessario in relazione alle diverse tipologie di dati da conservare, ai mezzi di comunicazione considerati, alle persone implicate e alla durata di conservazione. E si potrà accedere ai dati conservati solamente dopo un controllo preventivo da parte dell'Autorità giudiziaria o di un'Autorità indipendente[102].

La sentenza ha concluso quindi che la conservazione generalizzata dei dati è inammissibile perché altrimenti «porta alla conseguenza che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce la regola, quando invece il sistema istituito dalla Direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione»[103].

Entrambe le sentenze esposte hanno dato un importante contributo ad una graduale ridefinizione dei limiti delle ingerenze pubbliche nella sfera privata[104].

3.4. Il principio di minimizzazione dei dati nella giurisprudenza nazionale italiana e straniera

3.4.1. *Il principio di minimizzazione dei dati nella giurisprudenza della Corte di Cassazione*

Il principio di minimizzazione è spesso di ardua applicazione nel rapporto contrattuale tra professionisti e consumatori. Ancora più nel rapporto contrattuale tra banca e privati quando e soprattutto il trattamento avviene anche su dati particolari.

La Cassazione ha pertanto ritenuto opportuno pronunciarsi dettagliatamente sul tema al fine di risolvere le questioni palesatesi soprattutto in relazione al contemperamento del principio di minimizzazione con quello dell'autonomia contrattuale.

La Suprema Corte di Cassazione[105], a fine 2019, è intervenuta in un caso di recupero crediti (con ordinanza n. 34113 del 30 ottobre 2019, ma pubblicata il 19 dicembre 2019)[106], ribadendo il principio di minimizzazione stabilito dall'art. 5, par.

---

[101] L'argomento su cui poggia la Corte di giustizia fa leva sull'applicazione dell'art. 15, par. 1, della dir. 2002/58, come modificata dalla dir. 2009/136, interpretato alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE.

[102] CGUE, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, cit., par. 117-121.

[103] *Ibidem*, par. 104.

[104] E. Spiller, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, in *Ianus*, 2017, 15-16, pp. 279-302.

[105] Cass. civ., ord. n. 34113 del 2019.

[106] Nel 2012, il Tribunale di Napoli aveva comminato al Banco di Napoli una sanzione aggiuntiva pari a 5.000 euro per la violazione della *privacy*.

1, lett. *c)*, GDPR, che il titolare del trattamento è tenuto a seguire nella raccolta dei dati personali degli utenti.

Nello specifico una cliente del Banco di Napoli aveva lamentato la violazione «della normativa sulla *privacy* al momento della cessione del credito della Banca ad un privato. In particolare, la Banca ha segnalato la debitrice a soggetti privati acquirenti di crediti fornendo loro dati sensibili in ordine alla persona del debitore, alla situazione debitoria e all'abitazione della debitrice»[107].

La Corte di Cassazione ha ritenuto che non si possa contestare alla banca la violazione della disciplina in materia di protezione dei dati personali «solo perché abbia fornito ai soggetti acquirenti del credito informazioni riguardanti la debitrice funzionali alla cessione del credito, quali la situazione debitoria, ubicazione dell'immobile vincolato alla garanzia del credito»[108]. La Corte, pur rilevando il mancato assolvimento dell'onere probatorio sulla violazione del principio di minimizzazione dei dati nella comunicazione verso soggetti terzi, nell'ambito dell'operazione di cessione del credito, ha comunque ribadito «che il trattamento delle informazioni personali effettuato nell'ambito dell'attività di recupero crediti sia lecito purché avvenga nel rispetto del criterio di *minimizzazione* nell'uso dei dati personali, dovendo essere utilizzati solo i dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati»[109].

3.4.2. *Il principio di minimizzazione dei dati nella giurisprudenza della Corte Regionale di Bonn*

Altro significativo caso è stato invece affrontato dal giudice tedesco, che ha vagliato il principio di minimizzazione dei dati con riferimento alla corretta gestione dei protocolli della rete Internet, regolata dalle clausole contenute nel contratto, di rilevanza internazionale, che disciplina i rapporti tra l'ente destore dei nomi a dominio (ICANN) e i c.d. *Registrar*.

Il caso è stato sottoposto all'attenzione della Corte Regionale di Bonn in merito alla corretta applicazione del Regolamento sulle *policy* di raccolta dei dati relative al protocollo di rete che permette di individuare l'appartenenza di un determinato indirizzo IP ad un *Internet Service Provider* (ISP).

Il protocollo utilizzato dalla rete racchiude informazioni che possono far risalire all'intestatario dell'indirizzo IP, al periodo in cui è avvenuta la registrazione e ad altre informazioni. L'ente che dirige e attribuisce (attraverso *Registrar*) i nomi di dominio, gli indirizzi IP e segue la sicurezza della rete è l'ICANN[110].

La *querelle* portata all'esame della Corte di Bonn riguarda le clausole contrattuali per l'accreditamento di un *Registrar* tedesco presso l'ICANN.

---

[107] Cfr. Cass., ord. n. 34113 del 2019, cit.

[108] *Ibidem*.

[109] *Ibidem*.

[110] ICANN (*Internet Corporation for Assigned Names and Numbers*), ente non governativo fondato il 30 settembre 1998 in California, sotto contratto con il Dipartimento del Commercio degli Stati Uniti.

Secondo le *policy* dell'ICANN, il *Registrar* è tenuto a raccogliere i dati di contatto di tutti i soggetti che ricoprono i diversi ruoli tecnici. Il *Registrar*, essendo un amministratore di sistema tedesco, si è invece adeguato alle disposizioni contenute all'interno del GDPR, in particolare agli artt. 5, par. 1, lett. *c)*, e 25 del GDPR (principio di minimizzazione e adozione di misure tecniche e organizzative per assicurare la protezione dei dati personali sin dalla progettazione e per impostazione predefinita) rifiutando di raccogliere dati ulteriori.

La Corte di Bonn, con sentenza del 30 maggio 2018[111], ha accolto la dichiarazione del *Registrar* tedesco, ritenendo eccessivi i dati ulteriori pretesi dall'ICANN e sufficienti quelli raccolti durante la registrazione da parte del predetto *Registrar* in relazione allo scopo specifico da questi perseguito nei rapporti intrattenuti con l'ICANN. La stessa ha contestato pertanto all'ICANN il mancato rispetto del principio di minimizzazione, a cui occorre invece uniformarsi.

3.5. Riflessioni conclusive

In una società sempre più tecnologica, connotata da un aumento considerevole della circolazione dei dati in rete in cambio dei più svariati servizi e spesso utilizzati per altre finalità, non sempre espresse in modo chiaro, il principio di minimizzazione risulta essere una vera e propria barriera che mira a limitare l'acquisizione dei dati personali e, quindi, l'ulteriore trattamento, possibile fonte di rischi per la libertà e la dignità degli individui[112], alimentati dalla raccolta "bulimica", realizzata sempre più spesso nella prassi per poter trarre il massimo vantaggio mediante un numero infinito di «informazioni da informazioni»[113].

Risulta chiaro come le Autorità di controllo e le Corti europee siano allineati nel riconoscere l'importanza di una gestione dei dati volta a ridurre l'esposizione a rischi non necessari, rispetto alle finalità perseguite, durante le varie operazioni di trattamento (in specie nella fase della raccolta e della conservazione), improntata all'affermazione del principio di minimizzazione.

[111] Landgericht Bonn, 30 maggio 2018, documento n. 10 O 171/18.

[112] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al Nuovo Regolamento Europeo*, cit.

[113] Si veda *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU.*

Capitolo VII
Il principio di esattezza

*Francesco Avveduto - Carlo Basunti**

SOMMARIO: 1. Inquadramento normativo. – 2. Portata del principio. – 2.1. Il principio di esattezza: un'ipotesi ricostruttiva. – 2.2. Il principio di esattezza come baluardo a difesa dei diritti e degli interessi dell'interessato. – 2.3. Il principio di esattezza tra obblighi e interesse del titolare. – 2.4. L'esattezza dei dati nell'ambito dei diritti dell'interessato previsti dal GDPR. – 3. Applicazione del principio nella casistica. – 3.1. Il diritto di rettificare dati inesatti al vaglio della Corte di giustizia. Il caso dei documenti dei concorsi professionali e delle valutazioni dell'esaminatore. – 3.2. Il principio di esattezza nelle pronunce del Garante.

1. Inquadramento normativo

La tutela della vita privata e familiare di cui all'art 8 CEDU si è ramificata in varie forme di protezione, inclusa quella relativa alla protezione dei dati personali che, nelle sue diverse sfaccettature, declina anche il principio di *esattezza* dei dati per come oggi lo conosciamo e per come si trova contemplato nella normativa vigente[1].

---

* Pur essendo lo scritto frutto di riflessione comune, il par. 1 è da attribuire a Francesco Avveduto, i par. 2 e 3 sono da attribuire a Carlo Basunti.

[1] L'art. 8 CEDU contempla un generale diritto alla tutela della vita privata e familiare nei confronti di ingerenze pubbliche o private («Art. 8. *Diritto al rispetto della vita privata e familiare*. – 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui»), che reclama un bilanciamento con altri diritti fondamentali di pari rango. La Corte europea dei diritti dell'uomo ha interpretato tale diritto ricomprendendo nella sua tutela esigenze di protezione diverse, inclusa la tutela della riservatezza e dei dati personali, la tutela dell'immagine e del nome, la tutela dell'identità personale e, in particolare, la tutela dell'individuo alla rappresentazione veritiera delle vicende che interessano il soggetto. L'incidenza del diritto alla tutela della vita privata e familiare di cui all'art. 8 CEDU, come interpretato dalla Corte europea, non è stata immediata nel nostro ordinamento giuridico nazionale, né da parte del legislatore né da parte della giurisprudenza, che ha faticato a riconoscere il diritto alla riservatezza. Si pensi, ad esempio, alla celebre sentenza della Cass., n. 4487/1956, con riguardo alle vicende legate alla vita del celebre tenore Caruso, nei confronti delle quali i suoi eredi lamentavano l'illiceità della loro divulgazione, perché, anche se verificatesi al di fuori del domicilio, non avrebbero avuto diretto interesse per i terzi. Nel caso di specie tuttavia la S.C. si espresse sancendo che «chi non ha saputo o voluto tener celati i fatti della propria vita, non può pretendere che il segreto sia mantenuto dalla discrezione altrui; la curiosità ed anche un innocuo pettegolezzo, se pur costituiscono una manifestazione non elevata dell'animo, non danno luogo di per sé ad un illecito giuridico (…)», arrivando addirittura ad affermare che «(…) nell'ordinamento giuridico italiano non esiste un diritto

L'art. 5, par. 1, lett. *d)*, del Reg. (UE) 2016/679 (GDPR), nel sancire che i dati debbano essere «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza")», pone in evidenza l'importanza riservata dal legislatore alla "qualità" del dato personale come fondamento per la tutela dei diritti del soggetto[2]. Di fatto, solo salvaguardando la qualità delle informazioni, con riguardo all'esattezza delle stesse, è possibile assicurare che l'interessato sia reso incolume dal pregiudizio derivantegli da una falsa rappresentazione di sé o da altri aspetti, di natura personalistica o patrimonialistica, che lo riguardano.

Una prima importante tappa dell'evoluzione normativa che, a livello internazionale, ha reso evidente l'acquisita consapevolezza del principio di esattezza dei dati si ha con l'emanazione della *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* n. 108 del 28 gennaio 1981, con la quale – presa coscienza della sempre più rilevante mole di dati in circo-

alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto». Successivamente, una diversa sensibilità giuridica sulle nuove esigenze di protezione della sfera privata e, più recentemente, l'esponenziale aumento della mole di dati in circolazione ha portato a più recenti pronunce in cui si evidenzia la declinazione del diritto alla tutela della vita privata anche quale diritto alla *esatta* rappresentazione dell'individuo in elementi quali il nome e la sua immagine che compongono la sua identità che il singolo ha diritto a determinare e ad ottenere la giusta tutela. Si tratta di una nozione ampia, elaborata dapprima dalla giurisprudenza della Corte di Strasburgo, che consente, dunque, di includere numerosi aspetti dell'identità di un individuo (in tal senso cfr. M.G. PUTATURO DONATI, *Il diritto al rispetto della «vita privata e familiare» di cui all'art. 8 della CEDU, nell'interpretazione della Corte Edu: il rilievo del detto principio sul piano del diritto internazionale e su quello del diritto interno*, in *Europeanrights.eu*, articolo consultabile all'url http://www.europeanrights.eu/public/commenti/Commento_Putaturo.pdf visitato da ultimo in data 7 aprile 2023. Sul punto si vedano altresì le pronunce della Corte di Strasburgo ivi segnalate, tra le quali la sent. 5 dicembre 2013, sez. V, *Henry Kismoun contro Francia*, in tema di cambiamento del cognome e del nome delle persone fisiche, nonché la sent. 7 febbraio 2012, Grande Camera*, Von Hannover contro Germania*).
Più di recente la Corte EDU ha ribadito la portata di tale tutela che, giova dirlo, prescinde dalla lesione del diritto all'onore, dovendosi tenere a monte conto della necessità del diritto alla corretta rappresentazione del soggetto nel suo complesso ed in ogni aspetto della sua personalità (cfr., in tal senso, la decisione della Corte EDU del 21 febbraio 2017, *Rubio Dosamantes c. Espagne*, in tema di bilanciamento tra libertà di espressione e tutela della vita privata e familiare. La ricorrente lamentava la mancata tutela del proprio diritto innanzi all'autorità giudiziaria riguardo alla legittimità di dichiarazioni rese dal produttore della cantante, che aveva rivelato aspetti relativi alla presunta omosessualità della donna e ad una relazione affettiva ormai conclusasi. I giudici spagnoli avevano rigettato la domanda ritenendo che in tale vicenda non fosse rinvenibile una lesione all'onore della cantante. La Corte Edu ha invece ritenuto sussistente una violazione dell'art. 8 per non avere le Corti spagnole adempiuto al proprio obbligo positivo di protezione della vita privata della ricorrente). L'evoluzione del sistema di protezione della vita privata e familiare di cui all'art. 8 CEDU, giunto progressivamente a ricomprendere anche la tutela della persona contro una falsa rappresentazione della propria identità, ha portato alla progressiva affermazione del principio di esattezza, tutelato ora anche nell'ambito della puntuale disciplina in materia di protezione dei dati personali.

[2] Si veda anche il *considerando* n. 39 del GDPR, nella parte in cui prevede che «è opportuno adottare tutte le misure ragionevoli affinché i dati *inesatti* siano rettificati o cancellati».

lazione già nella società del tempo – si volle realizzare una prima tutela concreta con riguardo alle persone interessate dal trattamento[3], prevedendo espressamente, all'art. 5, che «I dati a carattere personale oggetto di elaborazione automatica devono essere (…) *d)* esatti e, se necessario, aggiornati (...)»[4]. L'esattezza del dato rimane strettamente interconnessa con il principio di finalità, liceità e correttezza, poiché solo se il dato è esatto è possibile raggiungere il fine del trattamento, giustificando l'interferenza con la sfera privata del soggetto interessato; solo se il dato è esatto è possibile considerare il trattamento come lecito e corretto, perché svolto consentendo di avere una rappresentazione attendibile e non adulterata dell'identità personale dell'interessato[5]. L'esattezza del dato, ovviamente, incide anche su altri aspetti, non essendo confinabile al solo connotato dell'identità personale, come ben si comprende, a mero titolo esemplificativo, se si pensa all'esattezza dei dati delle movimentazioni bancarie nei conti correnti, in difetto della quale si hanno rischi di compromissione dei diritti patrimoniali o, ancora, all'esattezza dei dati di una cartella clinica, in difetto della quale sono evidenti i rischi sulla salute: si tratta dunque di diritti della personalità (quello alla vita e alla salute), diversi dal diritto all'identità personale. L'esattezza del dato, così come in generale l'intera disciplina sulla protezione dei dati personali, mantiene la sua vocazione ad essere precondizione per l'esercizio di altri diritti dell'individuo a cui i dati medesimi si riferiscono.

Tale consapevole interconnessione del principio di esattezza con quelli di finalità, liceità e correttezza del trattamento è stata la chiara ispirazione del legislatore comunitario nella redazione della dir. 95/46/CE (c.d. Direttiva Madre), da cui ha avuto origine la legislazione degli Stati membri in ambito del trattamento dati personali. Si legge infatti, all'art. 6, che «Gli stati membri dispongono che i dati personali devono essere (…) *d) esatti* e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati». Si tratta di un articolo che compone la Sezione I del Capo II del citato provvedimento comunitario, significativamente dedicata ai «*Principi relativi alla* qualità *dei dati*».

L'attenzione posta dal legislatore europeo sulla "qualità" del dato – ed in particolare sul connotato di esattezza – ha influenzato ovviamente gli ordinamenti nazionali, in occasione dell'emanazione della normativa di recepimento. Evidenza di ciò si ha già nella l. 31 dicembre del 1996 n. 675[6], la quale, nel proprio *incipit*, esordiva

---

[3] Già in quel contesto identificate dall'art. 2, lett. *a)*, come persona fisica identificata od identificabile cui sono riferibili i dati personali fatti oggetto del trattamento.

[4] *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* n. 108 del 28 gennaio 1981, art. 5.

[5] Così P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione de dati personali*, Milano, 2003, I, pp. 455-460, dove nello specifico si rivolge l'attenzione al caso della tutela della identità in ambito giornalistico. In tali circostanze, infatti, la centralità della qualità della informazione data regge sulle proprie spalle la bontà dell'intero trattamento, perché da essa deriva la censurabilità o meno della condotta di chi diffonde una notizia.

[6] L. n. 675 del 31 dicembre 1996 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (testo consolidato con il d.lgs. 28 dicembre 2001, n. 467) (Pubblicato sulla Gazzetta

dichiarandosi come volta, tra l'altro, alla garanzia della tutela della riservatezza e dell'identità personale[7] ed, all'art. 9 (rubricato «*Modalità di raccolta e requisiti dei dati*»), dettava alcuni requisiti qualitativi dei dati oggetto di trattamento, con lo scopo di assicurarne la completezza, l'esattezza, l'aggiornamento e la non eccedenza rispetto alla finalità perseguita[8].

Anche nel nostro ordinamento, il principio di esattezza dei dati appare il frutto di un lento processo di sedimentazione normativa, dato che è possibile rinvenirlo anche in altri contesti, diversi da quello specificamente previsto in tema di *data protection*. Si pensi al d.p.r. n. 600/1973, al cui art. 33 si rinveniva una facoltà per gli uffici delle imposte, in caso di fondati sospetti sulla inesattezza dei dati, di disporre le opportune verifiche. Si pensi, ancora, alla l. n. 1/1991 («*Disciplina dell'attività di intermediazione mobiliare e disposizioni sull'organizzazione dei mercati mobiliari*») che all'art. 25 (rubricato «*Offerta e commercializzazione di servizi o prodotti informatici o telematic*i») faceva esplicito riferimento alla necessità che i dati fossero «veritieri»[9].

In materia di protezione dei dati personali, la completezza del dato e la conseguente esattezza dello stesso vanno considerate nell'ottica della finalità del trattamento di cui il dato medesimo è fatto oggetto. Infatti, non in astratto, ma in maniera direttamente e strettamente collegata con il contesto in cui il trattamento viene effettuato, sarà necessario calibrare l'attenzione volta alla completezza del dato, non potendosi, a titolo meramente esemplificativo, obbligare il titolare del trattamento ad acquisire anche notizie e dati ulteriori ed eccedenti rispetto a quelli necessari per l'attività di trattamento e le finalità della stessa[10].

Ufficiale n. 5 dell'8 gennaio 1997, Suppl. Ordinario n. 3).

[7] Cfr. art. 1, co. 1, della l. 675/96 cit., che, con riguardo alle finalità, prevedeva espressamente che «la presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale».

[8] L'art. 9, co. 1, della l. 675/96 cit. prevedeva, testualmente, che «i dati personali oggetto di trattamento devono essere: *a)* trattati in modo lecito e secondo correttezza; *b)* raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi; *c) esatti* e, se necessario, aggiornati; *d)* pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; *e)* conservati in una forma che consenta l´identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati».

[9] La l. n. 1/1991 cit. – successivamente abrogata dal d.lgs. 58/1998, T.U.I.F.) – prevedeva espressamente, all'art. 25, co. 1, che «l'offerta o la commercializzazione di servizi, realizzati mediante strumenti informatici e telematici, aventi per oggetto la diffusione al pubblico di dati concernenti i corsi, le quantità scambiate, le condizioni di domanda ed offerta relative alle negoziazioni di valori mobiliari trattati nei mercati regolamentari ai sensi della presente legge, sono soggette ad autorizzazione da parte della Consob. La Consob può negare o revocare l'autorizzazione qualora ritenga che, in relazione alle modalità di acquisizione ed elaborazione dei dati ovvero alla natura ed ai fini del servizio offerto o commercializzato, sussista il rischio che i dati stessi non siano *veritieri* ovvero siano tali da *indurre in errore i destinatari*».

[10] Sulla importanza dell'attenzione alla *qualità* dei dati si veda G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, pp. 265-270. Sempre sulla rilevanza della *qualità* del dato si veda anche G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 116-118, che pone l'attenzione sulle normative che regolamentano il trattamento

È con il codice della *privacy* (d.lgs. 196/2003) che il legislatore italiano compie un significativo passo in avanti verso la riorganizzazione sistematica dell'intera disciplina interna in materia di protezione dei dati personali, tenendo conto anche degli orientamenti giurisprudenziali e delle decisioni rese dal Garante per la *privacy* in tale materia. L'avvento del predetto codice non ha però modificato – nella forma e nella sostanza – quanto già previsto nella l. n. 675/96, rimanendo invariata, anche nella codificazione di inizio millennio, la formula usata dal legislatore nazionale nel recepire l'obbligo di mantenere i dati «esatti» ed «aggiornati», conformemente a quanto previsto dall'art. 6 della dir. 95/45/CE: quest'ultimo stabilisce che i dati debbano essere esatti e se necessario aggiornati e che devono essere prese tutte le misure ragionevoli necessarie affinché possa essere mantenuta tale esattezza; il codice della *privacy* nella sua versione originale del 2003 prevede all'art. 11, lett. *e)*, che i dati debbano essere «esatti e, se necessario aggiornati», riprendendo in maniera letterale la previsione dell'art. 9, lett. *c)*, dell'abrogata l. 675/96.

Il legislatore italiano, sia con la l. 675/1996 sia con il d.lgs. 196/2003 (codice in materia di protezione dei dati personali), in cui tale legge è confluita, ha voluto prevedere non solo l'obbligo di adozione di misure minime di sicurezza (art. 15, co. 2, l. 675/96 e art. 33 d.lgs. 196/2003, anteriforma del 2018), assistito da sanzioni penali, ma anche l'obbligo di adozione di misure "adeguate" (art. 15, co. 1, l. 675/96 e art. 31 d.lgs. 196/2003), finalizzate, tra l'altro, al mantenimento dell'*esattezza* dei dati personali nella dinamica dello svolgimento delle attività di trattamento.

Con il Reg. UE 679/2016 (GDPR) viene ripreso il fondamentale concetto di "adeguatezza" delle misure per il mantenimento della esattezza dei dati, già presente nella dir. 95/46 (senza alcuna specifica previsione di sanzioni penali per la mancata adozione di misure "minime" di sicurezza), viene esplicitato il principio di "esattezza" all'art. 5 (che da "requisito" del dato diviene "principio" a cui informare il trattamento) ed, altresì, viene affermato il nuovo principio di "responsabilizzazione" o *accountability* (in forza del quale il titolare del trattamento è tenuto ad adottare misure tecniche ed organizzative per garantire e per dimostrare la corretta applicazione dei principi in materia di protezione dei dati personali, ivi incluso il principio di esattezza)[11]. Viene così in rilievo, in maniera uniforme per tutti gli altri ordinamenti

dei dati da parte di soggetti pubblici, evidenziando l'importanza dell'attenzione alla esattezza e completezza dei dati anche in tale contesto. Si pensi alla l. n. 35/1999 che all'art. 3, co. 3, prevedeva un obbligo per l'ente pubblico di effettuare una verifica periodica della esattezza dei dati, completezza e necessità rispetto alle finalità del trattamento, al fine di assicurare la pertinenza e non eccedenza dei dati rispetto al trattamento. Si pensi ancora al CAD, d.lgs. 235/2010, in cui si prevede per le amministrazioni di aggiornare tempestivamente gli archivi al fine di evitare una falsa rappresentazione dell'individuo e le conseguenze pregiudizievoli che da ciò potrebbero derivare allo stesso.

[11] Cfr. artt. 5, par. 2, e 24 del Reg. UE 679/2016. Sulla rilevanza dell'*accountabillity* si veda G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 12 ss.; sul ruolo del principio di esattezza in prospettiva dinamica e della proporzionalità delle misure da adottare M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 208-213. Sul principio di *accountability* si veda anche, nel presente volume, il Capitolo XIII.

dei Paesi membri dell'UE, una nuova prospettiva della protezione dei dati personali nell'ottica della *accountability*, per la quale l'esattezza dei dati diventa fondamentale in quanto punto di contatto dei vari principi su cui si fonda la normativa stessa sul trattamento dei dati: l'esattezza del dato presuppone e impone l'adozione di adeguate misure tecniche e organizzative di sicurezza, incluse quelle che delineano efficaci procedure di gestione dei dati.

Con l'entrata in vigore del Reg. UE 679/2016 e, successivamente, con la sua effettiva applicazione (stabilita a far data dal 25 maggio 2018), s'è avvertita la necessità di riformare gli strumenti normativi interni e internazionali, per coordinarli con la nuova disciplina dell'UE.

Così, con il d.lgs. n. 108/2018 s'è avuta la riforma del codice in materia di protezione dei dati personali, dal quale sono stati espunti i riferimenti sia all'obbligo di esattezza e aggiornamento dei dati – in quanto previsti nel principio di esattezza di cui all'art. 5, par. 1, lett. *e)*, del GDPR – sia all'obbligo di adozione di misure di sicurezza adeguate volte a garantire (anche) l'esattezza stessa dei dati personali oggetto di trattamento – perché già previsto nelle più articolate norme del GDPR, che impongono, su diversi livelli di operatività, l'adozione di adeguate misure tecniche e organizzative (cfr. artt. 24, 25 e 32 GDPR).

Sul versante internazionale, invece, l'applicazione del Reg. UE 679/2016, unitamente all'evoluzione sociale e tecnologica, ha portato il Consiglio d'Europa ad aggiornare anche la citata Convenzione n. 108 del 1981, con la previsione di un protocollo addizionale del 18 maggio 2018 (c.d. Convenzione 108+), che l'Italia ha provveduto a ratificare con l. 22 aprile 2021 n. 60. Il nuovo testo della Convenzione conserva sul punto una immutata previsione: all'attuale art. 5, par. 4, lett. *d)* della Convenzione 108+, così come nell'originario art. 5, par. 1, lett. *d)*, della Convenzione 108 del 1981, si trova stabilito che «*Personal data undergoing processing shall be* (…) *accurate and, where necessary, kept up to date*». Cambia tuttavia il contesto in cui ora detto obbligo si inserisce, in quanto l'art. 5 viene ad essere arricchito di ulteriori paragrafi che trascendono il solo riferimento alla "qualità" dei dati, inserendo l'esattezza dentro un quadro normativo ben più vasto, in cui diviene evidente anche un più stretto collegamento con i principi di liceità, proporzionalità e finalità del trattamento[12].

[12] L'originario art. 5, rubricato «*Quality of data*», stabiliva che «*Personal data undergoing automatic processing shall be*: a) *obtained and processed fairly and lawfully*; b) *stored for specified and legitimate purposes and not used in a way incompatible with those purposes*; c) *adequate, relevant and not excessive in relation to the purposes for which they are stored*; d) *accurate and, where necessary, kept up to date*; e) *preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*». L'attuale art. 5 della Convenzione 108+, riscritto a seguito del protocollo modificativo del 2018, è ora rubricato «*Legitimacy of data processing and quality of data*» e in esso si trova ora stabilito che «1. *Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.* 2. *Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.* 3. *Personal data undergoing processing shall be processed lawfully.* 4. *Personal data undergoing processing shall be*: a) *processed fairly and in a transparent manner*; b) *collected*

2. Portata del principio

2.1. Il principio di esattezza: un'ipotesi ricostruttiva

Il principio di esattezza – nonostante i limitati contributi che lo hanno interessato, che tendono perlopiù a porlo in endiadi con altri principi, trattandolo solo incidentalmente ed in maniera unicamente connessa all'analisi di taluni diritti dell'interessato – riveste, in realtà, un ruolo tutt'altro che marginale nell'alveo dei principi del trattamento dei dati personali, che rappresentano il «denominatore comune minimo di garanzia»[13] posto alla base della normativa *privacy*. L'esiguità delle analisi dedicate a tale principio da parte degli studiosi è probabilmente dovuta alla presunta (ma forse, almeno in parte, fuorviante) semplicità, nonché al suo essere autoesplicativo: del resto, come ha affermato l'*Information Commisioner's Office* (ICO), «*it will usually be obvious whether personal data is accurate*»[14].

Posto che i dati trattati devono essere "esatti" affinché il trattamento possa considerarsi lecito, e che il parametro dell'esattezza di un dato può variare in base al contesto[15], ci si deve domandare, in mancanza di una puntuale definizione da parte del legislatore, quando tali dati rispettino il principio in esame. E questo, prendendo le mosse da una definizione che se ne può dare sul piano interpretativo, in via di prima approssimazione, quale principio che sancisce l'obbligo di assicurare la ragionevole precisione e correttezza dei dati, trattati in rapporto diacronico con la realtà e con riferimento al contesto in cui il trattamento dei dati si inserisce. Ne consegue che il principio di esattezza, nel guidare l'operato del titolare del trattamento, impone un obbligo di «fedeltà contenutistica»[16] dei dati che vengono trattati così da garan-

for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes; c) *adequate, relevant and not excessive in relation to the purposes for which they are processed*; d) *accurate and, where necessary, kept up to date*; e) *preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed*».

[13] Così G. Buttarelli, *Banche dati e tutela della riservatezza*, cit., p. 9.

[14] Così si esprime l'*Information Commisioner's Office* (ICO) – l'autorità di controllo britannica – in merito al principio di esattezza (*accuracy* per utilizzare il lemma anglosassone) in una *Guide to the GDPR*. La guida, riferita al principio in esame, è rinvenibile al seguente *link*: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/*.

[15] Sottolinea come un dato possa essere considerato «*entirely accurate and sufficient*» in un contesto e, invece, «*wholly incomplete and misleading*» in un altro A.R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, in *Mich. Law Rev*., 1969, p. 1115.

[16] In questi termini si esprime M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., p. 210 in cui l'A. paragona il principio di esattezza a quello di minimizzazione dei dati e sottolinea come da questi principi derivi il dovere del titolare, al fine di tutelare l'interessato, di controllare costantemente la «corrispondenza del contenuto dei dati in suo possesso alla realtà dagli stessi rappresentata».

tire, almeno tendenzialmente, il minimo livello di interferenze nella sfera giuridica dell'interessato.

A parere di chi scrive, pare potersi enucleare una triplice declinazione dell'esattezza: (a) da un lato, sotto il profilo oggettivo, il principio si riferisce al dato in sé, richiamando quindi la qualità e l'accuratezza del dato stesso; (b) dall'altro, in una declinazione soggettiva, si riferisce al compito incombente sul titolare del trattamento (sulla scorta del principio di *accountability*)[17] di provvedere ad una puntuale verifica dei dati trattati, anche senza la necessità di una precipua richiesta da parte dell'interessato o dell'autorità Garante; (c) infine, in una declinazione funzionale, il principio di esattezza appare configurabile in chiave prodromica all'esercizio di alcuni diritti da parte dell'interessato tra i quali spiccano sicuramente il diritto di limitazione del trattamento *ex* art. 18 GDPR ed il diritto di rettifica *ex* art. 16 GDPR.

Con riguardo al primo aspetto tratteggiato (a), pare opportuno sottolineare che se è vero che, al pari di un dato errato, un dato parziale potrebbe considerarsi inesatto (rendendo così inesatto e quindi illecito il trattamento posto in essere), altrettanto vero è che il dato, laddove sovrabbondante, rischia di porsi in contrasto con quanto sancito all'art. 5, par. 1, lett. *b)* e *c)* del GDPR, in riferimento alla limitazione delle finalità e al principio di minimizzazione. Si dovrà, pertanto, ricercare il più corretto bilanciamento, caso per caso, tra la non eccedenza rispetto alle finalità (determinate, esplicite e legittime) del trattamento e la presenza di un livello sufficiente di completezza tale da permettere il raggiungimento di dette finalità.

Il secondo profilo (b) ha, invece, riguardo al soggetto che, con valutazioni rigorose, deve occuparsi del necessario bilanciamento emerso *sub* (a). Nel nuovo assetto delineato dal GDPR, ricade nella discrezionalità e sotto la responsabilità del titolare del trattamento l'obbligo, ai fini dell'esattezza dei dati, di assicurarsi di trattare dati esatti, che possiedano le caratteristiche della qualità e della completezza, adottando inoltre, eventualmente e in modo tempestivo, tutte le misure che appaiono ragionevoli per cancellare o rettificare i dati inesatti.

L'ultima direzione in cui sembra si muova ed in cui pare quindi potersi inquadrare il principio di esattezza (c) fa riferimento ai casi in cui l'interessato agisca nei confronti del titolare quando quest'ultimo abbia trattato dati inesatti. Il *data subject* potrà infatti richiedere la rettifica dei dati inesatti (o la loro integrazione laddove incompleti) come pure la cancellazione o la limitazione del trattamento. Si nota come in quest'ultima accezione l'(in)esattezza dei dati rappresenti la condizione (o una delle condizioni) affinché l'interessato possa esercitare un suo diritto riconosciuto dal Regolamento.

Il principio di esattezza, nella cui essenza è rinvenibile un'eco del criterio di verità dell'informazione, deve essere rigorosamente rispettato proprio per garantire una piena tutela alla persona cui i dati trattati si riferiscono. I dati personali, strettamente legati alla persona umana, concorrono a formarne l'identità virtuale ed il di-

[17] Il principio di *accountability*, una delle innovazioni più significative del GDPR, rappresenta un vero e proprio cambio di paradigma in ambito *privacy*, sul tema si rinvia a G. FINOCCHIARO, *Il principio di* accountability, in *Giur. it*., 2019, 12, pp. 2778 ss., nonché al capitolo dedicato al principio di *accountability*, nel presente volume.

ritto alla loro protezione risulta, sotto vari aspetti, «cangiante nel tempo»[18]. Le ripercussioni negative che l'interessato può subire nel caso in cui i suoi dati siano inesatti possono, del resto, essere soggette ad un esponenziale aggravio dovuto alla possibile combinazione con ulteriori informazioni anch'esse inesatte, unite alle prime e trattate ad un tempo, eventualmente, con l'ausilio dei moderni sistemi automatizzati[19].

2.2. Il principio di esattezza come baluardo a difesa dei diritti e degli interessi dell'interessato

In questo quadro, emerge l'inscindibile legame che unisce il principio di esattezza con il diritto all'identità personale dell'interessato che deve essere garantito (anche e soprattutto) attraverso un rigoroso rispetto del principio in esame. Come già storicamente affermato dalla Corte di Cassazione, ogni individuo ha «interesse a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale»[20]. Il diritto all'identità personale deve pertanto essere inteso come il «diritto di essere sé stessi»[21], il diritto alla propria identità attraverso la quale la persona si rappresenta liberamente con i propri principi, le proprie idee e la propria storia. In altri termini, il diritto a non vedere travisato, offuscato o contestato ciò che il soggetto esprime e rappresenta.

È quindi la proiezione sociale di ogni soggetto – determinante appunto per la sua identità personale – ad essere minata a causa di una circolazione di dati inesatti. Seguendo l'incontrovertibile pensiero di autorevole dottrina, «il diritto all'identità personale comporta una corretta rappresentazione della personalità del soggetto. La

[18] In questo senso G. Alpa, *La "proprietà" dei dati personali*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 18.

[19] Sul punto vedi E. Navarretta, *Art. 11: Modalità del trattamento e requisiti dei dati*, in C. M. Bianca-F. D. Busnelli (a cura di), *La protezione dei dati personali, Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, Padova, 2007, p. 268, in cui l'A. afferma: «il singolo dato (…) è come la tessera di un complesso mosaico, la cui costruzione, affidata alla mente dell'operatore e alle connessioni informatiche, può facilmente sfuggire allo specchio della realtà».

[20] Il riferimento è alla celebre pronuncia Cass., 22 giugno 1985, n. 3769, tra le altre in *Foro it*., 1985, 1, cc. 2211 ss., relativa al c.d. caso Veronesi: il noto oncologo aveva rilasciato una intervista in cui spiegava il nesso tra il fumo ed alcuni tumori maligni, specificando che alcune sigarette "*light*" potevano avere ripercussioni meno severe, ma concludendo comunque affermando come «tutto sarebbe più semplice se la gente si convincesse a non fumare»; in seguito a ciò una società produttrice di tabacco iniziò a pubblicizzare i propri prodotti "*light*" affermando che secondo il prof. Veronesi tali sigarette riducessero sostanzialmente il rischio di cancro; detta sentenza era stata preceduta dall'altrettanto nota pronuncia Pret. Roma, 6 maggio 1974, tra le altre in *Giur. it.*, 1975, 1, 2, pp. 514 ss., con nota di D'Angelo, relativa alla vicenda di un uomo ed una donna che avevano visto una loro immagine (prodotta in un contesto del tutto estraneo) essere utilizzata in un manifesto per la propaganda del Comitato nazionale per il referendum sul divorzio senza alcuna autorizzazione; su entrambe le pronunce, ed in generale sul percorso giurisprudenziale che ha consacrato il diritto all'identità personale cfr. V. Zeno Zencovich, *Identità personale*, in *Dig. disc. priv*., 1993, p. 294 ss., spec. pp. 297 ss.

[21] Sul punto v. G. Alpa, *Il diritto di essere se stessi*, Milano, 2021; in questi termini già Corte cost., 3 febbraio 1994, n. 13, tra le altre in *Giust. civ*., 1994, 1, p. 2435 che parla dell'identità personale come «diritto ad essere sé stesso».

mancata o infedele rappresentazione integra una lesione del diritto»[22], e ciò a prescindere dal fatto che la falsa rappresentazione del soggetto implichi una connotazione "in negativo", dal momento che la semplice inesattezza in sé causa una lesione del diritto.

Il diritto all'identità personale quale prisma di elementi che compongono l'io di un determinato individuo, inteso come autonomo diritto della personalità «trovato»[23] dal diritto oggettivo e tutelato dalla clausola a fattispecie aperta di cui all'art. 2 Cost.[24], pare richiedere, in concreto ai fini della sua tutela, un comportamento attivo del titolare del trattamento che deve assicurarsi di trattare dati esatti e rispondere celermente ad eventuali segnalazioni da parte dell'interessato, proprio per non travisare la proiezione sociale della persona i cui dati vengono trattati.

Tale diritto esplica la sua importanza in forza della sua natura relazionale: i terzi in buona fede che si rapportano con il soggetto titolare del diritto devono considerarlo come è o come, anche idealmente, ritiene di essere. Ogni persona deve quindi potersi presentare all'esterno nel rispetto della identità (o delle identità) con cui ha deciso di mostrarsi, indossando anche, magari, diverse "maschere" in diversi contesti ed assumendo così differenti identità, come del resto ci suggerisce anche l'etimologia greca del termine "persona", *pròsopon*, il cui significato è anche (e primariamente) quello di "maschera".

Proprio la massiccia circolazione dei dati in rete, nuovo scenario dell'agire umano e nuovo contesto in cui l'individuo sviluppa la sua personalità, rischia di danneggiare la persona nella più vulnerabile delle sue proiezioni, quella digitale[25] nel caso in cui non si prevedano misure idonee a garantire l'esattezza delle informazioni in tutte le loro vicende circolatorie. L'identità digitale è particolarmente esposta proprio perché relativa all'esplicazione della persona su Internet dove, come è noto, è assai arduo eliminare determinate informazioni una volta diffuse, nonostante il tempo le abbia, eventualmente, rese non più attuali e non corrispondenti all'identità aggiornata del soggetto cui si riferiscono.

Il tempo gioca, infatti, un ruolo cruciale per l'identità personale di ognuno, destinata, appunto, a mutare senza rimanere staticamente relegata ad un preciso momento storico[26]. L'esattezza del dato è strettamente collegata alla sua attualità e contestualizzazione: un dato non attuale non potrà certo essere considerato esatto.

---

[22] Così G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Dig. disc. priv. agg.*, 2010, p. 726; analogamente F. GALGANO, *Trattato di Diritto civile*, vol. I, Padova, 2015, pp. 191 s. afferma: «il diritto all'identità personale è leso anche se le azioni o convinzioni attribuite al soggetto non sono di per sé disonorevoli e lesive della sua reputazione».

[23] La fortunata espressione è di F. GALGANO, *Trattato di Diritto civile*, *supra cit*., p. 171 in cui l'Autore sostiene che vi siano «diritti soggettivi che si dicono 'trovati' dal diritto oggettivo: sono i diritti dell'uomo, che si considerano esistenti indipendentemente da ogni norma giuridica che li riconosca e che il diritto oggettivo si limita a garantire».

[24] Sull'art. 2 Cost. quale norma a fattispecie aperta cfr. A. BARBERA, *Commento all'art. 2 Cost*., in G. BRANCA (a cura di), *Commentario alla Costituzione italiana*, Bologna, 1975, spec. pp. 96 ss.

[25] In questo senso M. TAMPIERI, *L'identità personale: il nostro documento esistenziale*, in *Eur. dir. priv*., 2019, 4, p. 1223.

[26] Sul punto v. G. ALPA, *Il diritto di essere se stessi*, cit., p. 229 in cui l'Autore sottolinea «l'evoluzione della personalità nel corso del tempo, e il graduale mutamento dell'immagine e dell'identità

Se in passato, la società si preoccupava di preservare la propria storia, la propria memoria e le proprie informazioni attraverso la scrittura o la diffusione orale di notizie, oggi la situazione appare ribaltata, dal momento che lo sviluppo tecnologico, e soprattutto l'avvento di Internet, ha reso sempre più difficile dimenticare, obbligando, spesso anche contro la volontà degli interessati, al ricordo. Tra le problematiche che emergono nella c.d. società dell'informazione è sicuramente presente quella relativa alla contestualizzazione delle informazioni: il terreno dal quale è sorto il diritto all'oblio.

Senza volere, in questa sede, analizzare il diritto all'oblio nella sua evoluzione legislativa (si ricorda che solo con il GDPR il diritto all'oblio ha conosciuto una puntuale previsione all'art. 17) e nel dibattito dottrinale e giurisprudenziale, incentrato sul difficile bilanciamento tra diritto di informazione e di cronaca da un lato e diritto alla protezione dei dati personali e alla riservatezza dall'altro, basti sottolineare come tale diritto risulti di primaria importanza affinché l'identità personale dell'interessato, nel costante divenire che la caratterizza, sia fedelmente rappresentata all'esterno. Si fa quindi riferimento al rapporto tra fatti che, seppur realmente accaduti e lecitamente diffusi nella loro esattezza, devono essere relegati nel passato di un soggetto e avvenimenti più recenti che hanno alterato la situazione pregressa. Il diritto all'oblio non rappresenta, in realtà, un nuovo diritto della personalità: si tratta infatti di un diritto funzionale e strumentale alla realizzazione e all'esercizio di altri consolidati diritti, quali il diritto all'identità personale e quello alla protezione dei dati personali[27]. Esso permette quindi di evitare che l'identità di un soggetto venga travisata ed opera, per così dire, in concerto con il principio di esattezza affinché l'identità personale dell'interessato venga tutelata da un punto di vista diacronico, nei mutamenti che la riguardano.

Il principio di esattezza, relativo ai dati pubblicati in rete, anche in rapporto al diritto all'oblio, non pare però potersi spingere al di là di quello che può essere ragionevolmente richiesto ai gestori degli archivi *online*, nei quali le notizie (esatte al momento della pubblicazione) sono contenute. Posto infatti che le informazioni devono certamente rispettare, tra gli altri, il principio di esattezza ed essere aggiornate nel momento in cui vengono immesse in rete, l'esigenza di un costante aggiornamento di tali informazioni (per la tutela dell'identità dell'interessato) deve essere proporzionalmente bilanciata con i costi e gli sforzi ragionevolmente richiedibili ai gestori degli archivi. A differenza di quanto sembrava affermare la Corte di Cassazione[28],

"ideale" di ogni persona»; Id., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impr*., 2017, 3, pp. 723 ss.; e G. Finocchiaro, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inf*., 2012, 3, spec. p. 389 in cui l'Autrice afferma: «la persona è ciò che è in un determinato momento storico e l'identità muta col tempo. Divengono essenziali la storicizzazione e la contestualizzazione. Eventi occorsi in una certa epoca possono non corrispondere più alla personalità di un soggetto in un diverso momento storico»; Id., *Identità personale (diritto alla)*, cit., spec. p. 735.

[27] In questo senso, cfr. G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf*., 2014, 4-5, pp. 600 ss.

[28] Cass., 5 aprile 2012, n. 5255, tra le altre in *Resp. civ. e prev*., 2012, 4, pp. 1147 ss.; e sulla quale vedi la ricostruzione operata da G. Alpa, *Il diritto di essere se stessi*, cit., pp. 233 ss.

non pare potersi richiedere al gestore di un archivio *online* un costante impegno di ricerca, indirizzato a qualsivoglia ulteriore informazione che rappresenti un aggiornamento di notizie pubblicate precedentemente, al fine di attualizzarle e contestualizzarle così da renderle aderenti alla attuale identità del soggetto interessato[29]. Non sembra, infatti, che si possa chiamare a rispondere un soggetto che, una volta pubblicata una notizia, non vi abbia successivamente (ricercato e) inserito il riferimento ad eventuali fatti sopravvenuti che abbiano reso la notizia a monte non più attuale. Va da sé che laddove l'interessato richiedesse l'aggiornamento o la cancellazione di una determinata notizia perché non più attuale e lesiva della sua identità, nonché priva di un pubblico interesse, il titolare dell'archivio dovrà, previa valutazione della fondatezza dell'istanza ricevuta, impegnarsi in tal senso. Analogamente, nel caso in cui si intendano pubblicare ulteriori informazioni sulla medesima vicenda, mutata nel tempo, o, più semplicemente ripubblicare la questione in sé (anche se, in realtà, nel mondo digitale è difficile parlare di una vera e propria "ripubblicazione" dato che, come si è detto, la rete difficilmente dimentica)[30], ci si dovrà adoperare affinché le notizie siano esatte e quindi, certamente, attuali e contestualizzate. Richiederebbe parimenti un intervento del gestore dell'archivio il caso in cui lui stesso si accorgesse di un'inesattezza a monte della notizia pubblicata: si tratterebbe però in questo

[29] Diverse sono state le voci critiche con riferimento ad un simile obbligo imposto sui gestori di archivi *online*, cfr. F. DI CIOMMO-R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e resp*., 2012, 7, pp. 701 ss., e spec. a p. 704 s. in cui gli Autori affermano che una simile soluzione non terrebbe in considerazione «i notevoli costi che la gestione di un sistema del genere richiederebbe, oltre che le oggettive difficoltà tecniche di realizzazione di una banca dati che, dunque, deve essere costantemente aggiornata e si deve alimentare di notizie che non è nemmeno detto siano inserite nel circuito informativo in cui "pesca" il suo gestore», aggiungendo che «il problema è di carattere più generale. Pensare che ognuno debba, a pena di responsabilità civile ed eventualmente penale, organizzare i propri archivi *on-line* in modo tale da renderli sempre aggiornati all'attualità vuol dire, per un verso, postulare una missione davvero impossibile, per l'altro trascurare la realtà della rete Internet»; M. BELLANTE, *Diritto all'identità personale e obbligo di aggiornamento degli archivi storici di testate giornalistiche*, in *Giur. it*., 2013, 5, pp. 1073 ss.; G. CITARELLA, *Aggiornamento degli archivi* online *tra diritto all'oblio e rettifica «atipica»*, in *Resp. civ. e prev*., 2012, 4, pp. 1155 ss., spec. p. 1159 in cui, secondo l'A. «garantire il rispetto dell'identità personale negli archivi *on-line* aperti al pubblico dei quotidiani, apportando aggiornamenti che scolorano nella rettifica, fino al limite della cancellazione e quindi dell'oblio, finisce per imporre agli editori una serie di problemi realmente insormontabili, e prima ancora comporta rilevanti conseguenze giuridico/sistematiche»; C. SCARPELLINO, *Contorsionismi del diritto all'oblio e criticità degli archivi* on line, in *Danno e resp*., 2020, 3, pp. 405 ss. la quale, pur commentando la decisione del Trib. Venezia, 26 settembre 2019, richiama criticamente la citata pronuncia della Corte di Cassazione; *contra* A. DI MAJO, *Il tempo siamo noi…*, in *Corr. giur.*, 2012, 6, pp. 769 ss., spec. p. 771 secondo cui «non sembra infatti fondato né convincente distinguere le due operazioni (pubblicazione della notizia e sua permanenza nell'archivio) (…). Va ribadito ancora una volta che la collocazione in un sito, destinato alla memoria storica, non può costituire impedimento acché la memoria da esso custodita, e a cui si accede via internet, subisca tutti i limiti e condizioni che incontra il "trattamento" dei dati personali, (…). Ancora una volta si viene a sezionare artificialmente un fenomeno che è unitario e la cui sezionabilità non può costituire una cortina fumogena, tale da far dimenticare che l'elemento da salvaguardare è pur sempre il diritto della persona acché il governo dei suoi "dati" corrisponda ai valori ad essa immanenti».

[30] Sull'argomento, cfr. G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, cit., pp. 391 s.

caso di un'azione richiesta al titolare non per un aggiornamento, ma per correggere l'informazione primigenia, sulla base dell'obbligo legale inscritto nel principio di esattezza, rafforzato dall'operatività del principio di *accountability*.

Se infatti da un lato, una informazione completa e vera in origine, successivamente non aggiornata, diviene «parziale e non esatta, e pertanto sostanzialmente non vera»[31], dall'altro non si può richiedere a colui che ha pubblicato tale informazione o a chi gestisce l'archivio in cui tale notizia è conservata, uno sforzo che, se non impossibile, appare di sicuro eccessivamente oneroso. I costi che deriverebbero da un obbligo di aggiornamento imposto *tout court*, ai fini del rispetto del principio di esattezza, in capo a chi pone a disposizione degli utenti uno strumento conoscitivo, verrebbero poi riallocati sugli utenti stessi.

A quanto detto, si aggiunga che il principio di esattezza presenta importanti ricadute anche su interessi e diritti ulteriori rispetto a quello all'identità personale.

Si pensi, ad esempio, ai dati contenuti all'interno delle cartelle cliniche: se tali dati fossero inesatti, il personale medico dedito alla cura del paziente-interessato non si ritroverebbe nelle condizioni di porre in essere le terapie corrette ed adeguate alla cura di cui il soggetto è bisognoso. Emergerebbe, in una simile fattispecie, un rischio per il diritto alla salute, finanche per la vita della persona.

Già nel 2015, il Garante per la protezione dei dati personali aveva pubblicato delle Linee guida relative ai *dossier* sanitari[32]. L'autorità Garante, pienamente consapevole della delicatezza dei dati sanitari, muove dall'esigenza di garantirne l'esattezza, l'integrità e la disponibilità. Nel settore in questione, del resto, oltre ai profili di responsabilità inerenti alla protezione dei dati personali, assumono rilievo gli aspetti relativi alla responsabilità deontologica e professionale. È quindi senz'altro presente un dovere, particolarmente incisivo data l'assolutezza dei diritti della persona che si rischia di ledere, in capo al titolare del trattamento: quello di garantire l'esattezza e l'aggiornamento dei dati sanitari, adottando ogni misura idonea a ridurre il rischio di cancellazione, manipolazione o estrapolazione dei dati.

L'esattezza del dato non rileva però unicamente nell'ambito dei diritti fondamentali della persona, ma anche con riguardo a diritti e interessi patrimoniali dell'interessato. Mi riferisco in particolar modo ai dati relativi ai conti correnti, alle movimentazioni bancarie e, più in generale, ai rapporti sussistenti tra gli istituti bancari e la clientela, anch'essi oggetto di Linee guida del Garante per la protezione dei dati personali[33]. Così, nell'esecuzione di ordini di pagamento, spetterà alla banca del debitore-interessato verificare l'esattezza dei dati trattati relativi alle coordinate bancarie e al conto corrente, mettendo in atto, in caso di dubbio, incongruenza o discordanza, adeguati controlli preventivi, contattando direttamente il cliente prima di eseguire un pagamento (eventualmente non dovuto) a carico dell'interessato.

Si aggiunga poi la rilevanza rivestita dal principio di esattezza con riferimento ai dati immessi nei sistemi di autenticazione biometrici, finalizzati all'accesso a

[31] Così Cass., 5 aprile 2012, n. 5255, cit.

[32] GPDP, Provv. 4 giugno 2015, doc. *web* n. 4091542; in argomento, di recente, cfr. GPDP, Provv. 15 dicembre 2022, doc. *web* n. 9870788.

[33] GPDP, Provv. 25 ottobre 2007, doc. *web* n. 1457247.

dispositivi, sistemi informatici, locali o ambienti fisici e così via. Tali sistemi che si basano sull'intelligenza artificiale si nutrono, per loro natura, di dati e tali dati devono essere esatti. L'importanza di immettere dati esatti in tali sistemi è finalizzata a contenere il più possibile l'indice FAR (*False Acceptance Rate*) con cui si misura la frequenza con la quale viene permesso un accesso non autorizzato; l'indice FRR (*False Rejection Rate*) con cui si misura la frequenza con la quale il sistema autorizza utenti il cui accesso non doveva, invece, essere autorizzato; e l'indice FIR (*False Identification Rate*) con cui si misura la frequenza con la quale il sistema riconosce l'utente, ma lo associa ad un'altra identità. Se solo idealmente tali indici possono essere pari a zero, in presenza di un sistema biometrico sostanzialmente perfetto, nella realtà, risulta comunque fondamentale diminuirli massimamente e, sul punto, l'esattezza dei dati alla base del sistema gioca un ruolo fondamentale.

Si aggiunga che, a maggior ragione alla luce delle concorrenti istanze di tutela poste alla base del GDPR, l'esattezza dei dati assume rilievo non solo ai fini della tutela della persona dell'interessato, dei suoi diritti ed interessi, ma anche per garantire un corretto funzionamento del mercato dei dati nel suo insieme[34].

2.3. Il principio di esattezza tra obblighi e interesse del titolare

Nonostante si tratti di un principio dalle origini ormai risalenti, le cui radici affondano nella Risoluzione (73) 22 del Consiglio d'Europa[35], è proprio nel contesto attuale, caratterizzato da un ampio utilizzo delle nuove tecnologie, capaci di permettere (o, talvolta, causare) una massima diffusione delle informazioni nella rete, che l'esattezza dei dati assurge a principio fondamentale della *data protection law*.

Si deve infatti ribadire che i recenti sviluppi della tecnologia presentano un margine di rischio particolarmente più elevato nel caso in cui i dati siano inesatti: la raccolta massiva di dati porta, infatti, a profili minuziosamente dettagliati, ma non sempre in linea con il principio di esattezza (oltre che con gli altri principi contenuti nel GDPR). Sebbene l'infinita mole di dati che i moderni sistemi permettono di raccogliere e trattare non rappresenti nemmeno un costo di particolare rilievo per i

[34] In questo senso, cfr. N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla* privacy, in ID. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 92 in cui l'Autrice afferma che: «è evidente, a titolo indicativo, che se i dati di carattere personale sono inesatti, non è leso solo il diritto della persona fisica a cui i dati si riferiscono, ma anche il corrispondente mercato risulta falsato».

[35] Si ricorda che il principio di esattezza veniva già menzionato dal *Council of Europe* nella *Resolution (73) 22 On the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies*, nella quale, all'art. 1, si legge «*the information stored should be accurate e and should be kept up to date*». L'importanza di mantenere una buona qualità dei dati, dato l'elevato rischio di danno presente nel trattamento dei dati personali viene anche sottolineato nell'*explanatory report* della Risoluzione. Di un solo anno successivo è il *Privacy Act of 1974* degli Stati Uniti in cui si rinvengono vari riferimenti all'*accuracy* dei dati; con riferimento a questa ultima fonte normativa e alle radici americane del principio di qualità dei dati v. T. HOEREN, *Big Data and Data Quality,* in ID., B. KOLANY-RAISER (a cura di), *Big Data in Context. Legal, Social and Technological Insights*, Cham, 2018, pp. 3 ss.

titolari[36], allo stato dell'arte, sorgono spesso problemi relativi alla (mancata) analisi e verifica dei dati raccolti che si traduce poi in ricadute qualitative sul trattamento effettuato. In altri termini, nonostante la quantità di dati disponibile sia attualmente sconfinata (anzi, forse proprio anche per questa ragione), tali dati necessitano di un adeguato processo di *data mining* e di una puntuale analisi, al fine di evitare distorsioni. Si pensi, ad esempio, alle *fake news*, a dati relativi ad insolvenze per crediti contestati che possono incidere sulla qualificazione di un soggetto come cattivo pagatore[37], come pure alla gestione dei profili reputazionali[38], in grado di determinare importanti pregiudizi sui diritti fondamentali dell'interessato e, in generale, incidere negativamente sulla sua sfera giuridica da un punto di vista sociale, lavorativo, etc.

Nell'odierna società, calata nel contesto della c.d. *data driven economy*, in cui sempre più spesso i dati personali, come è noto definiti il "nuovo petrolio", assumono un ruolo preminente nel contesto delle imprese che ne sfruttano sempre più sapientemente le potenzialità, il principio di esattezza esplica la sua centralità.

A livello europeo, è ormai chiaro il potenziale economico che lo sfruttamento dei dati personali racchiude ed anzi, tende ad essere sempre più incentivato, come dimostra, tra le altre, la Comunicazione della Commissione europea, intitolata «Strategia europea per i dati»[39]. Il valore economico dei dati personali ed il loro utilizzo nel mondo degli affari non devono indurre a sgretolare la «convinzione che l'essere umano sia e debba rimanere l'elemento centrale»[40]: non pare infatti corretto qualificare i dati personali come «"beni giuridici" in senso tecnico, quale "merce" che forma oggetto di commercializzazione, rimanendo pur sempre attributi della personalità, sui quali è possibile l'esercizio di diritti, anche nel senso di un uso di carattere patrimoniale»[41]. Proprio in questa direzione, il principio di esattezza rappresenta una

[36] Cfr., J. Chen, *The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle*, in *Eur. Data Prot. Law Rev*., 2018, 1, p. 40.

[37] F. Bravo, *I sistemi privati di informazione creditizia*, in G. Conte (diretto da), *Arbitrato Bancario e Finanziario*, Milano, 2021, pp. 229 ss.

[38] Con particolare riguardo ai sistemi che si offrono di elaborare i profili reputazionali di persone fisiche e giuridiche in modo da arrivare ad un vero e proprio *rating*, cfr. Cass. ord., 25 maggio 2021, n. 14381, in *Dir. inform*., 2021, 6, pp. 1001 ss., sulla quale cfr. il commento di F. Bravo, Rating *reputazionale e trasparenza dell'algoritmo. Il caso «Mevaluate»*, *ivi*, pp. 1005 ss.; per la ricostruzione della vicenda cfr. Gpdp, Provv. 24 novembre 2016, doc *web* n. 5796783; e successivamente l'impugnazione cui è seguita la pronuncia Trib. Roma, 4 aprile 2018, in *Dir. inform*., 2019, 2, pp. 520 ss., con nota di G. Giannone Codiglione.

[39] Commissione europea, *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Una strategia europea dei dati*, Bruxelles, 19 febbraio 2020, COM (2020) 66 final.

[40] *Idem*, p. 5.

[41] Così, condivisibilmente, F. Bravo, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impr. Eur*., 2021, 1, p. 14; in giurisprudenza sul tema v. Tar Lazio, 10 gennaio 2020, nn. 260 e 261 e le serrate critiche avanzate da F. Bravo, *La «compravendita» di dati personali?*, in *Dir. Internet*, 2020, 3, pp. 521 ss.; nonché Cass., 2 luglio 2018, n. 17278, tra le altre in *Giur. it*., 2019, 3, pp. 530 ss., con nota di S. Thobani, i cui risvolti vengono ampiamente affrontati da F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impr*., 2019, 1, pp. 34 ss.; e su cui sia anche consentito il rinvio a C. Basunti, *La (perduta) centralità del*

condizione affinché il titolare ne possa sfruttare al meglio il potenziale economico e, al contempo, un presidio che permette all'interessato di tutelarsi da rappresentazioni distorte della sua personalità e da altri pregiudizi anche di carattere patrimoniale.

Il dato, per acquisire importanza per il titolare e per essere quindi da lui utilizzato in chiave economica, deve essere necessario e finalizzato allo scopo da perseguire, come pure esatto e pertanto capace di fornire all'impresa tutte quelle informazioni utili ad instaurare una relazione *lato sensu* "personalizzata" tra impresa/titolare e soggetto interessato, quale possibile cliente. Si deve infatti tener ben presente che non è (solo) la quantità di dati che una impresa possiede e tratta, ma (anche e soprattutto) la loro qualità ed esattezza a rendere tali dati un *asset* strategico per operare sul mercato.

Il titolare del trattamento ha, pertanto, un assoluto interesse a trattare dati esatti, specialmente nell'ambito della profilazione dei soggetti (utilizzata prevalentemente per finalità di *marketing* che mirano a creare proposte commerciali mirate sui singoli consumatori). Tale interesse deve però rapportarsi, da un lato, con la pletora di dati disponibile al giorno d'oggi che caratterizza l'era dei *Big Data* (e quindi con la difficoltà di "estrarre" dati esatti) e, dall'altro, con l'eventualità che un soggetto fornisca (consapevolmente o inconsapevolmente) dati inesatti. Sotto quest'ultimo aspetto, oltre all'evidente contrasto con i principi di correttezza e buona fede relativi alla "cessione" (di un consenso al trattamento) di dati inesatti, si deve sottolineare come il titolare del trattamento, una volta scoperta l'inesattezza dei dati in questione sia tenuto ad intervenire, rettificandoli o cancellandoli. Il titolare non può, infatti, essere chiamato a trattare (consapevolmente) dati inesatti, essendo tenuto al rispetto dei principi di esattezza e *accountability*. Egli risulterebbe, quindi, responsabile nel caso in cui trattasse dati che ha riconosciuto essere inesatti, anche laddove lo facesse in seguito ad una specifica richiesta dell'interessato in tal senso. L'interessato potrà, tutt'al più revocare il consenso prestato (art. 7, par. 3 GDPR) ed il titolare dovrà interrompere ogni operazione di trattamento (senza pregiudizio per le operazioni effettuate prima della revoca), sempre che non sussista una condizione di liceità alternativa al consenso, e quindi non basata sulla volontà dell'interessato, su cui fondare il trattamento.

Il principio di esattezza rappresenta un obbligo che il titolare è tenuto a rispettare e che supera l'eventuale interesse del *data subject* al trattamento di dati inesatti sul suo conto perché a lui più congeniali. Una differente impostazione condurrebbe del resto ad inaccettabili ricadute di sistema: in tema di solvibilità del debitore; in materia fiscale; in ambito giudiziario; in materia assicurativa; con riguardo alle banche dati per la valutazione del merito creditizio[42]; con riferimento all'obbligo

consenso nello specchio delle condizioni di liceità del trattamento dei dati personali, in *Contratto e impr*., 2020, 2, spec. pp. 886 ss.

[42] In argomento cfr. F. BRAVO, *I sistemi privati di informazione creditizia*, cit., pp. 229 ss.; F. BRAVO, *La centrale di allarme interbancaria (CAI) e la centrale dei rischi (CR)*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, cit., pp. 265 ss.; R. DI RAIMO, *Accesso al credito e valutazione del merito creditizio*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, cit., pp. 211 ss.; A.A. DOLMETTA, *Disciplina di trasparenza e principio di trasparenza*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, cit., pp. 193 ss.

di verità oggettiva che, nel diritto di cronaca si somma al dovere di utilità sociale dell'informazione e continenza dell'esposizione dei fatti[43] e così via.

Al fine di evitare pericolose derive soggettivistiche del trattamento dei dati personali, risulta di massima importanza che il titolare del trattamento operi nel pieno rispetto del principio di esattezza (rafforzato da quelli di *accountability* e correttezza) per essere *compliant* con la normativa *privacy* e per raggiungere più efficacemente le proprie finalità di natura (anche) economica.

2.4. L'esattezza dei dati nell'ambito dei diritti dell'interessato previsti dal GDPR

Il principio di esattezza, *rectius*, il mancato rispetto di tale principio è, per l'interessato, il fondamento che consente l'esercizio di taluni diritti riconosciutigli dal Regolamento, e precisamente l'inesattezza del dato viene richiamata all'art. 16 GDPR sul diritto di rettifica; la contestazione dell'esattezza del dato si rinviene all'art. 18 GDPR inerente al diritto di limitazione di trattamento; e rileva inoltre nell'art. 17 GDPR sul diritto alla cancellazione (o all'oblio). Si tratta di diritti definibili come "dinamici", in quanto permettono all'interessato di intervenire sul trattamento posto in essere[44]. Tale dinamicità, propria della tutela, è necessaria per salvaguardare, come si è detto, i diritti fondamentali della persona come il diritto all'identità personale (diritto altrettanto dinamico che richiede una fedele rappresentazione del soggetto all'esterno e la correzione di eventuali rappresentazioni distorte)[45] o il diritto alla salute (si pensi al menzionato tema della gestione dei dati contenuti nelle cartelle cliniche), ma anche diritti di carattere patrimoniale (come ad esempio quelli inerenti alla correttezza delle operazioni bancarie ed ai conti correnti).

Precisamente, l'art. 16 del Regolamento sancisce il diritto dell'interessato di «ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo» (tale diritto alla rettifica si rinviene anche all'art. 8, par. 2, della Carta di Nizza) nonché «il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa».

Proprio tale diritto all'integrazione rappresenta una novità del Regolamento rispetto alla normativa previgente dal momento che la direttiva 95/46/CE prevedeva

---

[43] Sul punto il riferimento è alla nota decisione della Cass., 18 ottobre 1984, n. 5259, tra le altre in *Giur. it*., 1985, 1, pp. 1099 ss. che contiene una sorta di decalogo per il giornalista nell'esercizio del diritto di cronaca; sul tema cfr. per tutti M. Franzoni, *Dalla colpa grave alla responsabilità professionale*, Torino, 2017, pp. 175 ss.

[44] Cfr. F. Calisai, *I diritti dell'interessato*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 344.

[45] Cfr. A. Ricci, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove leggi civ. comm*., 2019, 3, p. 593 che afferma: «si potrebbe, semplificando, affermare che i diritti dell'interessato consentono alla persona di invocare una più generale pretesa all'esatta rivelazione della propria identità» e sottolinea come «attraverso il riconoscimento dei diritti dell'interessato si dà attuazione ai principi di base che ispirano la disciplina in materia di trattamento dei dati personali, così da poter conformare le attività poste in essere ai diritti e alle libertà fondamentali della persona».

semplicemente giusta l'art. 12, lett. *b)*, il diritto alla rettifica, alla cancellazione o al congelamento dei dati nei casi di incompletezza o inesattezza dei dati, senza appunto menzionare (almeno esplicitamente) alcuna possibilità di integrazione[46].

Il diritto di rettifica è esercitabile dall'interessato nei confronti del titolare – che si potrà poi, eventualmente, avvalere di responsabili o altri soggetti – in modo gratuito, ma, nel caso in cui la richiesta sia manifestamente infondata o eccessiva, in particolare per la ripetitività della stessa, il titolare potrà addebitare all'interessato un ragionevole contributo per le spese di carattere amministrativo e finanche rifiutare la richiesta (art. 12, par. 5, GDPR). Inoltre, l'inadempimento del titolare è soggetto ad una sanzione fino a venti milioni di euro e, per le imprese, fino al 4% del fatturato annuo dell'esercizio precedente laddove superiore [art. 83, par. 5, lett. *b)*, GDPR].

La rettifica riguarda, si è detto, dati inesatti, ma l'inesattezza deve far riferimento, come ha indicato l'*European Data Protection Supervisor* (EDPS), a dati oggettivi e fattuali, non a giudizi e valutazioni di carattere soggettivo che, ontologicamente, non possono essere fattualmente inesatte[47]. L'EDPS ha anche provveduto a tipizzare determinate fattispecie particolarmente significative per il diritto di rettifica (selezioni per assunzioni di personale, procedure di valutazione, dati di carattere medico-sanitario, procedure amministrative e disciplinari, *blacklisting* e *asset freezing*), indicando i limiti e le modalità di esercizio del diritto[48].

Pare corretto evidenziare come il diritto di rettifica e aggiornamento rappresenti per l'interessato una mera libertà e non un obbligo, come invece è per il titolare

---

[46] Dà conto di questa innovazione A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, p. 403 in cui l'A. sottolinea che, in effetti, «l'integrazione poteva, vigente la Direttiva, considerarsi implicita nel diritto alla rettifica, il cui esercizio di fatto si traduce in un intervento sui dati, giustificato dalla perdita di attualità dei dati medesimi, e finalizzato a colmare l'inesattezza che, in generale, si manifesta in un'assenza di qualità dell'informazione».

[47] Cfr. EDPS, *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data*, del 25 febbraio 2014, p. 18; v. anche sul punto GRUPPO DI LAVORO EX ART. 29, *Guidelines on the implementation of the Court of Justice of the European Union judgment on the "Google Spain and Inc. v. Agencia Española de protección de datos (AEPD) and Mario Costeja González" C-131/12*, p. 15. Sull'applicabilità del principio di accuratezza alle opinioni cfr. D. HALLINAN-F. ZUIDERVEEN BORGESIUS, *Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle*, in *Int. Data Privacy Law*, 2020, 1, pp. 1 ss.

[48] Cfr. EDPS, *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, supra cit.,* pp. 19-20 in cui, precisamente, con riferimento alle procedure di assunzione del personale, si sottolinea che una volta spirati i termini per l'invio delle domande, il diritto di rettifica è limitato ai soli dati inerenti ai criteri di ammissibilità (limitazione necessaria per la correttezza della procedura); con riferimento alle procedure di valutazione, si afferma che non possono essere sottoposte a rettifica le valutazioni soggettive fatte da un superiore in un *report* di valutazione, laddove ogni altro dato oggettivo e fattuale (come il nome) può essere rettificato; con riferimento ai dati di carattere medico-sanitario, stante la difficoltà di valutare esattezza e correttezza di tali dati, il diritto di rettificarli è in un certo qual modo limitato: si riconosce pertanto all'interessato il diritto di integrare la documentazione aggiungendo ulteriori opinioni mediche; con riferimento alle procedure amministrative, viene data all'interessato la possibilità di aggiungere suoi commenti al fascicolo disciplinare per assicurarne la completezza; con riferimento ai meccanismi di *blacklisting*, si sottolinea come il diritto alla rettifica abbia un'importanza chiave per garantire la qualità dei dati trattati, connessi al diritto di difesa.

del trattamento sia qualora gli venga richiesto dall'interessato sia qualora si renda conto lui stesso del difetto di esattezza del dato. Il titolare ha infatti un obbligo legale di intervento (che appunto discende dal principio in esame unito a quello di *accountability*) laddove si accorga che i dati da lui trattati siano inesatti, e questo anche senza preventiva richiesta dell'interessato come pure contro la sua eventuale volontà contraria, nei modi e nei termini che *supra* si sono tratteggiati. Il diritto in questione, solo da parte del *data subject* e solo entro determinati limiti, può quindi essere inteso quale «scelta soggettiva»[49] di cui egli può avvalersi durante il trattamento.

Si aggiunga che devono, comunque, essere sempre fatti salvi i doveri di correttezza e buona fede. Il rapporto tra titolare ed interessato non pare, infatti, poter prescindere dai principi generali di buona fede e correttezza – disciplinato, quest'ultimo, anche nel GDPR *ex* art. 5, par. 1, lett. *a)* – che rafforzano senza dubbio il principio di esattezza che non può certo essere interpretato in maniera unidirezionale, ossia valevole per il titolare nei confronti dell'interessato e non viceversa. In altri termini, la correttezza e la buona fede, così come codificate, tra gli altri, nel nostro codice civile, permeano l'intero diritto delle obbligazioni e dei contratti, ed incidono e governano anche l'agire sia del titolare sia dell'interessato.

Come si è accennato, il principio di esattezza rileva anche nell'ambito dell'art. 18 del Regolamento che, innovando rispetto alle previgenti fonti normative dell'ambito *privacy*, sancisce il diritto dell'interessato di ottenere dal titolare la limitazione del trattamento al ricorrere di una serie di ipotesi tassative[50] tra le quali figura, alla lett. *a)*, quella in cui l'interessato contesti l'esattezza dei dati personali. In tale fattispecie la limitazione dovrà essere concessa per il periodo di tempo necessario al titolare per operare una verifica in merito all'esattezza dei dati.

Il secondo paragrafo della norma, nel disporre che in caso di limitazione del trattamento, i dati siano trattati unicamente per la loro conservazione richiama la definizione che l'art. 4, par. 1, n. 3), fornisce di limitazione quale «contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro». I dati, infatti, non vengono cancellati, ma conservati dal titolare per un determinato lasso temporale; potranno essere trattati solo fondando il trattamento sul consenso dell'interessato o, senza necessità di consenso, ai fini di accertamento, esercizio o difesa di un diritto in sede giudiziaria o anche al fine di tutelare i diritti di un'altra persona fisica o giuridica, o infine per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro (art. 18, par. 2, GDPR).

---

[49] È questa la tesi sostenuta da E. Pelino, *I diritti dell'interessato*, in L. Bolognini-E. Pelino-C. Bistolfi (a cura di), *Il Regolamento* privacy *europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 257.

[50] Le ulteriori ipotesi contenute nella norma in oggetto sono: «*b)* il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; *c)* benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; *d)* l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato».

Nell'ambito delle previsioni normative inerenti alla limitazione del trattamento[51], si inserisce inoltre il *considerando* n. 67 del Regolamento che prevede le modalità attraverso le quali il titolare potrebbe (si tratta, del resto, di un *considerando* e non di una norma dotata di pieno valore precettivo)[52] procedere alla limitazione del trattamento[53]. Di particolare interesse risulta il richiamo agli archivi automatizzati che conoscono, al giorno d'oggi, un largo impiego.

Dunque, laddove l'interessato ritenga che i suoi dati siano inesatti – al di là della richiesta di una loro rettifica o eventuale cancellazione – avrà il diritto di chiedere al titolare di limitare il trattamento posto in essere (la limitazione, infatti, non opera automaticamente), senza dover fornire alcuna motivazione: ricadrà infatti, eventualmente, sul titolare l'onere di provare l'infondatezza della domanda avanzata[54]. In simili fattispecie, risulta ancora imprescindibile un sapiente utilizzo dei principi di buona fede e correttezza che devono, in tal caso, permeare, particolarmente, le azioni dell'interessato cui viene offerta una tutela tutt'altro che priva di costi per il titolare nelle more della verifica.

È proprio nell'ipotesi di richiesta di esercizio del diritto di limitazione del trattamento per inesattezza dei dati – così come nel caso *sub* lett. *d)* – che emerge la natura eminentemente cautelare[55] del diritto in questione (limitato nel tempo e suscettibile di revoca), la cui finalità è quella di evitare, per mezzo della conservazione, che si elimini un dato la cui verifica approfondita ne potrebbe delineare la liceità del trattamento posto in essere.

Anche il diritto alla limitazione del trattamento appare utile per sottolineare la centralità dell'esattezza dei dati personali e del connesso principio nell'ambito *privacy*.

---

[51] Non pare questa la sede per operare anche un confronto con la normativa previgente: a tal fine si rinvia però a A. RICCI, *I diritti dell'interessato*, cit., p. 430 s.; ed a F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 369.

[52] Sottolinea l'attenuata portata precettiva della disposizione F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, cit., pp. 368-369, che sottolinea come, oltre al fatto che la previsione sia contenuta in un *considerando*, in essa si possono leggere le parole «in linea di massima» che «riconoscono e lasciano, dunque, ai titolari del trattamento la possibilità di valutare, in relazione alla propria situazione concreta, le misure migliori per attuare la limitazione eventualmente richiesta dall'interessato».

[53] Ai sensi del *considerando* n. 67 del Regolamento «le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito *web*. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato».

[54] Cfr. G. BUTTARELLI, *op. cit*., p. 310, in cui l'A. prospetta la possibilità per il titolare di effettuare in prima persona la sua richiesta all'interessato; ed anche la possibilità di una previsione pattizia delle parti sul punto.

[55] Ne evidenzia tale natura unitamente ai profili procedurali A. RICCI, *I diritti dell'interessato*, cit., p. 431.

Il titolare dovrà provvedere immediatamente[56] a marcare i dati di cui si contesta l'esattezza, sottoponendoli a inutilizzabilità e inaccessibilità, limitandone, pertanto, il trattamento al fine di iniziare le verifiche del caso. Sempre nell'ottica di una piena tutela dell'interessato e della sua autodeterminazione informativa, devono essere inquadrati gli obblighi informativi in capo al titolare verso quest'ultimo nei casi di revoca della limitazione (art. 18, par. 3 GDPR) e verso i destinatari cui vengono trasmessi i dati sottoposti a limitazione (art. 19 GDPR). Sono, infatti, evidenti le ripercussioni fortemente negative, sia nell'ambito personale sia patrimoniale, che l'interessato i cui dati vengono trattati in modo inesatto può subire.

Per quanto non espressamente richiamato all'art. 17 GDPR, non si può ritenere che il principio di esattezza (precisamente, la sua violazione) non rilevi per il diritto alla cancellazione. Già nel rispetto dell'art. 5, par. 1, lett. *d)*, il titolare del trattamento è tenuto ad adottare tutte le misure ragionevoli per cancellare (oltre che rettificare) in modo tempestivo i dati di cui ha scoperto l'inesattezza. Tale dovere, oltre ad essere pienamente rispondente al principio di *accountability*, viene richiamato anche al *considerando* n. 39 GDPR. L'obbligazione che sorge in capo al titolare in caso di (fondata) richiesta da parte dell'interessato è comunque una obbligazione di mezzi e non di risultato, essendo chiamato ad adottare le misure che secondo ragionevolezza ci si può legittimamente attendere, avuto anche riguardo ai costi che l'operazione comporta e alla tecnologia a disposizione[57].

Il mancato rispetto del principio di esattezza sembra poter rientrare nel disposto dell'art. 17, par. 1, lett. *d)*, GDPR che sancisce il diritto dell'interessato di ottenere la cancellazione dei dati nel caso in cui siano stati «trattati illecitamente». Pare, infatti, che l'illiceità qui richiamata non attenga unicamente alla mancanza di una delle condizioni di liceità previste dal Regolamento *ex* art. 6 (la cui mancanza porta per certo ad una illiceità), ma debba essere letta in maniera più ampia, ricomprendendo anche la violazione di uno dei principi fondamentali del trattamento, e sicuramente quello di esattezza.

Si sottolinea come il titolare – che, si ricorda, deve (aggiornare, rettificare o) cancellare i dati trattati anche se si accorge *ex se* della relativa inesattezza – sia chiamato ad un compito particolarmente delicato nell'esercizio di questo diritto da parte dell'interessato. Il titolare è, infatti, chiamato a bilanciare gli altri diritti che emergono nel caso concreto (come, ad esempio, il diritto alla libertà di informazione)[58] per poi decidere di conseguenza quale diritto prevalga nella fattispecie.

---

[56] Tale immediatezza viene richiesta nelle *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data* dell'EDPS, cit., p. 21.

[57] A. Ricci, *I diritti dell'interessato*, cit., p. 412 aggiunge che «la cancellazione deve essere definitiva e deve riguardare ogni singola copia o riproduzione dei dati personali. A tale scopo i dati personali possono essere distrutti o anche anonimizzati, a condizione che non sia possibile la loro re-identificazione e non è sufficiente, ai fini della cancellazione, la pseudonimizzazione».

[58] Fattispecie prevista *ex* art. 17, par. 3 lett. *a)*, GDPR unitamente all'esercizio del diritto alla libertà di espressione; la disposizione prevede anche altri casi che non conducono alla cancellazione dei dati e precisamente: «*b)* per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; *c)* per motivi di interesse pubblico nel settore della sanità pubblica

3. Applicazione del principio nella casistica

3.1. Il diritto di rettificare dati inesatti al vaglio della Corte di giustizia. Il caso dei documenti dei concorsi professionali e delle valutazioni dell'esaminatore

Il principio di esattezza ed il connesso diritto di rettifica rivestono particolare rilevanza in una decisione della Corte di giustizia dell'Unione europea divenuta ormai nota: il caso *Nowak*[59]. In tale pronuncia, è stata infatti riconosciuta l'applicabilità del diritto di rettifica dei dati inesatti con riguardo ai documenti contenenti le correzioni di un esame pubblico.

La vicenda origina dal rifiuto del Garante per la protezione dei dati personali irlandese di consentire al sig. *Nowak*, l'accesso alla copia della propria prova di esame da esperto contabile, sostenuta in Irlanda con esito sfavorevole. Tale rifiuto veniva giustificato sul presupposto che le informazioni ivi contenute non fossero considerabili alla stregua di dati personali ai sensi della normativa sulla *privacy*.

Nonostante il rifiuto dell'autorità Garante fosse stato giustificato dalla *Circuit Court* prima, nonché dalla *High Court* e, in seguito, dalla *Court of Appeal*, la questione, sottoposta alla *Supreme Court*, veniva considerata ricevibile, ma il giudizio veniva sospeso e la questione rinviata al vaglio della Corte di Giustizia dell'Unione europea per la soluzione di pregiudiziali[60]. La Corte di Giustizia emana, pertanto, una sentenza che offre un'attenta disamina della normativa irlandese (*Data Protection Act* del 1988 come modificato dal *Data Protection Amendement Act* del 2003) di recepimento della direttiva 95/46/CE, tenendo altresì in considerazione la disciplina del GDPR che, all'epoca, non era ancora entrato in vigore.

La direttiva madre, così come anche il successivo Regolamento, accolgono una accezione ampia di dato personale, cuore della *data protection law*, anche laddove non riferibile a questioni private o familiari: «qualsiasi informazione» è oggetto della disciplina[61]. L'ampiezza delle definizioni rappresenta il fondamento per il giu-

---

in conformità dell'articolo 9, paragrafo 2, lettere *h)* e *i)*, e dell'articolo 9, paragrafo 3; *d)* a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o *e)* per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

[59] CGUE, 20 dicembre 2017, II sezione, C-434/16, *Peter Nowak* c. *Data Protection Commissioner*, in http://www.curia.europa.eu. Per un commento cfr. K. PODSTAWA, *Peter Nowak v. Data Protection Commissioner. You Can Access Your Exam Script Because It Is Personal Data*, in *European,* in *Data Prot. Law Rev*., 2018, 2, pp. 252 ss.; e D. JOVE, *Peter Nowak v Data Protection Commissioner: Potential Aftermaths Regarding Subjective Annotations in Clinical Records*, in *Data Prot. Law Rev*., 2019, 2, pp. 175 ss.

[60] Nella specie, dati i dubbi sul punto, si chiedeva alla Corte di Giustizia se le informazioni contenute nelle risposte del candidato durante un qualsivoglia esame professionale costituiscano dati personali e, in caso di risposta affermativa, quali fattori risultino determinanti per considerare la prova d'esame come dato personale e che peso tali fattori debbano avere.

[61] Con definizioni che riprendono quelle della direttiva 95/46/CE (art. 2 a e b), ai sensi dell'art. 4, 1), del Regolamento è qualificabile come "dato personale" «qualsiasi informazione riguardante una

dice al fine di stabilire che i documenti di un esame professionale e, in particolare, le valutazioni *ivi* contenute, debbano essere considerate dati personali.

È certamente pacifico che un candidato ad un esame pubblico sia una persona fisica che può (*rectius*, deve) essere identificata direttamente, attraverso il suo nome, o indirettamente, attraverso un codice identificativo, a nulla rilevando, come sostenuto invece dall'autorità Garante, il fatto che l'esaminatore possa o meno identificare il candidato al momento della correzione della prova, rimanendo sempre possibile del resto per l'ente organizzatore (nel caso di specie l'organizzazione professionale degli esperti contabili) la possibilità di identificare il candidato al fine di attribuire le risposte ad un soggetto ben determinato[62]. Le informazioni in questione sono connesse alla persona del candidato: il contenuto delle risposte rispecchia il suo livello di conoscenze e preparazione; di più, nel caso di esame redatto a mano, contengono anche informazioni grafologiche. La raccolta delle risposte, al fine di valutare l'idoneità del candidato alla professione, incide sui diritti e sugli interessi del soggetto.

Appare, quindi, corretto secondo il convincente ragionamento della Corte – la quale non si pone solo in linea con le finalità normative di tutela dell'interessato e con l'orientamento dell'autorità Garante[63], ma che dimostra, anche in questa sede, il suo cruciale ruolo interpretativo e creativo[64] – qualificare come dati personali le

persona fisica identificata o identificabile»; all'art. 4, 2), si definisce poi come "trattamento", «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali». Data l'ampiezza di queste definizioni, la natura della normativa è da considerarsi onnicomprensiva; sul tema si rinvia alle considerazioni di M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ*., 2017, 2, pp. 165 ss.

[62] Inoltre, come affermato in CGUE, 19 ottobre 2016, *Breyer*, C- 582/14, EU:C:2016:779, punto 43, affinché una informazione costituisca un dato personale non è necessario che tutte le informazioni che consentono di identificare l'interessato siano in possesso di una singola persona.

[63] Il Garante per la protezione dei dati personali ha da tempo sottolineato l'esigenza di una ampia concezione di "dato personale": si richiama per tutti Gpdp, Provv. 17 giugno 1999, doc. *web* n. 48067, uno dei primissimi e più celebri provvedimenti dell'autorità Garante in cui si afferma come si possano intendere alla stregua di "dati personali" le valutazioni che concorrono a formare il giudizio annuale di rendimento di un lavoratore dipendente, le c.d. note di qualifica, dal momento che «ogni notizia o elemento che fornisce un contributo aggiuntivo di valutazione rispetto ad un soggetto identificato o identificabile. E questo in riferimento sia ad informazioni oggettive sia a descrizioni, giudizi, analisi o ricostruzioni di profili personali (riguardanti attitudini, qualità, requisiti o comportamenti professionali) che danno origine a valutazioni complessive del soggetto interessato», tali informazioni devono pertanto essere messe a disposizione dell'interessato che ne faccia richiesta.

[64] Per quanto non sia il tema centrale della presente indagine, la pronuncia permette di sottolineare l'importanza dell'intervento della Corte di Giustizia dell'Unione europea nell'ambito *privacy*, su cui v. per tutti G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Dir. inform*., 2015, 4-5, pp. 779 ss.; e F. Rossi Dal Pozzo, *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, in *Eurojus*, 27 dicembre 2018, pp. 8 ss. in cui l'A., oltre ad analizzare la protezione dei dati personali come nuova competenza dell'Unione europea e come autonomo diritto fondamentale, pone in luce il fondamentale apporto di pronunce come *Nowak* e *Breyer* per la concezione di "dato personale". Come autorevolmente già sostenuto da F. Galgano, *La globalizzazione nello specchio del diritto*, Bologna, 2005, p. 119, la funzione creativa del diritto in capo ai giudici, soprattutto europei, è infatti da tempo considerata come «dato di cultura giuridica ormai acquisito», v. anche p. 115 in cui l'A. sottolinea come «il giudice non possa più essere, quale lo aveva pensato Montesquieu, la *bouche qui pronunce les paroles de la loi*».

informazioni contenute sia nelle risposte del candidato sia nelle annotazioni dell'esaminatore[65], in ragione del loro contenuto, delle loro finalità e dei loro effetti. La scelta del Garante per la protezione dei dati irlandese si tradurrebbe quindi in una indebita costrizione della concezione di "dato personale" e, di conseguenza, dei diritti dell'interessato che non riceverebbe protezione in situazioni, come quella in esame, meritevoli di tutela[66].

Dovendosi pertanto ammettere l'esercizio dei diritti legislativamente previsti tra i quali il diritto di rettifica su tali dati e posto che tale diritto non può certo consentire al candidato di modificare *ex post* una o più risposte sbagliate, i giudici di Lussemburgo pongono l'accento sull'esattezza e la completezza dei dati personali, per la cui valutazione ci si deve rifare alle finalità con le quali i dati in questione sono stati rilevati. Nel caso di un concorso pubblico, la «finalità consiste (…) nel poter valutare il livello di conoscenza e di competenza di tale candidato al momento dell'esame. Orbene, tale livello si riflette proprio in eventuali errori in tali risposte. Di conseguenza, errori del genere non costituiscono affatto un'inesattezza, ai sensi della direttiva 95/46, che conferisca un diritto di rettifica ai sensi dell'articolo 12, lett. *b)*, della stessa. Per contro, è possibile che si presentino, situazioni nelle quali le risposte di un candidato a un esame e le annotazioni dell'esaminatore ad esse relative si rivelano inesatte, ai sensi dell'art. 6, par. 1, lett. *d)*, della direttiva 95/46, per esempio per il fatto che, per errore, le prove di esame sono state scambiate in modo tale che le risposte di un altro candidato siano state attribuite al candidato interessato, o che una parte dei fogli contenenti le risposte di tale candidato è stata smarrita con la conseguenza che tali risposte sono incomplete o, ancora, che le eventuali annotazioni dell'esaminatore non documentano correttamente la valutazione da esso effettuata delle risposte del candidato interessato»[67].

In argomento ci si limita a richiamare le considerazioni di S. ROMANO, *L'ordinamento giuridico*, Firenze, 1946, e di P. GROSSI, *Ritorno al diritto*, Roma-Bari, 2015, pp. 34 ss.; ID., *Il diritto civile tra le rigidità di ieri e le mobilità di oggi*, in M. LOBUONO (a cura di), *Scienza giuridica privatistica e fonti del diritto*, Bari, 2009; vedi anche il commento del pensiero di Grossi offerto da G. CONTE, *L'eredità della "modernità giuridica". In margine a un recente volume di Paolo Grossi sulla storia giuridica europea*, in *Riv. trim. dir. e proc. civ*., 2009, 1, pp. 376 ss. in cui secondo l'A., Grossi non mira ad un "esilio dell'attività legislativa", ma sottolinea la non esclusività, in capo alla legge, della funzione nomopoietica, ciò anche in ragione dell'attuale presenza di vari centri di produzione del diritto che sempre più spesso non hanno un preciso radicamento territoriale; v. poi A. RICCIO, *La giurisprudenza è, dunque, fonte del diritto*, in *Contratto e impr*., 2017, 3, pp. 857 ss.; *amplius* sul tema vedi F. BRAVO, Ubi societas ibi ius *e fonti del diritto nell'età della globalizzazione*, in *Contratto e impr*., 2016, 6, pp. 1344 ss.

[65] Secondo CGUE, 20 dicembre 2017, II sezione, C- 434/16, *Peter Nowak* c. *Data Protection Commissioner*, cit., punti 42 ss., anche le annotazioni dell'esaminatore riferite alle risposte del candidato costituiscono informazioni a quest'ultimo riferibili e ciò non è contraddetto dal fatto che esse costituiscano informazioni concernenti (anche) l'esaminatore.

[66] Analizza, in particolare, la rilevanza e l'impatto della sentenza in rapporto alla nozione di "dato personale", C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020, 2, pp. 390 ss.

[67] Così CGUE, 20 dicembre 2017, II sezione, C-434/16, *Peter Nowak* c. *Data Protection Commissioner*, cit., punti 53-54; v. anche le conformi conclusioni dell'Avvocato Generale Juliane Kokott.

La tutela dell'interessato e, precisamente, la liceità del trattamento dei suoi dati trova riconoscimento nella possibilità per l'interessato di esercitare (anche) il diritto di accesso, prodromico all'eventuale richiesta di rettifica (o cancellazione) di dati inesatti o di cui non risulta più necessaria la conservazione. Sotto questo ultimo profilo, si deve infatti ammettere che l'interessato-candidato possa richiedere che le risposte date in sede di esame e le annotazioni dell'esaminatore alle prime riferite, vengano cancellate una volta raggiunte le finalità per le quali tali dati personali erano stati rilevati e trattati: verosimilmente una volta conclusosi il procedimento e trascorsi i termini per presentare ricorso, momento nel quale non può escludersi la maturazione da parte dell'interessato di un legittimo interesse alla cancellazione dei dati, fatti salvi eventuali obblighi di legge sulla conservazione per una maggiore durata della documentazione concorsuale.

Il caso *Nowak* rappresenta una dimostrazione di come sia fondamentale comprendere quali informazioni debbano essere considerate come dati personali sia per definire al meglio l'ambito di applicazione materiale del GDPR e, in particolare, del principio di esattezza dei dati, sia per poter assicurare una massima tutela ai soggetti i cui dati vengono trattati. Solo in questo modo, l'interessato potrà attivarsi nel caso in cui i suoi dati siano inesatti, esercitando i diritti previsti dal Regolamento, al fine di scongiurare una falsa rappresentazione della sua identità ed altri probabili pregiudizi di natura personale e patrimoniale.

3.2. Il principio di esattezza nelle pronunce del Garante

Il principio di esattezza si rinviene in una molteplicità di pronunce del Garante per la protezione dei dati personali, ma spesso viene evocato unicamente a fianco di altri principi che paiono, almeno ad una prima lettura, assumere maggior centralità. Ne deriva l'opportunità di analizzare *funditus* il ruolo che tale principio svolge nelle argomentazioni dell'autorità Garante al fine di comprenderne l'effettiva portata.

A ben vedere, le pronunce del Garante denotano una spiccata consapevolezza dei pregiudizi che possono derivare all'interessato nel caso in cui i dati trattati siano inesatti: l'autorità è infatti intervenuta[68] condannando le società che non pongono in essere adeguate misure tecniche e organizzative volte ad assicurare da un lato l'esattezza dei dati trattati, anche intesa come un costante aggiornamento degli stessi, e, dall'altro, a diminuire i rischi per i diritti e le libertà degli interessati in caso di *data breach*, permettendo una tempestiva verifica da parte dell'autorità di controllo. Una errata gestione delle c.d. *black lists* di esclusione dei soggetti dalle campagne commerciali, perpetrata anche attraverso un loro mancato aggiornamento, finisce per

[68] Cfr., a titolo di esempio, GPDP, Provv. 15 gennaio 2020, doc. *web* n. 9256486, sanzionatorio nei confronti di Tim S.p.a., in cui viene richiesto alla società di effettuare entro centottanta giorni di operare un «rafforzamento delle misure volte ad assicurare la qualità, l'esattezza e il tempestivo aggiornamento dei dati personali trattati dai diversi sistemi della Società», nonché «l'effettuazione di specifici e documentati test di regressione volti a verificare, per ogni modifica (correttiva o evolutiva) riguardante i sistemi che trattano dati personali della clientela, che l'impatto della modifica stessa non riduca la qualità dei trattamenti effettuati e l'esattezza dei dati trattati»; in senso conforma v. anche GPDP, Provv. 9 luglio 2020, doc. *web* n. 9435753 e GPDP, Provv. 17 gennaio 2020, doc. *web* n. 9244351.

impattare sui consensi *privacy* forniti in precedenza e riportati nelle schede anagrafiche della clientela, rendendo pertanto illecito il trattamento.

Il presidente dell'autorità ha anche avuto modo di sottolineare come il principio di esattezza, legato alla qualità dei dati trattati, sia altresì fondamentale nel contesto della lotta all'evasione fiscale[69]. Solo attraverso l'utilizzo di dati personali esatti diviene infatti possibile stilare profili di rischio di evasione affidabili, fondati su solidi presupposti, scongiurando così accessi abusivi ai dati di un vastissimo numero di persone. La pretesa di protezione dei dati personali e la ancillare creazione di canali sicuri di trasmissione degli stessi non rappresentano un ostacolo, ma un contributo essenziale finalizzato ad un serio contrasto alla evasione fiscale: se i dati non sono esatti, non è infatti possibile combattere l'evasione in modo mirato e se, inoltre, non si garantisce la sicurezza della trasmissione delle informazioni, i dati espongono il fianco a violazioni e attacchi informatici[70]. Per perseguire tale nobile fine è quindi imprescindibile un puntale rispetto del principio di esattezza (intesa anche come non obsolescenza) dei dati in modo da sfruttare corrette rappresentazioni di capacità patrimoniale e rischio fiscale degli interessati su cui fondare gli accertamenti[71].

Un importante richiamo al principio di esattezza viene effettuato nel parere del Garante sullo schema di regolamento, predisposto dal Ministero della giustizia, volto a disciplinare il trattamento dei dati giudiziari in una pluralità di ambiti[72]. Il decreto, sul quale il Garante, seppur con alcune osservazioni, esprime un parere favorevole, nel prevedere una serie di garanzie minime, comuni a tutti i casi di trattamento previsto, già annoverava un obbligo di verifica periodica circa l'esattezza e l'aggiornamento dei dati trattati, insieme alla loro adeguatezza, pertinenza e necessità in rapporto alle finalità di volta in volta perseguite.

L'autorità Garante evidenzia, in primo luogo, come il Ministero della giustizia, facendo seguito alle indicazioni da lui fornite nelle diverse interlocuzioni, abbia introdotto specifiche garanzie indirizzate ad assicurare l'esattezza dei dati con particolare riguardo all'aggiornamento rispetto all'evoluzione della posizione giudiziaria dell'interessato, utilizzando fonti che siano affidabili e aggiornate, limitando altresì il trattamento ai soli dati indispensabili in vista delle finalità perseguite[73].

L'attenzione è, a più riprese, focalizzata sulle fonti e sulla loro attendibilità, come si può osservare con riguardo ai trattamenti svolti a fini di verifica della solidità, solvibilità ed affidabilità di potenziali controparti contrattuali, attività che può essere affidata solamente a soggetti muniti di licenza prefettizia[74]. Considerati i notis-

[69] GPDP, Provv. 3 ottobre 2019, doc. *web* n. 9152641.

[70] GPDP, Provv. 15 ottobre 2019, doc. *web* n. 9162435.

[71] GPDP, Provv. 7 luglio 2021, doc. *web* n. 9678216.

[72] GPDP, Provv. 24 giugno 2021, doc. *web* n. 9682603 che si è espresso ai sensi dell'art. 2-*octies*, co. 2 del Codice *privacy*, così come modificato dal d.lgs. 101/2018, che demanda al Ministero della Giustizia, sentito appunto il Garante, la previsione dei casi in cui è legittimo il trattamento dei dati giudiziari (ai sensi dell'art. 10 del GDPR) nei casi in cui non sia già ammesso da norme di legge o regolamentari che prevedano garanzie appropriate per i diritti e le libertà degli interessati e che non avvenga sotto il controllo della autorità pubblica.

[73] GPDP, Provv. 24 giugno 2021, doc. *web* n. 9682603, cit.

[74] *Ibidem*.

simi problemi inerenti alla tutela dei dati personali indicizzati (senza aggiornamenti) dai motori di ricerca, il Garante, criticando il ricorso a fonti c.d. aperte che non sono sempre in grado di garantire affidabilità ed esattezza, suggerisce il solo utilizzo, quali legittime fonti di raccolta, di siti istituzionali, di ordini professionali e di associazioni di categoria[75]. A questo aggiunge l'opportunità di escludere la possibilità di modificare il contenuto delle informazioni eventualmente acquisite da fonti aperte, salvo il loro puntuale aggiornamento, nonché di utilizzarle con finalità di elaborazione di informazioni valutative[76].

Il principio di esattezza viene poi richiamato in alcuni provvedimenti del Garante che hanno ad oggetto i trattamenti effettuati in relazione alla certificazione verde (c.d. *green pass*), in base al d.l. 22 aprile 2021, n. 52. L'autorità Garante[77], nel sottolineare come tale d.l. non rappresenti un'idonea base giuridica per legittimare i trattamenti, mancando in particolare un'indicazione esplicita e tassativa delle finalità perseguite con le certificazioni verdi, afferma che tale fonte normativa viola il principio di esattezza, «essenziale nella valutazione della proporzionalità della limitazione e della idoneità della misura di contenimento e contrasto dell'emergenza epidemiologica da Covid-19»[78]. Il contrasto con il principio di esattezza si palesava dal momento che il sistema transitoriamente posto in essere (nelle more dell'adozione di un decreto attuativo che istituisse la piattaforma nazionale *Digital Green Certificate*, DGC) non consentiva una verifica dell'attualità delle condizioni attestate, non potendo tener conto di eventuali modifiche dello stato di salute dell'interessato, sopraggiunte in un momento successivo al rilascio della certificazione, a causa della mancanza di una piattaforma. Erano, quindi, chiari i rischi per i diritti e le libertà degli interessati da un lato e la potenziale inefficacia della misura in rapporto alla finalità di contenimento della diffusione del virus Sars-Cov-2.

Il Garante ha successivamente avuto modo di esprimersi[79] sulla bozza di decreto del Presidente del Consiglio dei Ministri, da adottare ai sensi dell'art. 9, co. 10, del d.l. 52/2021, trasmessa all'autorità unitamente alla valutazione di impatto sui dati personali con riferimento ai trattamenti disciplinati dal DPCM ed in particolare a quelli effettuati attraverso la piattaforma DGC. Il parere (favorevole seppur con alcune condizioni) del Garante si sofferma sulle criticità già espresse in merito alla mancata indicazione delle finalità di trattamento, sottolineando la necessaria introduzione di una riserva di legge statale che individui puntualmente le finalità per le quali possano essere utilizzate le certificazioni verdi – attestanti l'avvenuta vaccinazione di un soggetto o la sua guarigione da Covid-19 o, ancora, l'esito negativo al virus Sars-Cov-2 in seguito ad un test antigenico rapido o molecolare – così da eliminare *ex ante* la possibilità di incorrere in interpretazioni discrezionali particolarmente estensive. L'obbligo di presentare il *green pass* per accedere a luoghi o servizi rappresenta del resto, come argomenta il Garante, una limitazione della libertà

[75] *Ibidem*.
[76] *Ibidem*.
[77] GPDP, Provv. 23 aprile 2021, doc. *web* n. 9578184.
[78] *Ibidem*. Espressamente, nel Provv. cit., il Garante ha affermato che «il decreto legge del 22 aprile 2021, 52, si ritiene violi anche il principio di esattezza».
[79] GPDP, Provv. 9 giugno 2021, doc. *web* n. 9668064.

personale che, in quanto tale, può essere ammessa solo se prevista da una norma di legge di rango primario.

Il parere in questione rileva anche, ai fini della presente trattazione, proprio per l'attenzione da esso riservata al principio di esattezza e, segnatamente, al superamento delle criticità precedentemente espresse sul contrasto con detto principio. La bozza di DPCM infatti – come, ovviamente, poi il DPCM stesso del 17 giugno 2021[80] – istituisce la piattaforma DCG e permette all'interessato di esercitare il diritto di rettifica con una modalità semplificata, ossia rivolgendosi ad un servizio messo a disposizione dal Ministero della salute, tramite un numero di pubblica utilità e ricevendo un riscontro in un termine congruo rispetto alla certificazione rilasciata. Viene in tal modo assicurato un doppio controllo, a monte dal titolare e poi dall'interessato, sull'esattezza e sull'aggiornamento dei dati così da scongiurare, almeno in linea di massima, i gravissimi pregiudizi che potrebbero derivare in capo all'interessato a causa di un inesatto trattamento di suoi dati sensibili e all'intera collettività per un utilizzo non congruo (soprattutto in termini di esattezza dei dati trattati) delle certificazioni verdi nella contingente situazione pandemica.

Da ultimo, pare opportuno sottolineare che l'attenzione del Garante per il principio di esattezza è dimostrato dai numerosi richiami che ne vengono effettuati in una pletora di provvedimenti che interessano i temi più diversi, ma nei quali tale principio assurge sempre a strumento fondamentale per guidare la *compliance* del trattamento posto in essere con la normativa *privacy*[81]. Proprio dal numero dei prov-

[80] Al DPCM di attuazione del d.l. 52/2021, ha fatto seguito una nota del Presidente del Garante per la protezione dei dati personali (GPDP, 21 giugno 2021, doc. *web* n. 9681670) in cui evidenzia come il DPCM tenga conto delle osservazioni formulate dal Garante nel parere del 9 giugno *supra cit*., sottolineando però la «necessità di soprassedere dall'adottare o dal dare attuazione a disposizioni adottate a livello locale che: – introducono fattispecie diverse da quelle allo stato previste dalla normativa di livello nazionale in cui possa essere richiesta l'esibizione dei certificati (…); – prevedono modalità di emissione, gestione e controllo delle predette certificazioni difformi da quelle disciplinate nel predetto decreto del Presidente del Consiglio dei Ministri».

[81] Cfr. a titolo di esempio, tra i più recenti, GPDP, Provv. 9 marzo 2023, doc. *web* n. 9868836 relativo all'approvazione di un codice di condotta per le attività di *telemarketing* e *teleselling*; GPDP, Provv. 21 dicembre 2022, doc. *web* n. 9856315 in merito ad un parere, richiesto al Garante dall'Organismo agenti e mediatori, con riguardo alle specifiche tecniche relative alla procedura di registrazione degli operatori in valute virtuali alla sezione speciale del Registro dei Cambiavalute; GPDP, Provv. 24 novembre 2022, doc. *web* n. 9842737 con riguardo all'esattezza dei dati usati per finalità di ricerca medica; GPDP, Provv. 15 settembre 2022, doc. *web* n. 9815094 riguardante un parere sullo schema di decreto del Ministero dell'Interno, recante «modalità di aggiornamento della piattaforma di funzionamento dell'Anagrafe Nazionale della Popolazione residente per l'erogazione dei servizi resi disponibili ai comuni per l'utilizzo dell'Archivio Nazionale informatizzato dei registri dello Stato Civile»; GPDP, Provv. 16 dicembre 2021, doc. *web* n. 9738899 sulla «necessità di assicurare il rispetto del principio di esattezza dei dati relativi ai consumi energetici che potrebbero risultare non correttamente associabili agli interessati»; GPDP, Provv. 13 dicembre 2021, doc. *web* n. 9727220 in merito alla «necessità di garantire l'esattezza e l'aggiornamento dei dati in base ai quali è generata la certificazione verde»; GPDP, Provv. 23 aprile 2021, doc. *web* n. 9582723 che lamenta come, nel caso concreto, la comunicazione o diffusione dei dati potrebbe «porsi in contrasto con il principio generale di "esattezza dei dati"»; GPDP, Provv. 21 aprile 2021, doc. *web* n. 9676101 in cui si rileva che «il trattamento (…) tramite il motore di ricerca risulta pertanto in contrasto con i principi di esattezza ed aggiornamento dei dati»; GPDP, Provv. 25 febbraio 2021, doc. *web* n. 9556958 che sottolinea: «in

vedimenti che lo richiamano a fondamento della decisione, e dalla sua rilevanza, sottolineata dal Garante stesso, emerge l'importanza del principio in esame e la sua assoluta centralità per l'impianto normativo volto a disciplinare la protezione dei dati personali.

Ad esempio, il Garante[82] ha evidenziato l'importanza del principio di esattezza, inteso come aggiornamento delle informazioni, ed il pregiudizio derivante alla reputazione personale e professionale di un soggetto dalla perdurante reperibilità in rete di articoli contenenti informazioni risalenti, relative a misure disposte nei suoi confronti successivamente revocate: in detti articoli (così come in altri reperibili) non si dava atto del decreto di archiviazione pronunciato nei suoi riguardi «determinando con ciò la circolazione di informazioni sul conto dell'interessato divenute ormai inesatte le quali, essendo collegate a gravi fattispecie di reato, risultano peraltro particolarmente pregiudizievoli per i diritti del medesimo»[83]. Simili considerazioni sono state svolte nel caso in cui i fatti collegati al soggetto e reperibili in rete, anche a distanza di un ampio lasso temporale, erano riferiti a vicende alle quali non era seguita alcuna condanna per l'interessato[84].

Divenuto celebre è invece il provvedimento[85] che contiene una (pesante) sanzione per l'impiego di un sistema di supervisione (*proctoring*), utilizzato durante le prove scritte d'esame, in modalità "a distanza", al fine di identificare e controllare gli studenti universitari nello svolgimento della prova.

A prescindere dalle considerazioni, ampiamente esaminate dal Garante, in tema di liceità, correttezza e trasparenza del trattamento, nonché di minimizzazione e conservazione dei dati, preme, ai fini del discorso che si intende sviluppare in questa sede, evidenziare come nel provvedimento in questione si sottolinei l'importanza di «un'adeguata valutazione in merito all'effettiva affidabilità dello strumento di supervisione, con riguardo sia alle funzioni di riconoscimento facciale (…) sia ai meccanismi con i quali vengono definiti gli indici di rischio, non essendo state, pertanto, valutate le possibili ripercussioni per gli interessati in caso di errori o falsi positivi/negativi»[86]. Quando si utilizzano strumenti di identificazione biometrica, è centrale l'affidabilità degli algoritmi utilizzati dal sistema e l'esattezza dei dati inseriti nel si-

assenza di dati esatti, la qualità del controllo effettuato (…) potrebbe risultare compromessa; il raffronto effettuato potrebbe infatti, da un lato, condurre all'individuazione di un soggetto sbagliato e, dall'altro, non consentire invece di identificare soggetti non aventi diritto»; GPDP, Provv. 10 dicembre 2020, doc. *web* n. 9575055 che rileva come il titolare del trattamento, nel caso di specie, abbia operato l'aggiornamento di determinate informazioni, necessario per conformare «il trattamento ai principi di esattezza».

82 GPDP, Provv. 25 novembre 2021, doc. *web* n. 9731941.

83 *Ibidem*, in cui si aggiunge che «il perdurante trattamento di tali dati in associazione al nominativo dell'interessato appare dunque in contrasto con i principi di esattezza ed aggiornamento previsti dal Regolamento (cfr. art. 5, par. 1, lett. *d)*)»; in senso conforme GPDP, Provv. 25 novembre 2021, doc. *web* n. 9732385; GPDP, 25 novembre 2021, doc. *web* n. 9732368; GPDP, Provv. 10 febbraio 2022, doc. *web* n. 9750669; GPDP, Provv. 13 febbraio 2020, doc. *web* n. 9308726; GPDP, Provv. 21 luglio 2022, doc. *web* n. 9812455.

84 GPDP, Provv. 10 febbraio 2022, doc. *web* n. 9750669.

85 GPDP, Provv. 16 settembre 2021, doc. *web* n. 9703988.

86 *Ibidem*.

stema per evitare distorsioni sull'identità dell'interessato, limitazioni dei suoi diritti e per un corretto e proficuo perseguimento delle finalità del trattamento.

Ancora, l'esattezza dei dati deve essere rispettata al fine di evitare l'accesso di dati personali a soggetti non legittimati, i cui risvolti negativi si acuiscono nel caso di categorie particolari dei dati personali come quelli sanitari. Si richiama sul punto il caso di una signora che, a causa di un errore dell'operatore nell'inserire i dati nel Fascicolo Sanitario Elettronico (FSE), aveva la possibilità di visualizzare, attraverso la sua utenza, il FSE di una minore sulla quale, in realtà, non vantava la responsabilità genitoriale[87].

Un rigoroso rispetto del principio di esattezza deve quindi essere considerato (e così pare essere nei provvedimenti del Garante) un'esigenza primaria ai fini di una piena tutela dei diritti e delle libertà del *data subject* e, altresì, per garantire uno sfruttamento anche in chiave economica dei dati personali la cui protezione non è una prerogativa assoluta (*considerando* n. 4 GDPR).

Il Garante per la protezione dei dati personali dimostra, pertanto, di essere profondamente consapevole dei danni che possono derivare all'interessato in caso di trattamento di dati inesatti: danni che, si è detto, potrebbero investire sia l'ambito personale sia quello patrimoniale. Nonostante la lente del Garante per indagare il principio di esattezza sia maggiormente quella della tutela dell'interessato, non devono essere tralasciati gli interessi che il titolare potrebbe avere nel trattare dati esatti. Come si è precedentemente accennato, infatti, dato che si ammette, sempre più ampiamente, uno sfruttamento economico dei dati da parte dei titolari, solo laddove i dati trattati siano esatti, le politiche di *marketing* possono essere mirate e quindi maggiormente efficaci.

Il principio di esattezza deve quindi essere considerato sotto la doppia luce della tutela dei diritti e delle libertà dell'interessato, da un lato, e del riconoscimento e della garanzia degli interessi del titolare dall'altro: solo un suo puntuale rispetto permette, infatti, di soddisfare le esigenze dei soggetti del trattamento e di garantire stabilità all'architettura dell'intero sistema *privacy*.

[87] GPDP, Provv. 24 giugno 2021, doc. *web* n. 9709119 in cui, però, si sottolinea che, nel caso di specie, il Garante si è limitato ad una mera ammonizione per il titolare del trattamento data la sua buona fede, il suo impegno immediato indirizzato alla correzione delle inesattezze dei dati e atteso che «ha attuato misure volte a ripristinare una corretta alimentazione dei Fascicoli sanitari elettronici dei soggetti interessati dalla vicenda oggetto della segnalazione, nonché previsto misure tecniche e organizzative volte a scongiurare che episodi come quello in esame posano ripetersi».

Capitolo VIII
Il principio di limitazione della conservazione

Alessandro Chiappini

Sommario: 1. Inquadramento normativo. – 2. Portata del principio. – 3. Applicazione del principio nella casistica. – 3.1. Il principio di limitazione della conservazione nei provvedimenti del Garante per la protezione dei dati personali. – 3.1.1. Il mutato approccio in materia di limitazione della conservazione: dai provvedimenti generali del Garante (o resi a seguito di verifica preliminare) all'applicazione del principio di *accountability*. – 3.1.2. I provvedimenti in materia di lavoro. – 3.1.3. I provvedimenti in materia di biometria. – 3.1.4. I provvedimenti in materia di videosorveglianza. – 3.1.5. I provvedimenti in materia di *marketing* e profilazione. – 3.1.6. I provvedimenti in ambito giudiziario. – 3.1.7. I provvedimenti in materia di trattamenti a fini statistici o di ricerca scientifica. – 3.2. Il principio di limitazione della conservazione nella giurisprudenza della Corte europea dei diritti dell'uomo. – 3.3. Il principio di limitazione della conservazione in materia di *data retention* tra la giurisprudenza della Corte di giustizia dell'UE e la normativa italiana. – 3.4. Principio di limitazione della conservazione, diritto alla cancellazione e diritto all'oblio.

1. Inquadramento normativo

Il principio di limitazione della conservazione, previsto all'art. 5, par. 1, lett. *e)*, del Reg. UE 2016/679 (GDPR) impone che i dati personali siano «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati»[1].

L'attuale formulazione del principio trae origine dalla disposizione di cui all'art. 5, par. 4, lett. *e)*, della Convenzione n. 108 del 1981 sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali. Tale Convenzione, infatti, nel testo anteriore alla riforma avutasi con il Protocollo addizionale del 2018, prevedeva che i dati a carattere personale oggetto di elaborazione automatica fossero «conservati sotto una forma che permetta l'identificazione delle persone interessate

[1] Sul principio di limitazione della conservazione dei dati nel GDPR, v. G. Malgieri, *Commento all'art. 5. Principi applicabili al trattamento dei dati personali*, in R. D'Orazio-G. Finocchiario-O. Pollicino-G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, pp. 187 ss.; F. Resta, *Commento all'art. 5. Principi applicabili al trattamento di dati personali*, in G.M. Riccio-G. Scorza-E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2019, pp. 59 ss.; M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento di dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 179 ss.; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, pp. 239 ss.

per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati».

Il testo della Convenzione è stato aggiornato nel 2018, sotto la spinta innovatrice del GDPR. Nell'attuale versione, denominata Convenzione 108+, il principio di limitazione della conservazione risulta riconducibile quasi integralmente alla disposizione del regolamento europeo. In tal senso, si segnala che l'ambito di applicazione della convenzione (e del principio in esame), inizialmente limitato ai dati oggetto di elaborazione automatica, risulta oggi esteso in generale ai dati personali oggetto di trattamento, a prescindere dall'uso o meno di strumenti elettronici. Inoltre, la terminologia della convenzione è stata allineata a quella adottata dal GDPR[2].

Nell'ordinamento europeo, il principio in parola ha trovato un primo riconoscimento nella Direttiva 95/46/CE (Direttiva), ove, all'art. 6, par. 1, lett. *e)*, veniva stabilito che «Gli Stati membri dispongono che i dati personali devono essere (…) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati»[3]. Tale disposizione faceva salva la possibilità per gli Stati Membri di consentire la conservazione dei dati per un tempo ulteriore per motivi storici, statistici o scientifici, prevedendo a tal fine garanzie adeguate[4].

In sede di attuazione, la direttiva era stata recepita con l. 675 del 1996, al cui art. 9, comma 1, lett. *e)*, veniva sancito il principio di limitazione della conservazione con formulazione sostanzialmente identica a quella della Direttiva. La disposizione era stata poi trasposta nell'art. 11, co. 1, lett. *e)*, del d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) con testo analogo a quello della l. 675 del

---

[2] In particolare, si rileva che, rispetto al testo originario della Convenzione n. 108, nell'attuale formulazione, è stata utilizzata, in relazione alla durata della conservazione, l'espressione *«necessary»* anziché *«required»*, analogamente a quanto previsto dall'art. 5, par. 4, GDPR, e, in relazione ai dati, il termine *«stored»* è stato sostituito con *«processed»*, ricomprendendo così tutte le operazioni di trattamento *ex* art. 4, n. 2, GDPR, di cui la registrazione è una specie.

[3] Sul principio di limitazione della conservazione dei dati nella Direttiva, v. F. BRAVO-J. MONDUCCI, *Regole generali applicabili a tutti i trattamenti di dati personali*, in J. MONDUCCI-G. SARTOR (a cura di), *Il Codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003 n. 196*, Padova, 2004, pp. 35 ss.; E. NAVARRETTA, *Commento all'art. 11. Modalità del trattamento e requisiti dei dati*, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 193 (Codice della privacy)*, Tomo I, 2007, Padova, pp. 242 ss.; G. FINOCCHARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 127 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997, pp. 259 ss.; P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, pp. 395 e ss.; M.G. LOSANO, *Commento all'art. 9. Modalità di raccolta e requisiti dei dati personali,* in E. GIANNANTONIO-M.G. LOSANO-V. ZENO ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999, pp. 96 ss.

[4] V. *considerando* n. 29 della Direttiva che prevedeva: «considerando che l'ulteriore trattamento di dati personali per scopi storici, statistici o scientifici non è generalmente considerato incompatibile con le finalità per le quali i dati erano stati preventivamente raccolti, purché gli Stati membri forniscano adeguate garanzie; che tali garanzie devono soprattutto impedire l'uso dei dati per l'adozione di misure o decisioni nei confronti di singole persone».

1996[5], fatta eccezione per la conservazione per scopi storici, statistici o scientifici, specificatamente recepita nell'art. 16 del Codice, in materia di «*Cessazione del trattamento*».

A livello terminologico, si noti poi che la rubrica dell'art. 11 del Codice, «*Modalità del trattamento e requisiti dei dati*», si discostava da quella precedentemente prevista dalla l. 675 del 1996, «*Modalità di raccolta e requisiti dei dati personali*». Anche la collocazione di tali disposizioni risultava diversa: l'art. 11 del Codice era collocato nel Capo I del titolo III, in materia di «*Regole per tutti i trattamenti*» mentre l'art. 9 della l. 675 del 1996 risultava inserito nella Sezione I del Capo III, in materia di «*Raccolta e requisiti dei dati*». Le menzionate modifiche della rubrica e della collocazione apportate dal Codice hanno sancito il carattere trasversale dei requisiti ivi previsti (ivi incluso il principio in parola) rispetto a tutte le operazioni del trattamento, consentendo di superare il rinvio restrittivo della l. 675 del 1996 alla sola raccolta del dato[6].

Si rileva altresì che, nel recepimento dell'art. 6 della Direttiva, il legislatore italiano ha omesso, sia nella l. 675 del 1996 che nel Codice, il riferimento alla natura di «*principi*», ricorrendo piuttosto al concetto di «*modalità del trattamento*» e «*requisiti del dato*». Tale asimmetria (oggi superata con l'adozione del GDPR) pone in luce meridiana la duplice natura del principio in parola: canone generale e fondamentale della disciplina e, allo stesso tempo, criterio determinativo delle modalità di trattamento[7]. Non risulta comunque che tale difformità di impostazione abbia prodotto contrasti interpretativi tra la normativa italiana e quella europea.

L'art. 11 del Codice è stato formalmente abrogato dall'art. 27, co. 1, lett. *a)*, n. 2, del d.lgs. n. 101 del 2018 con cui il legislatore italiano ha adottato le disposizioni per l'adeguamento della normativa nazionale alla disciplina del GDPR. Stante tuttavia l'applicazione diretta delle norme del regolamento, il principio di limitazione della conservazione, enunciato al già citato art. 5, par. 1, lett. *e)*, reg. cit., risulta uniformemente applicabile in tutti i Paesi membri dell'Unione europea.

La formulazione del principio prevista oggi dal GDPR risulta sovrapponibile, pur con alcune precisazioni formali, a quella del citato art. 6, par. 1, lett. *e),* della Direttiva. In particolare, si rileva che, se la Direttiva richiamava le «finalità per le quali [i dati] sono rilevati o sono successivamente trattati», il Regolamento riferisce il periodo di conservazione alle «finalità per le quali [i dati] sono trattati». Considerato però che la raccolta costituisce un'operazione di trattamento, *ex* art. 4, n. 2, del GDPR, non si rinviene una differenza sostanziale tra le disposizioni considerate.

In modo analogo a quanto previsto in precedenza dalla Direttiva, la conservazione dei dati per un ulteriore periodo risulta ammessa, *ex* art. 5, par. 1, lett. *e)* del GDPR, esclusivamente per pubblico interesse o per finalità statistiche o di ricerca

---

[5] Sulla portata delle modifiche introdotte dal Codice, v. E. Navarretta, *op. cit.*, p. 242, la quale evidenzia che, seppure le disposizioni dell'art. 11 del Codice e dell'art. 8 della l. 675 del 1996 si pongano nel solco della continuità, le nuove previsioni del Codice e delle altre fonti sistematicamente coordinate con lo stesso comportano un «potenziale effetto dirompente» nell'interpretazione del predetto art. 11.

[6] In tal senso, v. F. Bravo, in F. Bravo-J. Monducci, *op. cit.*, pp. 35 ss.

[7] Sul carattere operativo del principio di limitazione della conservazione, v. *amplius* il par. 2.

scientifica o storica, secondo quanto previsto dall'art. 89, par. 1, del Regolamento, fermo l'obbligo di adozione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato.

Si rileva, inoltre, che, al principio in esame, trovano applicazione le limitazioni di cui all'art. 23 del GDPR, di talché la conservazione per un periodo ulteriore è ammessa quando sia stata prevista in forza di una norma di legge, rappresenti una «misura necessaria e proporzionata in una società democratica per salvaguardare» gli interessi individuati nel predetto articolo e «rispetti l'essenza dei diritti e delle libertà fondamentali»[8].

Al di fuori dell'ordinamento europeo, l'applicazione del principio di limitazione della conservazione risulta attualmente estesa in forza del menzionato art. 5, par. 4, lett. *e)*, della Convenzione n. 108+ a tutti i 47 Stati aderenti al Consiglio d'Europa.

2. PORTATA DEL PRINCIPIO

Nelle opere dedicate alla materia, il principio di limitazione della conservazione non sembra aver ottenuto la stessa attenzione riservata agli altri principi oggi previsti dall'art. 5 GDPR. Il principio in esame costituisce, infatti, una diretta applicazione del principio di limitazione della finalità, sul quale si sono spesso concentrati gli sforzi ermeneutici della dottrina[9]. Inoltre, il carattere prettamente operativo del principio ha fatto sì che, specie nei provvedimenti dell'autorità di controllo antecedenti al regolamento, questo abbia trovato applicazione, di regola, sotto forma di previsione di un termine congruo alla finalità di volta in volta considerata. Pertanto, nel prosieguo del discorso, ci si propone di analizzare la portata del principio in esame, tenendo conto sia dell'interpretazione sistematica della norma in cui si trova espresso, sia della ricostruzione del dibattito dottrinale e istituzionale avutosi con riguardo ad essa[10].

Come anticipato, il GDPR ha ribadito la natura di principio della disposizione in esame, consentendo di superare le differenti terminologie adottate su base nazionale. Tale scelta è stata oggetto di particolare attenzione da parte della letteratura. In particolare, vi è chi[11] ha rilevato un utilizzo non tecnico dell'espressione «*principi*» da parte del legislatore europeo, considerato che i criteri *ex* art. 5 GDPR non sarebbero riconducibili né all'alveo dei principi fondamentali, né a quello dei principi generali, dovendosi piuttosto imputarne la nomenclatura al carattere indeterminato di direttiva fondamentale della materia. Inoltre, autorevole dottrina, nel ripartire i

[8] Sul punto cfr. CGUE, *La Quadrature du Net*, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, di cui si dirà meglio *infra*, *sub* par. 3.3.

[9] In tal senso, v. F. BRAVO, in F. BRAVO-J. MONDUCCI, *op. cit.*, p. 49; M.G. LOSANO, *op. cit.*, p. 105; E. NAVARRETTA, *Commento all'art. 11. Modalità del trattamento e requisiti dei dati*, cit., p. 267.

[10] Per l'analisi dell'applicazione del principio di limitazione della conservazione nella casistica, nazionale e sovranazionale, si rimanda, invece, all'analisi che sarà condotta, *infra*, al par. 3 del presente contributo.

[11] Cfr. F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civili commentate*, 2017, 2, p. 386.

principi in materia di protezione dei dati tra principi-valore e principi-funzionali, di fronte alla sua formulazione originariamente ospitata nel Codice in materia di protezione dei dati personali, ha ricondotto il principio di limitazione della conservazione alla seconda categoria[12], posto che la disposizione ad esso relativa (art. 11 del Codice, poi abrogato), afferiva direttamente alle modalità del trattamento.

Nel nuovo assetto normativo, la portata del principio deve essere, *in primis*, indagata in relazione alla sua natura traversale rispetto alle altre disposizioni di cui all'art. 5 GDPR, a partire dal principio di limitazione della finalità.

Già nella vigenza della Direttiva, si è notato che il principio *ex* art. 5, par. 1, lett. *b*), GDPR opera come criterio guida per l'intero regime di trattamento, dalla selezione dei dati personali all'utilizzo e conservazione degli stessi[13]. Secondo tale impostazione, il principio di limitazione della conservazione costituiva – e costituisce tuttora – la determinazione dinamica sul piano temporale del principio di limitazione della finalità[14].

Il principio in esame rappresenta, altresì, un corollario del principio di minimizzazione, come evidenziato dal *considerando* n. 39 GDPR[15]. Infatti, l'adozione di tempi di conservazione proporzionati alle finalità di trattamento riduce le possibilità che i dati diventino nel tempo inadeguati, irrilevanti o eccessivi[16].

Analogo ragionamento può proporsi per il principio di esattezza, posto che una conservazione del dato sproporzionata rispetto alla finalità per cui è stato raccolto aumenta il rischio di conservare dati inesatti o non aggiornati[17].

È possibile, inoltre, delineare un nesso funzionale tra il principio in parola ed i principi di correttezza, liceità e trasparenza, considerato che un trattamento ultroneo di dati personali risulterebbe abusivo ed imprevedibile per l'interessato, in quanto in contrasto con le finalità predeterminate dal titolare ed oggetto di informativa[18]. Tale connessione è stata formalmente sancita dal regolamento europeo negli artt. 13, par. 2, lett. *a)*, e 14, par. 2, lett. *a)*, i quali impongono espressamente, tra gli obblighi informativi, la comunicazione «del periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo»[19].

---

[12] Cfr. F. Bravo, in F. Bravo-J. Monducci, *op. cit.*, p. 49.

[13] Cfr. E. Navarretta, *op. cit.*, p. 267.

[14] Nello stesso senso, cfr. altresì: F. Bravo, in F. Bravo-J. Monducci, *op. cit*, p. 49; F. Pizzetti, *op. cit.*, p. 265; M.G. Losano, *op. cit.*, p. 105; M. Dell'Utri, *op. cit.*, pp. 214 ss.

[15] In dottrina, cfr. F. Resta, *op. cit.*, p. 59.

[16] In tal senso, si veda la guida dell'Information Commisioner's Office (ICO), «*Principle (e): Storage limitation*», consultabile al sito https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/.

[17] *Ibidem*. Cfr. altresì Gruppo di lavoro ex art. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 3 ottobre 2017, versione emendata del 6 febbraio 2018, p. 13.

[18] Cfr. L. Bolognini, *Principi del trattamento* in L. Bolognini-E. Pelino-C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 110, e P. Iamiceli, *op. cit*., p. 449.

[19] Sul punto, cfr. Gruppo di lavoro ex art. 29, *Linee guida sulla trasparenza ai sensi del Regolamento 2016/679*, 29 novembre 2017, versione emendata del 11 aprile 2018, Allegato recante «*Informazioni da fornire all'interessato ai sensi dell'articolo 13 o 14*», che prevede che il periodo di conservazione (o i criteri per determinarlo) «dovrebbe essere indicato in maniera tale da consentire

Il principio di limitazione della conservazione rileva, parimenti, in relazione al principio di sicurezza ed integrità dei dati personali atteso che «previene anche la possibilità di un accesso abusivo ad informazioni delle quali si può perdere il controllo, mancando un interesse attuale per il detentore»[20].

«Corollario in negativo» del principio in esame è rappresentato dal diritto alla cancellazione di cui all'art. 17 GDPR[21], il quale, per quanto qui interessa, prevede che l'interessato abbia il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali ove non siano più necessari per le finalità per cui sono stati raccolti[22].

Come si è visto, l'art. 5, par. 1, lett. *e)* GDPR, dispone la conservazione dei dati personali «in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati». In base al principio di responsabilizzazione *ex* art. 5, par. 2, GDPR, la determinazione dei tempi di conservazione spetta al titolare del trattamento; a tal fine, deve tenersi in considerazione il contesto e le finalità del trattamento, oltre al «rischio per i diritti e le libertà delle persone fisiche»[23]. Devono essere altresì valutati i codici di condotta, standard e linee guida di settore eventualmente applicabili. Resta fermo che, in presenza di norme di legge[24] che prevedano espressamente specifici periodi di conservazione, il titolare (al pari del responsabile) dovrà rispettare tali tempistiche[25].

---

all'interessato di stabilire quale sarà, in base alla sua specifica situazione, il periodo previsto per i dati/fini specifici. Non è sufficiente che il titolare del trattamento affermi in maniera generica che i dati personali saranno conservati finché sarà necessario per le finalità legittime del trattamento. Ove pertinente, dovrebbero essere fissati periodi di conservazione diversi per le diverse categorie di dati personali e/o finalità del trattamento, inclusi, se del caso, i periodi di archiviazione». In senso analogo cfr. GPDP, Provv. 10 novembre 2022, Ordinanza ingiunzione nei confronti di società Poliambulatorio Radiologico "il Sorriso" S.r.l., doc. *web* n. 9843603*,* e GPDP, Provv. 10 giugno 2021, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. doc. *web* n. 9675440.

[20] Cfr. G. BUTTARELLI, *op. cit.*, p. 262.

[21] Così D. ACHILLE, *Principi*, in A. BARBA-S. PAGLIANTINI (a cura di), *Commentario del Codice Civile. Delle Persone. Leggi Collegate, Vol. II*, Torino, 2019, pp. 111-112; M. DELL'UTRI*, op. cit*., p. 215; G. BUTTARELLI, *op. cit.*, p. 261.

[22] Sui diritti alla cancellazione e all'oblio, si rinvia al par. 3.4 del presente capitolo.

[23] Così, GPDP, *Videosorveglianza, Domande più frequenti (FAQ)*, consultabile al sito https://www.garanteprivacy.it/faq/videosorveglianza; in tal senso, cfr. anche GPDP, Provv. 15 ottobre 2020, doc. *web*. n. 9486485.

[24] Cfr., ad esempio: gli artt. 123 e 132 del Codice *privacy*, resi in materia di servizi di comunicazione elettronica; l'art. 24 della l. n. 167 del 20 novembre 2017 in materia di «*Termini di conservazione dei dati di traffico telefonico e telematico*»; l'art. 2220 c.c. in materia di «*Conservazione delle scritture contabili*»; l'art. 6, co. 8, del d.l. 23 febbraio 2009, n. 11, conv. con mod. dalla l. 23 aprile 2009, n. 38, sulla conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza da parte dei Comuni a fini di sicurezza urbana; la Circolare del Ministero della Sanità del 19 dicembre 1986 n. 900 2/AG454/260 in relazione alla conservazione delle cartelle cliniche; l'art. 5, d.m. 18 febbraio 1982 sulla documentazione inerente gli accertamenti effettuati nel corso delle visite per il rilascio del certificato di idoneità all'attività sportiva agonistica; l'art. 4, d.m. 14 febbraio 1997, in materia di documentazione iconografica radiologica.

[25] In tal senso, cfr. GPDP, Provv. 9 aprile 2003, doc. *web* n. 1075195, per il quale «Legittimamente una società che emette carte di credito conserva i dati relativi ad un rapporto contrattuale anche successivamente alla sua conclusione, per effetto della revoca della carta stessa, al fine di rispettare le disposizioni di legge contro il riciclaggio e per poter adempiere agli obblighi previsti dalla nor-

Al «conseguimento delle finalità» di trattamento, quale termine finale dell'«arco di tempo» della conservazione, possono equipararsi il venir meno, per il titolare, dell'interesse al trattamento o l'illiceità sopravvenuta della finalità perseguita, circostanze nelle quali il trattamento dovrà, pertanto, essere interrotto[26].

Nel caso di adozione della base giuridica del consenso, la durata della conservazione non può essere automaticamente estesa sino ad un'eventuale richiesta dell'interessato, quale la revoca del consenso o l'opposizione al trattamento. Sebbene, infatti, il consenso possa ritenersi valido fino alla sua revoca o all'opposizione dell'interessato, il titolare deve comunque procedere ad una conservazione limitata nel tempo dei dati trattati in ragione delle finalità perseguite «anche considerato che l'interessato potrebbe anche non mutare mai la propria volontà o mantenerla invariata per anni»[27].

Ove il trattamento si fondi, invece, sulla base del legittimo interesse del titolare del trattamento o di terzi, il periodo di conservazione dovrà essere previamente valutato nell'ambito dell'analisi del bilanciamento degli interessi (LIA) ai sensi dell'art. 6, par. 1, lett. *f)*, GDPR[28].

Inoltre, deve ritenersi legittima la conservazione dei dati per un tempo ulteriore rispetto al raggiungimento delle finalità di trattamento laddove necessaria al titolare per difendere o far valere un diritto in giudizio, nei limiti stabiliti dalle norme in materia di decadenza e prescrizione[29]. Ciò trova conferma nell'interpretazione

---

mativa sulla conservazione delle scritture contabili»; in senso analogo, cfr. altresì GPDP, Provv. 19 dicembre 2018, Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101, doc. *web* n. 9069653; GPDP, Provv. 7 marzo 2019, Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario, doc. *web* n. 9091942; GPDP, Provv. 28 febbraio 2019, Ordinanza ingiunzione nei confronti di Comune di Misterbianco, doc. *web* n. 9123981.

[26] Cfr. M. Dell'Utri, *op. cit.*, p. 215.

[27] *In tal senso, cfr. GPDP, Provv. 18 luglio 2023, doc. web. 9920942. par. 9.5. Cfr. altresì GPDP, Provv. 20 ottobre 2022, Ordinanza ingiunzione nei confronti di Douglas Italia S.p.A., doc. web n. 9825667, par. 4.*

[28] Sul legittimo interesse, cfr. Gruppo di lavoro ex art. 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014.

[29] In tal senso, cfr. GPDP, Provv. 1° marzo 2007, Lavoro: le linee guida del Garante per posta elettronica e internet, doc. *web* n. 1387522. Cfr. altresì GPDP, Provv. 1° febbraio 2018, doc. *web* n. 8159221, nel quale si è rilevato che «il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione avanzata dalla società risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento». Sul punto, cfr. anche EDPB, Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità, 9 marzo 2021, versione 2.0, p. 30, che ha osservato che i dati commerciali (quali informazioni di identificazione dell'interessato, dati relativi alle operazioni, dati relativi ai mezzi di pagamento, ecc.) «possono essere conservati in una banca dati attiva per l'intera durata del contratto. Al termine del contratto possono essere archiviati fisicamente (su un supporto distinto, ad esempio DVD) o logicamente (tramite gestione delle autorizzazioni) nell'eventualità di un contenzioso. Successivamente, una volta scaduti i termini legali di prescrizione, i dati devono essere cancellati o resi anonimi».

sistematica del regolamento europeo e, in particolare, dell'art. 17, par. 3 GDPR, il quale, tra le limitazioni del diritto alla cancellazione, prevede espressamente il caso in cui il trattamento sia necessario per «l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

I principi di privacy *by design* e *by default* (art. 25 GDPR)[30] richiedono che l'attuazione del principio in esame avvenga fin dalla progettazione e per impostazione predefinita «tramite misure tecniche ed organizzative adeguate»[31]. In particolare, devono essere adottate funzioni e procedure interne per la cancellazione e/o l'anonimizzazione dei dati al termine del periodo predefinito[32]. Ove possibile, tali operazioni dovrebbero avvenire con modalità automatiche soggette a controlli periodici circa il relativo funzionamento[33]. Inoltre, ai sensi del *considerando* n. 39 del Regolamento, il titolare deve implementare politiche interne per l'attuazione di verifiche periodiche dei dati «onde assicurare che i dati personali non siano conservati più a lungo del necessario»[34].

La cancellazione e l'anonimizzazione dei dati devono essere attuate in modo specifico, per ogni tipologia di dato raccolto, e in relazione allo scopo perseguito in concreto dal titolare, «evitando dunque il riferimento "a blocchi" di fasce temporali

---

[30] Sulla protezione dei dati fin dalla progettazione e per impostazione predefinita si rinvia a F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *op. cit.*, pp. 775 ss.; G. SCORZA, *Commento all'art. 25. Protezione dei dati fin dalla progettazione e protezione dei datti per impostazione predefinita*, in G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *op. cit.*, pp. 245 ss.

[31] Per un approfondimento sui modelli organizzativi e la gestione operativa del principio di limitazione della conservazione, si rinvia a I.M. ALAGNA, *Diritto all'oblio e mancato oscuramento dei dati sensibili*, Milano, 2023, pp. 61 ss.; M. ENZMANN-A. SELZER-D. SPYCHALSKI, *Data Erasure under the GDPR. Steps towards Compliance*, in *European data protection law review*, 2019, 3, p. 416 ss.

[32] Sul punto, cfr. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *GDPR developer's guide*, Fogli 7 e 14, consultabile al sito www.cnil.fr/en/gdpr-developers-guide, nel quale l'autorità di controllo francese (CNIL) propone di dividere il ciclo di conservazione del dato personale in tre fasi successive: *database* attivo, archiviazione intermedia e archiviazione finale o cancellazione. Segnatamente, i dati devono essere conservati nell'archivio attivo e accessibili dai servizi operativi sino al raggiungimento della finalità di trattamento. L'accesso all'archivio intermedio e l'estrazione di dati dallo stesso deve essere possibile solo ove necessario ed esclusivamente per i soggetti responsabili dello specifico servizio. Inoltre, devono essere previste specifiche modalità di accesso ai dati archiviati il cui utilizzo può avvenire solo per motivazioni *ad hoc* ed eccezionali. Il CNIL raccomanda inoltre di registrare, sotto forma di dati di *log*, la cancellazione automatica dei dati personali al fine della relativa prova e di utilizzare per la cancellazione e anonimizzazione dei dati personali le stesse modalità adottate per la gestione del diritto alla cancellazione, così da garantire un funzionamento omogeneo dei sistemi. In senso analogo, cfr. EDPB, *Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità*, cit., p. 30.

[33] In tal senso, v. G. BUTTARELLI, *op. cit.*, p. 262, che, già nella vigenza della l. 675/96, evidenziava l'utilità di un «*software* che realizzi un "oblio artificiale", attraverso la cancellazione programmata e periodica dei dati "remoti"».

[34] In tal senso, cfr. EDPB, *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*, 13 novembre 2019, pp. 22-23. In dottrina, v. P. VOIGT-A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR) A Practical Guide*, Cham, 2017, p. 92.

omogenee»[35]. A tal fine, devono essere considerati tutti i dati trattati dal titolare, ivi incluse le eventuali copie di *back up*[36] e i dati di *log*[37].

Per quanto riguarda i trattamenti operati dal responsabile del trattamento, il principio trova la propria estrinsecazione *sub* art. 28, par. 3, GDPR, il quale richiede che, con il contratto[38] per la designazione del responsabile, venga determinata anche la durata del trattamento[39]. La disposizione in parola prevede inoltre, tra i contenuti obbligatori dell'atto di designazione, l'obbligo per il responsabile di cancellare o restituire, su scelta del titolare, tutti i dati personali al termine dei servizi prestati. Tali disposizioni si traducono, a livello sistematico, nella contrattualizzazione degli elementi necessari per l'applicazione del principio anche nei confronti del responsabile[40]. Come poc'anzi anticipato, si rileva che il regolamento fa salva la conservazione dei dati da parte del responsabile – anche in contrasto con le istruzioni del titolare – qualora tale conservazione sia prevista dal diritto dell'Unione Europea o degli Stati membri.

Il testo adottato dal legislatore europeo con l'art. 5, par. 1, lett. *e)*, GDPR, consente di ritenere che il principio di limitazione della conservazione possa esse-

[35] Cfr.: GPDP, Provv. 9 gennaio 2020, *Provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A.*, doc *web*. n. 9263597. Cfr. altresì GPDP, Provv. 22 luglio 2021, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l., doc *web*. n. 9685994; GPDP, Provv. 10 giugno 2021, cit.; GPDP, Provv. 24 novembre 2022, Ordinanza ingiunzione nei confronti di Areti S.p.A., doc. *web* n. 983297.

[36] Sul punto, cfr. GPDP, Provv. 26 marzo 2020, Parere alla Provincia autonoma di Trento su uno schema di regolamento concernente il funzionamento del Registro Tumori, doc. *web* n. 9344651, nel quale, è stata ritenuta opportuna la conservazione dei *back up* del registro tumori, effettuati per consentire il ripristino dei dati in caso di guasti e malfunzionamenti del sistema, per un termine «nell'ordine di grandezza di mesi e non superiore all'anno». In dottrina, cfr. M. Enzmann-A. Selzer-D. Spychalski, *op. cit.*, pp. 419-420, ove è stata messa in luce la potenziale conflittualità tra l'obbligo di implementazione di politiche di *back up*, quale misura di sicurezza adeguata *ex* art. 32 GDPR, e l'obbligo di cancellazione dei dati personali; in particolare, gli autori ritengono sufficiente nella pratica che il titolare assicuri che, in caso di ripristino di dati personali da copia di *back up*, i dati personali previamente cancellati dal sistema non siano ivi rintrodotti per l'effetto del ripristino e che i *back up* siano ripristinati solo in caso di effettiva necessità a seguito di incidente di sicurezza.

[37] In tal senso, cfr. Gruppo di lavoro articolo 29, *Parere 05/2012 sul cloud computing*, luglio 2012, pp. 13 ss., e EDPB, *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*, cit., p. 23. Sulla conservazione dei dati di *log*, cfr.: GPDP, Provv. 27 novembre 2008, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, doc. *web* n. 1577499, il quale prevede un termine di conservazione per i dati di log non inferiore a sei mesi per gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema; GPDP, Provv. 12 maggio 2011, Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, doc. *web* n. 1813953, in base al quale il periodo di conservazione dei file di *log* delle operazioni di *inquiry*, in ambito bancario, non deve essere inferiore a 24 mesi dalla data di registrazione dell'operazione.

[38] In tal senso, cfr. A. Chiappini, *Riflessioni sul contratto tra titolare e responsabile del trattamento*, in *Contratto e impresa*, 2021, 1, pp. 317 ss.

[39] Cfr. EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, versione 1.0, 2 settembre 2020, p. 33, il quale prevede che la durata del trattamento possa essere determinata nella nomina del responsabile tramite un esatto periodo di tempo o tramite specifici criteri di calcolo.

[40] Sul punto si veda, ancora, A. Chiappini, *Riflessioni sul contratto tra titolare e responsabile del trattamento*, cit., p. 328.

re attuato non solo tramite la cancellazione dei dati personali ma anche attraverso l'anonimizzazione degli stessi[41]. Non risulta invece sufficiente la pseudoanonimizzazione, posto che tale operazione non esclude la possibilità di attribuire i dati ad un interessato specifico tramite l'utilizzo di informazioni aggiuntive[42].

La cancellazione o l'anonimizzazione dei dati personali potrebbero non essere sempre tecnicamente possibile. Sul punto, vi è chi ha rilevato che il GDPR non definisce la nozione di «*cancellazione*», la quale potrebbe essere interpretata, in via estensiva, come inaccessibilità[43]. Tale impostazione potrebbe trovare un sostegno normativo nel disposto di cui all'art. 25, par. 1 GDPR, il quale prevede che le misure organizzative e tecniche adeguate per l'attuazione dei principi di cui all'art. 5 GDPR, debbano essere attuate «*tenendo conto dello stato dell'arte e dei costi di attuazione*»[44]. Di contro, si rileva che il GDPR, in materia di diritti dell'interessato, è molto chiaro nel distinguere tra cancellazione dei dati e limitazione del trattamento; distinzione che invece risulta assente nell'art. 5, par. 1, lett. *e*), GDPR che si riferisce espressamente (ed esclusivamente) alla perdita del potere identificativo del dato. In favore della prima tesi, si registra che la normativa nazionale tedesca, in relazione al diritto all'oblio, prevede che il titolare possa procedere con la limitazione del trattamento, anziché con la cancellazione dei dati, qualora ciò sia reso impossibile dalle specifiche modalità di conservazione[45]. Anche l'autorità per la protezione dei dati inglese, l'*Information Commisioner's Office* (ICO), rilevando che non è sempre possibile eliminare tutte le «*tracce*» dei dati personali, riconosce che la questione chiave per la limitazione della conservazione sia la cessazione dell'utilizzo dei dati personali[46].

Le riflessioni che precedono trovano immediata applicazione alla tecnologia *blockchain.* Com'è noto, tale tecnologia integra, in sintesi, un registro distribuito ed immodificabile di eventi digitali occorsi tra i relativi partecipanti, protetto tramite crittografia a chiave asimmetrica[47]. Sebbene alcune caratteristiche della *blockchain*

---

[41] In relazione all'anonimizzazione dei dati personali, si rinvia a GRUPPO DI LAVORO ARTICOLO 29, *Opinion 05/2014 on Anonymisation Techniques*, 10 aprile 2014.

[42] Cfr. art. 4, n. 5, GDPR.

[43] In tal senso, cfr. M. FINCK, *Blockchains and Data Protection in the European Union*, in *Max Planck Institute for Innovation & Competition Research Paper*, 2018, 1, pp. 17 ss.

[44] A sostegno di tale tesi, si rileva che lo stesso art. 17, par. 2, GDPR, in relazione al diritto alla cancellazione, prevede che, qualora il titolare del trattamento abbia reso pubblici i dati personali e sia oggetto di una richiesta di cancellazione, debba informare gli altri titolari che stanno trattando i dati «tenendo conto della tecnologia disponibile e dei costi di attuazione». Sul punto, cfr. A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Torino, 2017, la quale rileva che l'art. 17, GDPR, «*sancisce in capo al titolare del trattamento un'obbligazione di mezzi e non di risultato*». Sul concetto di cancellazione ai sensi dell'art. 17 GDPR, cfr. altresì F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *op. cit.*, pp. 353 ss.

[45] Cfr. art. 35 del *Federal Data Protection Act* del 30 giugno 2017 (*Federal Law Gazette* I p. 2097), come modificato dall'art. 12 del *Act* del 20 novembre 2019 (*Federal Law Gazette* I, p. 1626).

[46] In tal senso, si veda la guida dell'INFORMATION COMMISIONER'S OFFICE (ICO), *cit.*

[47] Cfr. L. PAROLA-P. MERATI-G. GAVOTTI, *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018, 6, p. 681 ss. i quali descrivono nel dettaglio la *blockchain* come «(…) una tec-

(*in primis*, la pseudoanonimizzazione e la crittografia) ne facciano uno strumento in grado di assicurare un elevato grado di tutela dei dati ivi contenuti, sono stati sollevati diversi interrogativi sulla compatibilità della tecnologia con le norme in materia di protezione dei dati personali[48]. Per quanto qui interessa, l'impossibilità di cancellare i dati personali dal registro appare *prima facie* in contrasto con la norma di cui all'art. 5, par. 1, lett. *e)*, GDPR[49] [50].

Sul punto, è stato rilevato che la finalità di trattamento – quale parametro di valutazione della durata della conservazione – potrebbe essere individuata sia nella singola operazione effettuata tramite la *blockchain* che nel funzionamento della tecnologia[51]. In accordo a questa seconda interpretazione, considerate le caratteristiche di immutabilità della *blockchain*, sarebbe lo stesso funzionamento della tecnologia, se considerata quale finalità del trattamento, ad imporre la conservazione dei dati in perpetuo. Si tratterebbe però di interpretazione non condivisibile, perché cozzerebbe sia con la *ratio* della disciplina in tema di protezione dei dati personali, sia con la natura solamente temporanea del trattamento, sia con la sostanziale indisponibilità del diritto alla protezione dei dati personali, che non tollera trattamenti *sine die*.

Inoltre, come anticipato, il combinato disposto di cui agli artt. 5, par. 1, lett. *e)*, e 25, par. 1, GDPR, prevede che le misure organizzative e tecniche adeguate volte ad attuare il principio di limitazione della conservazione debbano essere attuate «tenendo conto dello stato dell'arte e dei costi di attuazione». Tale norma potrebbe aprire a soluzioni alternative alla cancellazione del dato compatibili con la tecnologia

---

nologia finalizzata alla gestione di transazioni attraverso la creazione di un *database* distribuito tra gli utenti di una rete (1). In altre parole, essa consiste in un registro pubblico e condiviso in grado di aggiornarsi automaticamente su ciascuno dei client che partecipano alla catena (i cc.dd. nodi). Tale registro è strutturato in blocchi, ognuno dei quali rappresenta un numero di transazioni la cui provenienza e ora di esecuzione sono attribuite in modo indelebile e immutabile, rispettivamente, attraverso un meccanismo di crittografia a chiave asimmetrica (2) e una marcatura temporale (il c.d. *timestamping*). Ciascun blocco è collegato irreversibilmente a quello precedente tramite una particolare operazione logaritmica (la c.d. funzione di *hash* (3)) e forma, in tal modo, la catena di blocchi (il *blockchain* appunto) accessibile e consultabile da tutti i nodi della rete. Prima di essere aggiunto alla catena, ogni blocco è controllato, validato e crittografato da alcuni dei nodi (cc.dd. *miner*) tramite la soluzione di un'operazione matematica (4) e risulta così a prova di manomissione (5)».

[48] Sulla tecnologia *blockchain* e la sua conformità al GDPR, cfr.: A.M. Gambino-C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Il Diritto dell'informazione e dell'informatica*, 2019, 3, pp. 619-646; F. Sarzana di S'Ippolito-M. Nicotra, *Diritto della blockchain, intelligenza artificiale e Iot*, Milano, 2018, pp. 85 ss.; P. Gallo, *DLT,* blockchain *e* smart contract*,* in M. Cian-C. Sandei (a cura di), *Diritto del Fintech*, Milano, 2020, pp. 137 ss.; M. Finck, *op. cit.*, pp. 17 ss.; M. Berberich-M. Steiner, *Blockchain Technology and the GDPR. How to Reconcile Privacy and Distributed Ledgers*, in *European data protection law review*, 2016, 3, pp. 422 ss.

[49] Analoghe considerazioni possono essere dispiegate per il diritto di rettifica e il diritto all'oblio di cui agli artt. 16 e 17 del Regolamento. In tal senso, v.: A.M. Gambino-C. Bomprezzi, *op. cit.*, p. 642; F. Sarzana di S'Ippolito-M. Nicotra, *op. cit.*, pp. 84 ss.

[50] Secondo A.M. Gambino-C. Bomprezzi, *op. cit.*, p. 642, le citate frizioni tra il GDPR e l'immutabilità della *blockchain* si pongono per la *blockchain* di tipo *permissionless*, mentre sono ridotte in caso di *blockchain* del tipo *permissioned* e inesistenti nelle *blockchain* private.

[51] Cfr. M. Berberich-M. Steiner, *op. cit.*, p. 426.

blockchain[52]. Ad esempio, risulterebbe possibile anonimizzare i dati contenuti nella *blockchain* eliminando quegli strumenti che consentono l'identificazione dell'interessato, quale la chiave crittografica[53].

3. Applicazione del principio nella casistica

3.1. Il principio di limitazione della conservazione nei provvedimenti del Garante per la protezione dei dati personali

3.1.1. *Il mutato approccio in materia di limitazione della conservazione: dai provvedimenti generali del Garante (o resi a seguito di verifica preliminare) all'applicazione del principio di* accountability

Esaminato il contesto normativo e la portata del principio in esame, l'analisi che si sta conducendo mira ora ad approfondire la casistica relativa a tale principio, nel tentativo di individuarne, in una prospettiva giusrealista, le più significative implicazioni al cospetto delle fattispecie concrete.

Come si vedrà, il principio di limitazione della conservazione ha trovato un primo riconoscimento nei provvedimenti del Garante per la protezione dei dati personali (Garante) tesi a dare applicazione, prima, alla Direttiva 95/46/CE e, poi, al GDPR. Ulteriori chiavi di lettura sono state fornite dalle corti europee (Corte EDU e CGUE), le quali si sono pronunciate sui tempi di conservazione imposti da disposizioni normative nazionali e sovranazionali. Da ultimo, la presente analisi non potrà prescindere da alcuni cenni sul diritto all'oblio che, come poc'anzi menzionato, risulta strettamente connesso al principio *de quo*.

Sotto la vigenza della Direttiva e delle relative norme di attuazione, il principio di limitazione della conservazione ha trovato ampia applicazione nei provvedimenti del Garante. Si richiamano, *in primis*, i numerosi provvedimenti generali di settore e le linee guida[54] che, di volta in volta, hanno prescritto dei termini massimi

[52] L'apertura a soluzioni alternative rispetto alla cancellazione o anonimizzazione del dato trova altresì sostegno nelle considerazioni precedentemente dispiegate in ordine alla nozione di «*cancellazione*» e alla relativa interpretazione estensiva come «*inaccessibilità*». In tal senso, cfr. A.M. GAMBINO-C. BOMPREZZI, *op. cit.*, p. 642.

[53] Cfr. M. BERBERICH-M. STEINER, *op. cit.*, p. 425, i quali, per l'implementazione dei principi in materia di dati personali alla *blockchain*, propongono le seguenti soluzioni: «*This may include eliminating ways that would allow tracking back pseudonyms to individual users, or adding 'noise' to BC data so that transactions are mixed up. Another promising idea is to combine on chain and off chain storage for more sensible data and using BC only as a 'pointer' to centrally stored data, as it is the case in the MIT 'ENIGMA' project, which uses modified distributed hashtables for storing secret shared data in combination with an external BC for network, access and identity control*».

[54] Cfr., senza pretese di esaustività, i seguenti provvedimenti: in materia di amministratore di sistema, GPDP, Provv. 27 novembre 2008, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, doc. *web* n. 1577499; in ambito bancario, GPDP, Provv. 25 ottobre 2007, Linee guida

di conservazione dei dati per ciascuna finalità considerata. L'estensione dei tempi prescritti risultava in allora ammissibile, a fronte di speciali esigenze del titolare, previa verifica preliminare del Garante, ai sensi dell'art. 17 della previgente versione del Codice[55].

Il predetto approccio è mutato con l'avvento del GDPR e il riconoscimento normativo del principio di *accountability*, di cui all'art. 5, par. 2, GDPR, che impone ai titolari del trattamento di «mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento»[56] rispetto alle norme del GDPR. In base a tale principio, non spetta più, di norma, alle autorità di controllo determinare astrattamente la durata del trattamento. È, bensì, compito del titolare del trattamento fare concreta applicazione del principio di limitazione della conservazione decidendo, caso per caso, i tempi di conservazione dei dati, conformemente ai principi di necessità e proporzionalità[57].

Per quanto riguarda i termini di conservazione individuati dal Garante prima dell'entrata in vigore del GDPR, deve ritenersi che il titolare possa continuare a farvi riferimento. Purtuttavia, in presenza di speciali ed effettive esigenze, risulta possibile

per trattamenti dati relativi al rapporto banca-clientela, doc. *web* n. 1457247; in ambito giudiziario, GPDP, Provv. 26 giugno 2008, Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero, doc. *web* n. 1534086; in materia di lavoro, GPDP, Provv. 23 novembre 2006, Linee guida sul trattamento di dati personali dei lavoratori privati, doc. *web* n. 1364939, e Provv. 1° marzo 2007, Lavoro: le linee guida del Garante per posta elettronica e internet, doc. *web* n. 1387522; in materia di *marketing* e profilazione, GPDP, Provv. 3 febbraio 2005, TV interattiva: misure necessarie ed opportune per un trattamento dei dati conforme alle disposizioni vigenti, doc. *web* n. 1109503, GPDP, Provv. 24 febbraio 2005, "Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione, doc. *web* 1103045; in materia di pubblicità e trasparenza della pubblica amministrazione, GPDP, Provv. 15 maggio 2014, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, doc. *web* n. 3134436; in ambito sanitario, GPDP, Provv. 24 luglio 2008, Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali, doc. *web* n. 1533155, GPDP, Provv. 16 luglio 2009, Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario, doc. *web* n. 1634116, GPDP, Provv. 19 novembre 2009, Linee guida in tema di referti on-line, doc. *web* n. 1679033, GPDP, Provv. 5 maggio 2011, Linee guida in tema di trattamento di dati per lo svolgimento di indagini di customer satisfaction in ambito sanitario, doc. *web* n. 1812910, e GPDP, Provv. 4 giugno 2015, Linee guida in materia di Dossier sanitario, doc. *web* n. 4084632; in materia di videosorveglianza, GPDP, Provv. 8 aprile 2010, Provvedimento in materia di videosorveglianza, doc. *web* n. 1712680.

[55] Cfr. parr. 3.1.2. ss.

[56] Cfr. *considerando* n. 74, GDPR.

[57] In tal senso, cfr. EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, 29 gennaio 2020, versione 2.0, p. 31; GPDP, Provv. 15 ottobre 2020, doc. *web* n. 9486485, e GPDP, Provv. 22 maggio 2018, Verifica preliminare. Estensione dei tempi di conservazione di dati personali riguardanti la clientela per attività di profilazione e di marketing, doc. *web* n. 9022048. In tal senso cfr. altresì, G. Scorza, Marketing e videosorveglianza (Scorza: «Spetta al titolare stabilire i termini di liceità del trattamento». Intervento di Guido Scorza), doc. *web* n. 9500127, consultabile al sito www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9500127, secondo il quale «anche alcuni dei termini di conservazione fissati dal Garante per la protezione dei dati personali prima dell'entrata in vigore del Regolamento devono, oggi, essere superati da scelte autonome e responsabili dei titolari del trattamento».

per il titolare superare, in autonomia, tali termini[58]. Qualora il prolungamento della conservazione dei dati possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare sarà tenuto ad effettuare una valutazione d'impatto *ex* art. 35 GDPR e, ove necessario, alla consultazione preventiva dell'autorità di controllo *ex* art. 36 GDPR.

Nei paragrafi che seguono, verranno pertanto esaminati i più significativi ambiti della casistica su cui è intervenuto il Garante, con l'obiettivo di fornire al lettore una chiave applicativa del principio in esame[59]. Verranno, altresì, prese in considerazione le Regole deontologiche, oggetto di recente verifica da parte del Garante circa la relativa conformità al GDPR[60].

3.1.2. *I provvedimenti in materia di lavoro*

Il trattamento di dati personali nell'ambito del rapporto di lavoro è stato oggetto di grande attenzione da parte del Garante, specie in relazione a quegli strumenti tecnologici da cui possa derivare un controllo a distanza dei lavoratori[61]. Non potendo esaurire l'intera casistica nel presente paragrafo, ci si soffermerà su quegli ambiti che sono stati interessati, con maggiore frequenza, dall'autorità di controllo italiana a partire dai provvedimenti di carattere generale.

Nel 2007, si è assistito all'adozione di specifiche linee guida per l'uso della posta elettronica e della rete Internet da parte dei lavoratori[62]. Tale provvedimento, richiamando il principio in esame, dispone che l'allungamento dei tempi di trattamento ordinariamente previsti – specificati nel prosieguo della trattazione – debba avere carattere eccezionale ed essere giustificato in forza di «esigenze tecniche o di sicurezza del tutto particolari», dell'«indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria» o dall'«obbligo di custodire o conse-

[58] Cfr. G. SCORZA, *op. cit.* Sul punto, cfr. altresì GPDP, Provv. 18 luglio 2023, cit., par. 9.5, in materia di marketing e profilazione, nel quale l'autorità garante, pur valorizzando il principio di accountability, ha riconosciuto che il provvidemento generale del 2005 "Fidelity card' e garanzie per i consumatori", sebbene non presenti più carattere vincolante, «è da considerarsi ancora applicabile con valore di linea guida e pertanto lo è anche la tempistica ivi prevista», tempistica dalla quale il titolare del trattamento non può «scostarsi in modo eccessivo».

[59] Ai sensi dell'art. 22, co. 4, d.lgs. n. 101/2018, a decorrere dal 25 maggio 2018, i provvedimenti del GPDP continuano ad applicarsi, in quanto compatibili con il GDPR e con le disposizioni del predetto decreto.

[60] Cfr. art. 20, d.lgs. n. 101/2018.

[61] Sul trattamento dei dati personali nell'ambito del rapporto di lavoro, cfr. V. TURCO, *Il trattamento dei dati personali nell'ambito del rapporto di lavoro*, in CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *op. cit.*, pp. 517 ss., C. DEL FEDERICO, *Trattamento dei dati nell'ambito del rapporto di lavoro*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., pp. 629 ss., e M. PANETTA, *I controlli aziendali e le indagini difensive*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, Milano, 2019, pp. 367 ss.

[62] Cfr. GPDP, Provv. 1° marzo 2007, Lavoro: le linee guida del Garante per posta elettronica e internet, doc. *web* n. 1387522.

gnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria»[63].

Con particolare riferimento al sistema di posta elettronica aziendale, il Garante ha ritenuto necessario che alla cessazione del rapporto di lavoro, «il titolare del trattamento provveda alla rimozione dell'*account*, previa disattivazione dello stesso e contestuale adozione di sistemi automatici volti ad informarne i terzi e a fornire a questi ultimi indirizzi *e-mail* alternativi riferiti alla sua attività professionale»[64]. Viceversa, l'autorità ha censurato la conservazione sistematica dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli *account* aziendali per periodi prolungati, come un arco di tempo pari a dieci anni[65] o per tutta la durata del rapporto di lavoro e, successivamente, per periodi di uno e dodici mesi rispettivamente per gli impiegati e i dirigenti o altre figure apicali[66]. Infatti, tali termini non sono stati ritenuti proporzionati rispetto «alle ordinarie necessità di gestione dei servizi di posta elettronica, comprese le esigenze di sicurezza dei sistemi»[67], né si è ritenuto che possano essere giustificati nell'ipotetica eventualità di una controversia[68]. È stata comunque ritenuta ammissibile la «messa a disposizione del dipendente dell'intero archivio delle *email* scambiate tramite il proprio account aziendale» a condizione che vengano impartite istruzioni allo stesso di verifica e

[63] *Ibidem*, par. 6.2, nel quale il Garante prescrive che «I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la c.d. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria».

[64] Cfr. GPDP, Provv. 7 aprile 2022, Ordinanza ingiunzione nei confronti di Palumbo Superyacht Ancona s.r.l., doc. *web* n. 9771545, par. 2. Cfr. altresì: GPDP, Provv. 21 luglio 2022, Ordinanza ingiunzione nei confronti di Stay Over s.r.l., doc. *web* n. 9809466; GPDP, Provv. 16 dicembre 2021, Ordinanza ingiunzione nei confronti di Corradi s.r.l., doc. *web* n. 9739653; GPDP, Provv. 29 settembre 2021, Ordinanza ingiunzione nei confronti di Solera Italia s.r.l., doc. *web* n. 9719914; GPDP, Provv. 29 ottobre 2020, Ordinanza ingiunzione nei confronti di Gaypa s.r.l., doc. web n. 9518890; GPDP, Provv. 2 luglio 2020, Ordinanza ingiunzione nei confronti di Mapei S.p.A., doc. *web* n. 9445180; GPDP, Provv. 4 dicembre 2019, doc. *web* n. 9215890; GPDP, Provv. 1° febbraio 2018, Trattamento di dati personali effettuato sugli account di posta elettronica aziendale, doc. *web* n. 8159221. Cfr. altresì Consiglio di Europa, *Raccomandazione del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale*, 1 aprile 2015, CM/Rec(2015)5, par. 14.5, che afferma: «Al cessare del rapporto di lavoro con un dipendente, il datore di lavoro dovrebbe prendere tutte le misure tecniche ed organizzative necessarie per disattivare automaticamente *l'account* di messaggeria elettronica del dipendente. Se un datore di lavoro ha necessità di recuperare i contenuti riferiti all'*account* di un dipendente ai fini dell'efficace gestione dell'impresa/dell'ente, ciò dovrebbe avvenire prima della cessazione del rapporto di lavoro del dipendente in oggetto e, se possibile, alla presenza di quest'ultimo».

[65] Cfr. GPDP, Provv. 22 dicembre 2016, Accesso alla posta elettronica dei dipendenti, doc. *web* n. 5958296, par. 3.3.

[66] Cfr. GPDP, Provv. 1° febbraio 2018, cit., par. 3.2.

[67] Cfr. GPDP, Provv. 22 dicembre 2016, cit., par. 3.3.

[68] Cfr. GPDP, Provv. 1° febbraio 2018, cit., par. 3.2, il quale sul punto dispone che «il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti».

cancellazione periodica dei messaggi conservati e che a tale account possa accedere solo il dipendente a cui è intestato l'*account* medesimo[69].

Per quanto riguarda i sistemi di *logging* della posta elettronica per il sicuro funzionamento del servizio, l'autorità italiana ha espressamente limitato la conservazione dei dati esteriori del messaggio, c.d. *envelope*, per un arco di tempo non superiore a sette giorni[70].

Di recente, è stata, inoltre, censurata la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, per generiche finalità di sicurezza informativa, per un periodo di 180 giorni, ritenendo tale termine non giustificato dal perseguimento di tali finalità e da contenersi «in ogni caso entro limiti temporali ben più ristretti»[71].

Nel 2011, il Garante è nuovamente intervenuto in materia di rapporto di lavoro con il provvedimento generale sui sistemi di localizzazione dei veicoli[72]. Si tratta di quegli strumenti installati dal datore di lavoro a bordo dei veicoli aziendali, in genere, per esigenze organizzative, produttive e di sicurezza, con possibilità di localizzare la posizione dei lavoratori a cui è assegnato il veicolo.

Con riferimento al principio *de quo*, l'autorità italiana si è espressa escludendo, di regola, il monitoraggio continuativo della posizione del veicolo, la quale deve essere registrata solo quando necessario per le finalità perseguite. Anche per quanto riguarda la conservazione dei dati così raccolti, il Garante ha fatto rinvio alle finalità concrete di raccolta di ciascuna tipologia di dato coinvolto nel trattamento. Così, in relazione alla tenuta del libro unico del lavoro, si è ritenuta ammissibile la conservazione per cinque anni dei dati personali necessari a tale scopo, quali i dati relativi alla presenza, ai tempi di lavoro, anche straordinario, e di riposo[73].

L'autorità garante è successivamente intervenuta con svariati provvedimenti nell'esame di richieste di verifica preliminare da parte di soggetti pubblici e privati, fornendo utili direttive. Tali provvedimenti hanno riguardato la localizzazione dei dipendenti anche tramite altri dispositivi in dotazione agli stessi, quali gli *smartphone* aziendali[74].

Con riferimento ad una società attiva nei servizi di vigilanza, si è ammessa la localizzazione geografica dei dispositivi *smartphone* o *tablet* consegnati alle guardie giurate, per finalità organizzative e di sicurezza. In tal caso, il Garante ha ritenuto

---

[69] *Ibidem*.

[70] Cfr. GPDP, Provv. 13 luglio 2016, doc. *web* n. 5408460, par. 4.3.

[71] Cfr. GPDP, Provv. 1° dicembre 2022, Ordinanza di ingiunzione nei confronti di Regione Lazio, doc. *web* n. 9833530, par. 3.7. Sul punto, cfr. altresì, GPDP, Provv. 13 luglio 2016, cit., e GPDP, Provv. 29 ottobre 2020, cit.

[72] Cfr. GPDP, Provv. 4 ottobre 2011, Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro, doc. *web* n. 1850581.

[73] *Ibidem*, par. 3. In tal senso, cfr., altresì, GPDP, Provv. 7 luglio 2011, Localizzazione dei veicoli aziendali a prova di privacy. Verifica preliminare presentata da Loex s.r.l., doc. *web* n. 1828371, e GPDP, Provv. 8 settembre 2016, Verifica preliminare. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze, doc. *web* n. 5497522.

[74] Cfr. GPDP, Provv. 18 maggio 2016, Trattamento di dati personali effettuato attraverso la localizzazione di dispositivi *smartphone*, doc. *web* n. 5217175.

congrua la frequenza della rilevazione della posizione effettuata dal sistema ogni due minuti rispetto alla «necessità di predisporre con urgenza interventi a tutela della pattuglia in caso di aggressione oppure a tutela di persone e beni in caso di segnalazione di illeciti in corso»[75]. Detta valutazione ha tenuto in considerazione anche il termine breve di memorizzazione dei dati di localizzazione pari a ventiquattro ore, ferma l'ulteriore conservazione per l'adempimento degli obblighi normativi di settore[76].

Parimenti, il Garante ha ritenuto di accogliere la richiesta di verifica preliminare relativa all'installazione di un sistema di localizzazione satellitare sui veicoli in uso alla polizia locale per finalità statistiche, di sicurezza del personale, di ottimizzazione dell'uso operativo del personale e dei veicoli e di indagine, escludendo, viceversa, l'uso dei dati raccolti per scopi disciplinari. Per tale fattispecie, il Garante ha accolto la richiesta di rilevazione dei dati di localizzazione ogni 30 secondi, attesa la «necessità di coordinare le attività e gestire eventuali situazioni di criticità ed emergenze»[77], nonché il fatto che il sistema, alla fine del turno, non consentisse l'ulteriore identificabilità degli operatori[78]. Il periodo di conservazione dai dati così raccolti è stato individuato in 30 giorni allo scopo di rendicontazione delle spese di servizio[79].

Inoltre, il Garante ha considerato proporzionato l'utilizzo della geolocalizzazione di dispositivi in dotazione ai dipendenti per finalità di miglioramento del servizio di supporto alla clientela, di supporto in attività emergenziali e di sicurezza del personale, con periodizzazione temporale della localizzazione ogni dieci minuti e cancellazione, ad ogni nuova registrazione, della precedente[80].

Risulta altresì consentita la localizzazione del personale non su base temporale ma al verificarsi di determinati eventi. Ad esempio, con riferimento ad una società di logistica, si è ammessa la registrazione della posizione dei corrieri al fine di digitalizzare i documenti di trasporto e incrementare l'automazione dei processi operativi, al verificarsi di una serie di eventi predefiniti, quali, ad esempio, la consegna e il ritiro della merce o la richiesta d'aiuto[81]. La conservazione di tali dati è stata distinta in relazione alle diverse finalità perseguite: per finalità di miglioramento dei servizi i

[75] Cfr. GPDP, Provv. 18 aprile 2018, Verifica preliminare. Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali, doc. *web* n. 9358266.

[76] *Ibidem*.

[77] Cfr. GPDP, Provv. 29 marzo 2018, Verifica preliminare. Installazione di un sistema di localizzazione satellitare sui veicoli in uso alla polizia locale, doc. *web* n. 8576577.

[78] *Ibidem*.

[79] *Ibidem*.

[80] Cfr. GPDP, Provv. 30 marzo 2017, Verifica preliminare. Attivazione di una funzionalità di localizzazione di telefoni cellulari o altri strumenti (device) forniti da una società ai propri agenti di vendita, doc. *web* n. 6407700, e GPDP, Provv. 9 ottobre 2014, Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a., doc. *web* n. 3505371.

[81] Cfr. GPDP, Provv. 15 giugno 2017, Verifica preliminare. Trattamento di dati personali connesso all'utilizzo di un dispositivo informatico multifunzione (mobile worker Incab) da parte degli autisti dei furgoni di un'azienda, doc. *web* n. 6697925.

dati possono essere usati solo se anonimizzati e aggregati mentre per le altre finalità è stato fissato un termine pari a centoventi giorni[82].

Si è altresì accolta la richiesta di verifica preliminare rispetto a sistemi di registrazioni audio e video e di rilevamento della posizione e ad altre informazioni sui movimenti del veicolo, al verificarsi di determinate condizioni tali da far presumere che il mezzo sia stato coinvolto in un incidente. In particolare, è stata valutata congrua la conservazione dei predetti dati per ventiquattro mesi, in considerazione dei termini prescrizionali per il risarcimento del danno da circolazione del veicolo *ex* art. 2947, co. 2, c.c. [83].

In altri casi, si è ritenuta proporzionata la conservazione dei dati relativi alla localizzazione del personale dipendente per un periodo pari a novanta giorni, per finalità di tutela in caso di contestazione di violazione amministrativa con modalità non immediata[84] e due anni, a fronte di concrete necessità di rendicontazione presso la pubblica amministrazione[85].

Con riferimento all'uso dei telefoni aziendali, risulta altresì ammessa la raccolta – tramite sistemi Voip o comunicazione del provider del servizio di telefonia – dei dati relativi alle chiamate operate dai dipendenti, quali numero chiamato o chiamate, giorno e ora dell'inizio della chiamata e durata della stessa, per finalità di verifica delle fatture correlate nonché per il contenimento dei costi e per far fronte ad eventuali contestazioni[86]. Il Garante ha prescritto che tali dati possano essere conservati esclusivamente per un arco di tempo non superiore a sei mesi dalla raccolta al fine di «*omogeneizzare*» i tempi di conservazione per finalità di fatturazione rispetto alla disciplina prevista dall'art. 123, co. 2, del Codice, che dispone un termine analogo per i fornitori di servizi di comunicazione elettronica[87].

3.1.3. *I provvedimenti in materia di biometria*

Negli ultimi decenni si è assistito ad un crescente uso da parte di soggetti pubblici e privati dei dati biometrici per l'accertamento dell'identità personale o per altre finalità. Le tecnologie che sfruttano la biometria sono utilizzate ormai quotidianamente al fine di regolare l'accesso ad ambienti digitali, sistemi informativi e ad aree fisiche, attivare dispositivi elettronici e macchinari e sottoscrivere documenti informatici[88].

---

[82] *Ibidem*.

[83] Cfr. GPDP, Provv. 16 marzo 2017, Verifica preliminare. Trattamento di dati personali di dipendenti effettuato attraverso la localizzazione di veicoli aziendali, doc. *web* n. 6275314.

[84] *Ibidem*.

[85] Cfr. GPDP, Provv. 18 febbraio 2010, Trattamento di dati personali del dipendente mediante sistemi di localizzazione satellitare, doc. *web* n. 1703103.

[86] Cfr.: GPDP, Provv. 11 gennaio 2018, *Verifica preliminare. Trattamento dei dati personali dei dipendenti cui è stato assegnato un telefono aziendale*, doc. *web* n. 7554790; GPDP, Provv. 21 luglio 2011, *Il Garante privacy al Poligrafico: più tutele per i lavoratori*, doc. *web* n. 1829641.

[87] *Ibidem*.

[88] Per un approfondimento sul trattamento di dati biometrici, cfr. R. DUCATO, *I dati biometrici*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1285 ss.

La materia in esame è stata affrontata dal Garante, con un significativo provvedimento a carattere generale, in relazione alla rilevazione di impronte digitali ed immagini per l'accesso agli istituti di credito[89]. In tale occasione, l'autorità italiana ha prescritto che i dati relativi alle impronte digitali dei clienti possano essere conservati per un periodo non superiore ad una settimana al fine di elevare, sulla base di circostanze obiettive, il grado di sicurezza di beni e persone[90].

Analoga disposizione è stata adottata dal Garante, con le Linee guida del 2006 sul trattamento di dati personali dei lavoratori privati, per la regolamentazione dell'accesso a specifiche aree aziendali da parte del dipendente[91]. I sistemi esaminati dal provvedimento prevedono la creazione di un modello di riferimento a partire dalle caratteristiche fisiche o comportamentali della persona, come l'impronta digitale, che vengono di volta in volta confrontante con quelle dell'individuo che tenta di accedere all'area riservata. Segnatamente, l'autorità garante ha prescritto che i dati biometrici necessari alla creazione del modello (*biometric enrolment*) vengano utilizzati esclusivamente per tale operazione senza possibilità di ulteriore conservazione[92]. Viceversa, la registrazione del singolo accesso del dipendente può essere registrata, di regola, per un periodo non superiore a sette giorni[93].

Successivamente, il Garante è intervenuto con le linee-guida del 2014, fornendo un quadro unitario in materia di riconoscimento biometrico e firma grafometrica[94]. Con riferimento ai termini di conservazione, analogamente a quanto rilevato in materia di lavoro, il Garante ha disposto che «i campioni biometrici impiegati nella realizzazione del modello biometrico possono essere trattati solo durante le fasi di registrazione e di acquisizione necessarie al confronto biometrico, e non devono essere memorizzati se non per il tempo strettamente necessario alla generazione del modello stesso»[95].

---

[89] Cfr. GPDP, Provv. 27 ottobre 2005, Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: limiti e garanzie, doc. *web* n. 1246675. Per un precedente, si veda anche GPDP, Provv. 28 settembre 2001, Videosorveglianza e dati biometrici. Rilevazioni biometriche presso istituti di credito, doc. *web* n. 39704.

[90] Cfr. GPDP, Provv. 27 ottobre 2005, Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: limiti e garanzie, doc. *web* n. 1246675, cit., ove è stato previsto, inoltre, che «la banca, in presenza di una richiesta di accesso da parte dell'interessato, oppure di eventi criminosi verificatisi o, ancora, di una richiesta da parte dell'autorità giudiziaria, potrà assicurare la disponibilità dei dati raccolti, evitandone l'automatica cancellazione alla scadenza del periodo di conservazione previsto».

[91] Cfr. GPDP, Provv. 23 novembre 2006, Linee guida sul trattamento di dati personali dei lavoratori privati, doc. *web* n. 1364939.

[92] Cfr. GPDP, Provv. 23 novembre 2006, cit.; cfr. altresì GPDP, Provv. 8 aprile 2019, Trattamento di dati biometrici per finalità di autenticazione di accesso a particolari aree aziendali, doc. *web* n. 1610018, e GPDP, Provv. 17 settembre 2009, Vigilanza più "vigilata" negli aeroporti, doc. *web* n. 1655708.

[93] *Ibidem*.

[94] Cfr. GPDP, Provv. 12 novembre 2014, Provvedimento generale prescrittivo in tema di biometria, doc. *web* n. 3556992, Allegato A.

[95] *Ibidem*.

Per quanto riguarda invece i «dati ottenuti tramite elaborazione di quelli precedentemente citati (modelli o riferimenti biometrici)»[96], il Garante ha fatto rinvio al principio di limitazione della conservazione in considerazione delle concrete finalità di trattamento perseguite dal titolare[97]. Per la nostra disamina, soccorrono dunque le pronunce dell'autorità italiana intervenute a fronte delle specifiche richieste di verifica preliminare.

Nell'ambito del rapporto di lavoro, si è ritenuto lecito e proporzionato il trattamento operato tramite un apparato integrato di rilevatori di impronte biometriche per l'accesso a particolari aree e ai sistemi ICT di una struttura ospedaliera[98]. Nel caso di specie, il sistema esaminato risultava basato sul «confronto tra le impronte digitali rilevate e il template, memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità dei lavoratori interessati»[99]. Il Garante ha quindi prescritto la conservazione dei «dati di *log* per l'accesso alle diverse applicazioni aziendali per fini di gestione dell'Ospedale» per un termine massimo di sei mesi e i «dati di *log* relativi agli orari di ingresso alle aree riservato» per un periodo massimo di dieci giorni[100].

In relazione ad una richiesta di verifica preliminare per un centro orafo, il Garante ha accolto l'allungamento dei termini di conservazione fino a trenta giorni dei dati rilevati dal sistema di controllo accessi biometrico, a fronte di oggettive esigenze di sicurezza correlate alla stessa attività svolta, alla collocazione della struttura in un'area ad alto tasso di criminalità e alla sua superficie molto estesa, nonché ai vari episodi delittuosi verificatisi in precedenza[101].

Con riferimento all'uso da parte di diversi istituti di credito di un sistema di rilevamento biometrico dei propri clienti per consentirne l'accesso in autonomia alle relative cassette di sicurezza, il Garante ha ritenuto proporzionato il trattamento ove non sia prevista una conservazione di tali dati in archivi centralizzati, ma il dato criptato dell'impronta digitale venga memorizzato esclusivamente sulla *smart card* in esclusiva disponibilità del cliente[102].

Sempre in ambito bancario, si richiamano le pronunce in materia di servizi di firma digitale con autenticazione grafometrica tramite *tablet* al fine di garantire

---

[96] *Ibidem*.

[97] *Ibidem*, par. 8.5.

[98] Cfr. GPDP, Provv. 15 aprile 2008, Più sicurezza in ospedale con le impronte digitali, doc. *web* n. 1523435.

[99] *Ibidem*.

[100] *Ibidem*.

[101] Cfr. GPDP, Provv. 20 aprile 2017, Verifica preliminare. Conservazione fino a 30 giorni delle immagini registrate da un sistema di videosorveglianza e dei dati rilevati da un sistema di controllo accessi biometrico, doc. *web* n. 6393088.

[102] Cfr. GPDP, Provv. 15 aprile 2010, Banche: cassette sicure con le impronte digitali, doc. *web* n. 1719879, GPDP, Provv. 13 settembre 2012, Installazione di un sistema completamente automatizzato di cassette di sicurezza. Verifica preliminare richiesta da Cassa Raiffeisen di Lagundo Soc. coop, doc. *web* n. 1927441, GPDP, Provv. 19 settembre 2013, Sistema per l'accesso della clientela in modalità self service, 24 ore su 24, alle cassette di sicurezza, con trattamento di dati biometrici. Verifica preliminare richiesta da Credito Lombardo Veneto S.p.A., doc. *web* n. 2710934, e GPDP, Provv. 6 febbraio 2014, Sistema automatizzato di cassette di sicurezza basato sul rilevamento dell'impronta digitale dei clienti. Verifica preliminare richiesta da Banca degli Ernici di credito coop. ScpA, doc. *web* n. 3000045.

maggiore sicurezza nelle operazioni allo sportello per i clienti degli istituti di credito. In questo caso, il Garante ha ritenuto che gli "*specimen*", ovvero le rappresentazioni digitali sintetiche (*template*) raccolte quale termine di raffronto per le successive operazioni di autenticazione, possano essere conservati per l'arco di tempo di erogazione del servizio, fatta salva l'eventuale ulteriore conservazione in caso di contestazioni[103]. Resta fermo che, in presenza di specifici obblighi di legge o regolamentari, la conservazione dei dati biometrici deve essere riferita all'arco di tempo previsto da dette disposizioni[104].

Da ultimo, si segnala il recente provvedimento nei confronti di Clearview AI, in relazione ad un motore di ricerca per il riconoscimento facciale che raccoglieva, attraverso tecniche di *web scraping*, le immagini di persone fisiche presenti sul *web* e le elaborava con tecniche biometriche, creando un *database*, stratificato ed alimentato in modo progressivo e costante, al fine di fornire un servizio di ricerca biometrica[105]. Per quanto qui di interesse, il Garante ha rilevato la violazione del principio di cui all'art. 5, par. 1, lett. *e)*, GDPR, in quanto i dati raccolti da Clearview AI risultavano conservati a tempo indeterminato e cancellati solo su espressa richiesta degli interessati.

3.1.4. *I provvedimenti in materia di videosorveglianza*

In relazione all'uso di sistemi di videosorveglianza, il Garante è intervenuto con il provvedimento generale del 2010, prescrivendo la limitazione della conservazione delle immagini «a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria»[106]. Nel citato provvedimento, si riteneva ammissibile l'allungamento dei tempi di conservazione, nel massimo fino ad una settimana, a fronte di specifiche esigenze tecniche o della particolare rischiosità dell'attività svolta dal titolare del trattamento. Ci si riferiva, ad esempio, ai casi delle immagini raccolte sui mezzi di trasporto o presso gli istituti di credito per i quali una registrazione più risalente nel tempo può agevolare le indagini in caso di reato.

---

[103] Cfr. GPDP, Provv. 31 gennaio 2013, Trattamento di dati biometrici. Verifica preliminare richiesta da Unicredit S.p.A., doc. *web* n. 2304808. Cfr. altresì Gar GPDP, Provv. 21 luglio 2016, Sistema di rilevazione delle caratteristiche biometriche della firma autografa in ambito bancario. Verifica preliminare, doc. *web* n. 5411652.

[104] Cfr. GPDP, Provv. 17 dicembre 2015, Verifica preliminare. Utilizzo di un servizio di firma elettronica avanzata con autenticazione biometrica, doc. *web* n. 4645479, GPDP, Provv. 24 settembre 2015, Trattamento di dati personali nell'ambito del «Processo di rilascio con riconoscimento a mezzo webcam» per firma elettronica qualificata o digitale. Verifica preliminare, doc. *web* n. 4367555, e GPDP, Provv. 26 luglio 2017, Verifica preliminare. Riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming, doc. *web* n. 6826368.

[105] Cfr. GPDP, Provv. 10 febbraio 2022, Ordinanza ingiunzione nei confronti di Clearview AI, doc. *web* n. 9751362, par. 3.6.1.

[106] Cfr. GPDP, Provv. 8 aprile 2010, Provvedimento in materia di videosorveglianza, doc. *web* n. 1712680.

Il provvedimento del 2010 consentiva in via eccezionale l'allungamento dei tempi di conservazione anche oltre il termine di sette giorni, subordinandolo alla richiesta di verifica preliminare del Garante *ex* art. 17 del Codice (nella versione previgente). Tale estensione risultava consentita in presenza di una «specifica esigenza di sicurezza»[107] o al fine della custodia o della consegna di una copia dei dati raccolti in base ad una richiesta dall'autorità giudiziaria o dalla polizia giudiziaria nell'ambito di un'attività investigativa[108].

Nell'esame delle richieste di verifica preliminare ricevute, il Garante ha ritenuto proporzionati i seguenti termini di conservazione: (i) quattordici giorni dall'ENEA (Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile) per le immagini raccolte mediante i sistemi di videosorveglianza installati presso un centro ricerche, considerati i periodi di chiusura del centro (che possono arrivare fino a tredici giorni), i rischi chimici derivanti dalle attività di ricerca e sviluppo ivi realizzate in caso di accessi fraudolenti, nonché le attività nucleari che hanno esposto in passato il sito ad eventi delittuosi di terroristi e i rischi di furto[109]; (ii) quindici giorni per le registrazioni operate da alcune sale da gioco, in ragione della frequenza minima dei controlli periodici delle sale e delle immagini registrate, delle richieste delle Forze di P.S. di messa a disposizione delle immagini per le indagini, nonché dei gravi danni economici subiti dal titolare in occasione di tali illeciti[110]; (iii) trenta giorni per la conservazione delle immagini raccolte dai sistemi di videosorveglianza di alcuni musei nelle Marche «al fine di prevenire ed eventualmente reprimere sottrazioni di opere d'arte di interesse storico-artistico presenti nel museo, come già in passato si è verificato, nonché pianificare l'esecuzione di servizi di vigilanza dinamica presso i siti di interesse culturale che potrebbero essere maggiormente esposti a minaccia terroristica»[111], anche in considerazione di «documentate valutazioni effettuate dal Comando Legione dei Carabinieri "Marche"»[112]; (iv) sessanta giorni per la videosorveglianza di un magazzino, attesi gli standard di sicurezza internazionale adottati dalla *Transported asset protection associatio*n (TAPA), nonché i «ripetuti e documentati atti criminosi che hanno interessato il magazzino» e le «obiettive difficoltà di accertare in tempi brevi – nonostante le procedure di verifi-

[107] *Ibidem*.

[108] *Ibidem*.

[109] Cfr. GPDP, Provv. 11 aprile 2013, Conservazione di immagini raccolte mediante sistemi di videosorveglianza. Verifica preliminare richiesta da ENEA, doc. *web* n. 2464185.

[110] Cfr. GPDP, Provv. 18 settembre 2014, Allungamento dei termini di conservazione delle immagini registrate dai sistemi di videosorveglianza installati presso sale da gioco - Verifica preliminare richiesta da Romagna Giochi s.r.l. doc. *web* n. 3522533. Cfr. altresì GPDP, Provv. 18 dicembre 2013, Allungamento dei termini di conservazione delle immagini registrate dai sistemi di videosorveglianza installati presso sale da gioco. Verifica preliminare richiesta da Riviera Giochi s.r.l., doc. *web* n. 2914191.

[111] Cfr. GPDP, Provv. 18 ottobre 2012, Videosorveglianza e tempi di conservazione delle immagini. Verifica preliminare richiesta dalla Soprintendenza per i beni archeologici delle Marche, doc. *web* n. 2138277. Cfr. altresì GPDP, Provv. 8 marzo 2012, Videosorveglianza. Verifica preliminare richiesta dalla società Palazzo Grassi S.p.A., doc. *web* n.1891026.

[112] *Ibidem*.

ca già implementate – gli illeciti perpetrati a danno del patrimonio aziendale»[113]; (v) novanta giorni per le immagini raccolte da una società operante nel settore dei servizi logistici integrati, in considerazione *(a)* del fatto che «non è infrequente il caso in cui il destinatario si trovi a rilevare eventuali manomissioni dopo un "lasso temporale anche considerevole" rispetto alla data di immagazzinaggio»[114], *(b)* dell'organizzazione interna aziendale («tempi mediamente impiegati dal personale di controllo per la redazione e l'invio dei verbali contenenti informazioni riguardanti danni, rotture e danneggiamenti degli imballaggi, oppure merci caricate in modo non conforme ai requisiti di sicurezza»)[115], *(c)* delle «vigenti norme pattizie in tema di trasporto aereo ed alle stesse previsioni del codice civile che, in caso di "perdita parziale" o "avaria non riconoscibili al momento della riconsegna", attribuisce all'interessato la possibilità di denunziare il fatto fino ad otto giorni dopo il ricevimento della spedizione (art. 1698 c.c.)»[116], nonché *(d)* dello *status* di "Operatore economico autorizzato" della richiedente, che impone alla stessa di segnalare alla Dogana sospetti di reato per le spedizioni gestite potendo trattenerle per diversi giorni presso i propri magazzini, con la possibilità che eventi dannosi vengano accertati anche diversi giorni dopo la consegna della merce[117]; (vi) novanta giorni per l'impianto di videosorveglianza di un sito produttivo nella filiera di dispositivi elettronici, valutata la «zona isolata e adiacente a vie di fuga facilmente raggiungibili»[118] in cui si trova lo stabilimento e gli elevati standard di sicurezza richiesti per il settore produttivo in cui opera la società, anche dalle norme tecniche ISO[119]; (vii) ventiquattro mesi per la videosorveglianza operata da un'azienda metalmeccanica la quale ha «subìto numerosi atti di sabotaggio da parte di ignoti dopo la conclusione delle normali fasi di ispezione e di collaudo del "prodotto finito"»[120] le cui conseguenze possono essere rilevate dai clienti anche oltre due anni dopo la fabbricazione e confezionatura, con notevoli

[113] Cfr. GPDP, Provv. 13 marzo 2014, Conservazione fino a 60 giorni delle immagini registrate mediante un impianto di videosorveglianza. Verifica preliminare, doc. *web* n. 3117736.

[114] Cfr. GPDP, Provv. 18 settembre 2014, Richiesta di allungamento dei tempi di conservazione delle immagini relative agli impianti di videosorveglianza installati presso le filiali di Schenker Italiana S.p.A., doc. *web* n. 3457674. Cfr. altresì GPDP, Provv. 30 gennaio 2014, Allungamento dei tempi di conservazione delle immagini registrate attraverso i sistemi di videosorveglianza. Verifica preliminare richiesta da SAES Advanced Technologies S.p.A., doc. *web* n. 3017416, e GPDP, Provv. 21 marzo 2013, Conservazione delle immagini registrate dalle videocamere di sorveglianza presso un'azienda. Verifica preliminare richiesta da Dhl Global Forwarding (Italy) S.p.A., doc. *web* n. 2448362.

[115] *Ibidem*.

[116] *Ibidem*.

[117] *Ibidem*.

[118] Cfr. GPDP, Provv. 14 luglio 2011, Allungamento dei tempi di conservazione delle immagini registrate dall'impianto di videosorveglianza. Verifica preliminare richiesta da DNP Photomask Europe S.p.A., doc. *web* n. 1836335.

[119] *Ibidem*.

[120] Cfr. Garante GPDP, Provv. 7 luglio 2011, Allungamento dei tempi di conservazione delle immagini registrate da un impianto di videosorveglianza. Verifica preliminare richiesta da NN Europe S.p.A, doc. *web* n. 1836347.

danni economici e reputazionali per l'azienda e rischi per l´incolumità dei fruitori dei prodotti sabotati[121].

La disciplina in esame deve essere, oggi, interpretata alla luce delle linee guida sulla videosorveglianza dell'*European Data Protection Board* (EPDB)[122]. Come anticipato precedentemente[123], l'autorità europea ha ribadito che è compito del titolare del trattamento determinare i tempi di conservazione delle immagini nel rispetto dei principi di proporzionalità e necessità. Atteso che le finalità legittime della videosorveglianza sono di norma la tutela del patrimonio e la raccolta di elementi probatori, l'EDPB ha rilevato che è possibile generalmente individuare la commissione di un illecito nell'arco di uno o due giorni e che, pertanto, «nella maggior parte dei casi»[124], le immagini registrate debbano essere cancellate «dopo alcuni giorni e preferibilmente tramite meccanismi automatici»[125]. Secondo l'autorità europea, quanto «più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione»[126].

Al pari del provvedimento del 2010, le linee guida dell'EDPB fanno salvi eventuali termini più ampi imposti da specifiche norme di legge. Per quanto riguarda l'Italia, si richiama l'art. 6, co. 8, del d.l. 23 febbraio 2009, n. 11, conv. con mod. dalla l. 23 aprile 2009, n. 38, il quale, in relazione all'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, limita la conservazione delle immagini ai sette giorni successivi alla rilevazione, ferme eventuali speciali esigenze di ulteriore conservazione.

3.1.5. *I provvedimenti in materia di marketing e profilazione*

A fronte del crescente sviluppo tecnologico dei servizi offerti ai consumatori e le maggiori opportunità per i titolari di monitoraggio e profilazione dei relativi dati, il Garante è intervenuto, nel 2005, con due provvedimenti sulla TV interattiva[127] e sulla

[121] *Ibidem*.

[122] Cfr. EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, 29 gennaio 2020.

[123] *Sub* par. 3.1.1.

[124] *Ibidem*.

[125] *Ibidem*.

[126] Cfr. *ibidem*, par. 122, le quali prevedono, ad esempio, che: «Normalmente, il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato. Se viene rilevato un danno, può essere anche necessario conservare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro l'autore del reato».

[127] Cfr. GPDP, Provv. 3 febbraio 2005, TV interattiva: misure necessarie ed opportune per un trattamento dei dati conforme alle disposizioni vigenti, doc. *web* n. 1109503.

c.d. *fidelity card*[128], individuando precisi termini di conservazione dei dati per finalità di profilazione e *marketing*[129].

Nel primo provvedimento, relativo a servizi televisivi interattivi o ad accesso condizionato, il Garante ha prescritto ai titolari del trattamento la conservazione dei dati di dettaglio su acquisti e servizi per finalità commerciali, pubblicitarie o di profilazione per un arco di tempo non superiore a dodici mesi dalla loro registrazione. Tale utilizzo deve comunque essere interrotto in caso di cessazione del rapporto con l'interessato[130].

Nel medesimo periodo, il Garante ha adottato il provvedimento sulla c.d. *fidelity card*. Ci si riferisce in particolare a quella prassi delle aziende della c.d. grande distribuzione di adottare delle carte in forza delle quali i clienti possono usufruire «di alcuni vantaggi per effetto della titolarità della carta, oppure del genere o volume di spesa o delle prestazioni richieste (ad es., sconti per l'acquisto di prodotti; premi o *bonus* correlati; priorità; servizi accessori; facilitazioni di pagamento)»[131]. Il rilascio di tali carte e il loro utilizzo comporta, di regola, la raccolta da parte dei titolari del trattamento, non solo di dati anagrafici per l'adesione al programma, ma anche dei dati relativi all'acquisto di beni o servizi. I dati così raccolti per il programma di fidelizzazione possono essere oggetto, previo ottenimento di specifico consenso, di attività di profilazione e *marketing*.

Per tali trattamenti, il Garante ha indicato che i dati relativi al dettaglio degli acquisti di clienti identificabili possono essere conservati per finalità di profilazione e di *marketing* «per un periodo non superiore, rispettivamente, a dodici e a ventiquattro mesi dalla loro registrazione»[132]. È stato inoltre prescritto un termine massimo di tre mesi per l'ulteriore conservazione dei dati, alla cessazione del programma di fidelizzazione, per esclusive finalità di amministrazione, fermi gli obblighi di legge sulla conservazione dei documenti contabili.

Successivamente, la materia in esame è stata oggetto di numerosi interventi del Garante nell'ambito delle richieste di verifica preliminare di cui all'art. 17 del Codice (nella versione previgente alla riforma del 2018). In particolare, il Garante ha accolto la richiesta di allungamento del periodo di conservazione per finalità di profilazione e *marketing* ogni qualvolta la frequenza media di acquisto dei beni e servizi considerati fosse inferiore a quella della grande distribuzione, oggetto del provvedimento sulle *fidelity card*, e tale da ridurre l'utilità per il titolare di tali attività. Segna-

[128] Cfr. GPDP, Provv. 24 febbraio 2005, "Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione, doc. *web* n. 1103045.

[129] Per un approfondimento su marketing e profilazione, cfr. C. Alvisi, *Dati personali e diritti dei consumatori*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo,* cit., p. 669 ss., M. Massimi, *Quali orizzonti per il* marketing*?*, in R. Panetta (a cura di), *op. cit.*, pp. 483 ss.

[130] Cfr. GPDP, Provv. 3 febbraio 2005, cit., par. 6.

[131] Cfr. GPDP, Provv. 24 febbraio 2005, cit., par. 1.

[132] *Ibidem*, par. 8. Cfr., inoltre, GPDP, Provv. 18 luglio 2023, cit., par. 9.5, nel quale si è rilevato che «il provvedimento del Garante del 24 febbraio 2005 "Fidelity card' e garanzie per i consumatori", sebbene non più di carattere vincolante, è da considerarsi ancora applicabile con valore di linea guida e pertanto lo è anche la tempistica ivi prevista», tempistica dalla quale il titolare del trattamento non può «scostarsi in modo eccessivo».

tamente, l'autorità garante ha ritenuto congrui e proporzionati alle finalità in esame i seguenti periodi di tempo: sette o dieci anni in relazione ai dettagli d'acquisto di beni di lusso, ove la frequenza media d'acquisto fosse al massimo di due beni all'anno[133]; dieci anni in relazione ai dettagli d'acquisto di beni di considerevole valore, quali gli autoveicoli, ove la frequenza media d'acquisto fosse pari ad otto anni[134]; quindici anni con riferimento ai dati relativi alla locazione e compravendita di beni immobili, considerato che i clienti si rivolgevano alla rete di agenzie immobiliari da una a due volte nell'arco di dieci anni, per operazioni di compravendita di immobili, e da una a quattro volte, per operazioni di locazione di immobili[135].

Viceversa, deve ritenersi contraria al principio in esame la conservazione dei dati, per finalità di *marketing* e profilazione, fino alla revoca del consenso o all'opposizione al trattamento da parte dell'interessato. Infatti, come anticipato *sub* paragrafo 2, il titolare del trattamento deve procedere ad una «conservazione selettiva e limitata (con particolare riguardo, rispettivamente, alla tipologia e alla durata) dei dati (…) a prescindere dalla revoca del consenso o da richieste provenienti dall'interessato»[136].

In caso di acquisizione di un nuovo valido consenso dell'interessato, la conservazione dei dati personali può essere protratta per un ulteriore arco di tempo non superiore, comunque, al primo[137].

3.1.6. *I provvedimenti in ambito giudiziario*

Nell'ambito giudiziario, si registrano le linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero[138] e le regole deontologiche relative ai trattamenti di dati perso-

[133] *Ex multis*, cfr. i seguenti provvedimenti: GPDP, Provv. 24 aprile 2013*, Trattamento e conservazione di dati personali della clientela per finalità di profilazione. Verifica preliminare richiesta da Bulgari S.p.A.,* doc. *web* n. 2499354; GPDP, Provv. 30 maggio 2013, Trattamento dei dati personali della clientela per finalità di profilazione e *marketing*. Verifica preliminare presentata da Salvatore Ferragamo S.p.A., doc. *web* n. 2547834; GPDP, Provv. 7 novembre 2013, Conservazione dei dati personali riguardanti la clientela per attività di profilazione e *marketing*. Verifica preliminare richiesta da Tod's S.p.A., doc. *web* n. 2920245; GPDP, Provv. 2 dicembre 2015, Verifica preliminare. Trattamento di dati personali diretto alla profilazione della clientela, doc. *web* n. 4642844; GPDP, Provv. 18 maggio 2016, Verifica preliminare. Trattamento di dati personali riferiti alla clientela e raccolti su scala globale per finalità di profilazione e *marketing*, doc. *web* n. 5260385; GPDP, Provv. 5 luglio 2017, Verifica preliminare. Trattamento di dati personali riferiti alla clientela per finalità di profilazione e promozionale, doc. *web* n. 6844421.

[134] Cfr. GPDP, Provv. 18 aprile 2018, Verifica preliminare. Prolungamento dei tempi di conservazione dei dati personali riferiti alla clientela per il loro utilizzo a fini di profilazione e di promozione commerciale profilata, doc. *web* n. 8997404.

[135] Cfr. GPDP, Provv. 30 giugno 2016, Conservazione dei dati personali riguardanti la clientela per attività di profilazione e di marketing, doc. *web* n. 5411203.

[136] Cfr. GPDP, Provv. 20 ottobre 2022, cit., par. 4, e GPDP, Provv. 18 luglio 2023, cit., par. 9.5.

[137] Cfr. GPDP, Provv. 2 dicembre 2015, Verifica preliminare. Trattamento di dati personali diretto alla profilazione della clientela, doc. *web* n. 4642844.

[138] Cfr. GPDP, Provv. 26 giugno 2008, Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero, doc. *web* n. 1534086.

nali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria[139].

Con il primo provvedimento, il Garante ha disposto che, nell'ambito dei procedimenti civili, penali e amministrativi, il consulente tecnico e i periti ausiliari del giudice e del pubblico ministero devono, al termine dell'incarico, così come in caso di revoca o rinuncia allo stesso, «consegnare per il deposito agli atti del procedimento non solo la propria relazione, ma anche la documentazione consegnatagli dal magistrato e quella ulteriore acquisita nel corso dell'attività svolta»[140]. L'ausiliario non può dunque conservare, in originale o in copia, informazioni personali raccolte nel corso dell'incarico, salve eventuali diverse disposizioni di legge o autorizzazioni dell'autorità giudiziaria[141].

Analoga previsione è disposta dalle regole deontologiche *ut supra* citate le quali, in relazione ai trattamenti effettuati dagli investigatori privati, impongono la conservazione dei dati per un arco di tempo «non superiore a quello strettamente necessario per eseguire l'incarico ricevuto»[142]. Conclusa l'attività investigativa, è fatto obbligo all'investigatore di cessare ogni trattamento, «fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico, i quali possono consentire, anche in sede di mandato, l'eventuale conservazione temporanea di materiale strettamente personale dei soggetti che hanno curato l'attività svolta, a i soli fini dell'eventuale dimostrazione della liceità, trasparenza e correttezza del proprio operato»[143].

Per quanto riguarda il trattamento operato da avvocati e praticanti avvocato nell'ambito delle attività di assistenza giudiziale e stragiudiziale e di consulenza, le regole deontologiche prevedono che la definizione di un grado di giudizio o la cessazione dell'incarico professionale non comportino di per sé l'obbligo di automatica cessazione del trattamento. Infatti, al professionista è consentito protrarre la conservazione di atti e documenti afferenti al mandato ricevuto, qualora, in base alla tipologia dei dati, «ciò risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento»[144].

---

[139] Cfr. GPDP, Provv. 19 dicembre 2018, *Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101*, doc. *web* n. 9069653.

[140] Cfr. GPDP, Provv. 26 giugno 2008, cit.

[141] Cfr. GPDP, Provv. 26 giugno 2008, cit., par. 4, ove si prevede che, in caso di richieste di chiarimenti o di supplementi di indagine, il perito e il consulente possono comunque acquisire dal fascicolo processuale «la documentazione necessaria per fornire i nuovi riscontri».

[142] Cfr. GPDP, Provv. 19 dicembre 2018, cit.

[143] Cfr. GPDP, Provv. 19 dicembre 2018, cit., par. 10, che riconoscono altresì la possibilità per il difensore o per il soggetto che ha conferito l'incarico, qualora sia stato contestato il trattamento, di «fornire all'investigatore il materiale necessario per dimostrare la liceità, trasparenza e correttezza del proprio operato, per il tempo a ciò strettamente necessario». In senso analogo, cfr. altresì GPDP, Provv. 5 giugno 2019, Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 10, doc. *web* n. 9124510.

[144] *Ibidem*, par. 4.

3.1.7. *I provvedimenti in materia di trattamenti a fini statistici o di ricerca scientifica*

Per i trattamenti effettuati a fini statistici o di ricerca scientifica è possibile individuare specifici tempi di conservazione nelle Regole deontologiche, oggetto di recente verifica da parte del Garante, le quali trovano applicazione ai trattamenti effettuati dalle università, altri enti o istituti di ricerca e società scientifiche, nonché dai relativi ricercatori e soci[145]. Tale provvedimento prevede la conservazione del progetto di ricerca presso il titolare del trattamento «in forma riservata e per cinque anni dalla conclusione programmata della ricerca», ferma la possibilità di ulteriore conservazione per scopi statistici o scientifici *ex* art. 5, par. 1, lett. *e)*, GDPR[146].

In materia, si registrano altresì le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale le quali consentono, per finalità statistiche, la conservazione dei dati personali anche oltre il periodo di tempo necessario per il raggiungimento della finalità perseguita, secondo quanto previsto dall'art. 5, par. 1, lett. *e)*, GDPR e dall'art. 6-*bis* del d.lgs. 6 settembre 1989, n. 322[147].

Nel caso in cui la raccolta delle categorie particolari di dati personali «sia effettuata con particolari modalità, quali interviste telefoniche o assistite da elaboratore», entrambi i provvedimenti dispongono che il consenso esplicito possa essere documentato in forma scritta. Per tali circostanze, le regole deontologiche prevedono espressamente un termine di conservazione pari a tre anni per la documentazione sulla prestazione dell'informativa all'interessato e la raccolta del relativo consenso[148].

Di recente, il Garante si è espresso, in sede di consultazione preventiva *ex* art. 36 GDPR, sul periodo di conservazione dei dati clinici e dei campioni dei pazienti arruolati per la realizzazione di uno studio clinico osservazionale retrospettivo multicentrico. In considerazione del valore scientifico delle informazioni cliniche e dei campioni raccolti e che su tali campioni il titolare era in grado di svolgere ricerche e analisi per periodi di tempo molto lunghi, si è ritenuto proporzionato un tempo di conservazione pari alla durata del progetto finanziato, ovvero sette anni con possibilità di rinnovo per ulteriori sette anni. Il Garante ha, inoltre, ammesso che, in caso lo studio ottenga ulteriori finanziamenti, tali per cui potrebbe proseguire, per il

[145] Cfr. GPDP, Provv. 19 dicembre 2018, *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101*, doc. *web* n. 9069637.

[146] Con analoga previsione, cfr. GPDP, Provv. 5 giugno 2019, cit., par. 4.11, il quale dispone altresì che i «dati e i campioni biologici utilizzati per l'esecuzione della ricerca sono conservati mediante tecniche di cifratura o l'utilizzazione di codici identificativi oppure di altre soluzioni che, considerato il numero dei dati e dei campioni conservati, non li rendono direttamente riconducibili agli interessati, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. A tal fine, è indicato nel progetto di ricerca il periodo di conservazione, successivo alla conclusione dello studio, al termine del quale i predetti dati e campioni sono anonimizzati». Al riguardo, cfr., inoltre, GPDP, Provv. 24 luglio 2008, Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali, doc. *web* n. 1533155.

[147] Cfr. GPDP, Provv. 19 dicembre 2018, cit.

[148] Cfr. GPDP, Provv. 19 dicembre 2018, cit., par. 5.3.

perseguimento dei medesimi scopi, il titolare possa definire un ulteriore periodo di conservazione, previa informativa agli interessati[149].

3.2. Il principio di limitazione della conservazione nella giurisprudenza della Corte europea dei diritti dell'uomo

Nella giurisprudenza della Corte europea dei diritti dell'uomo (Corte EDU), la necessità di una conservazione dei dati limitata nel tempo ha trovato tutela in forza dell'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU), sul diritto al rispetto della vita privata. Segnatamente, con riferimento ad alcune normative nazionali relative al settore di polizia, la Corte EDU ha ritenuto che la conservazione dei dati personali debba essere proporzionata alla finalità di contrasto della criminalità.

Nel noto caso *S. e Marper c. Regno Unito*[150], ai due ricorrenti, accusati rispettivamente di tentato furto e di molestie, erano stati prelevati impronte digitali e campioni di cellule e, sulla base di quest'ultimi, erano stati creati i corrispondenti profili DNA. Nonostante il primo ricorrente fosse stato assolto e nei confronti del secondo fosse stato dichiarato il non luogo a procedere, tali materiali non venivano cancellati in forza di una normativa nazionale che ne consentiva la conservazione a tempo indeterminato.

Nel procedimento in esame, la Corte EDU ha statuito che le impronte digitali, i campioni di cellule ed i profili DNA costituiscono dati personali e la relativa conservazione integra un'ingerenza nel diritto degli individui al rispetto della loro vita privata ai sensi dell'art. 8, par. 1, CEDU[151]. Si è, viceversa, escluso che una tale conservazione possa essere ritenuta necessaria in una società democratica e sia pertanto giustificabile secondo l'art. 8, par. 2, CEDU. A tale riguardo, la Corte ha contestato il carattere generale ed indifferenziato della conservazione operata in Inghilterra e Galles, indipendentemente dalla natura e dalla gravità del reato e dall'età dell'indagato[152]. Si è, inoltre, censurato il fatto che la normativa nazionale fosse formulata in modo generico ed aperto ad una interpretazione eccessivamente ampia rispetto alle condizioni e alle modalità di conservazione e di utilizzo delle informazioni personali in esame[153].

---

[149] Cfr. GPDP, Provv. 24 novembre 2022, doc. *web* n. 9842737.

[150] Cfr. Corte EDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008, n. 30566/04. Per un commento sulla sentenza, cfr. V. Sellaroli, *Il "*Caso S. e Marper*" e la Corte Europea: Il dna e il bilanciamento tra opposte esigenze in una società democratica,* in *Legislazione penale*, 2009, 4, pp. 639-649; C. Sartoretti, *Il diritto alla privacy tra sicurezza e principio di proporzionalità: il punto di vista della Corte europea dei diritti dell'uomo. Nota a Corte eur. Dir. Uomo 4 dicembre 2008 (S. e Marper c. Regno Unito),* in *Diritto pubblico comparato ed europeo*, 2009, 2, pp. 583-590; A.M. Capitta, *Conservazione dei "*DNA profiles*" e tutela europea dei diritti dell'uomo*, in *ArchivioPenale.it*, 2013, 1, pp. 1-34.

[151] *Ibidem*, par. 68 ss. Già con la sentenza *Van der Velden c. Paesi Bassi*, 7 dicembre 2006, n. 29514/05, la Corte EDU aveva stabilito che la raccolta di campioni di cellule e la creazione dei correlati profili DNA costituiscono un'ingerenza nel diritto degli individui al rispetto della loro vita privata ai sensi dell'art. 8, par. 1, CEDU.

[152] *Ibidem*, par. 119.

[153] *Ibidem*, par. 95 ss.

Tali principi sono stati successivamente ripresi nel procedimento *M.M. c. Regno Unito*[154]. La ricorrente era stata arrestata nel 2000 ma, considerate le circostanze del caso, le autorità avevano deciso di non agire nei suoi confronti e di limitarsi a diffidarla. L'annotazione di tale provvedimento nella fedina penale della ricorrente, inizialmente prevista per cinque anni, veniva successivamente estesa a vita, per un cambio di prassi da parte delle autorità di polizia.

In tale caso, la Corte ha ribadito che la conservazione di dati relativi alla vita privata di un individuo ricade nell'ambito di applicazione dell'art. 8 CEDU. Infatti, sebbene i dati contenuti nella fedina penale siano pubblici, la loro sistematica conservazione può comportarne la divulgazione anche dopo un lungo lasso di tempo, quando tutti gli individui diversi dall'interessato si sono dimenticati dell'accaduto. Con il trascorrere del tempo, il provvedimento diventa, pertanto, parte della vita privata dell'individuo. La Corte EDU ha quindi censurato[155], come violativa dell'art. 8 CEDU, la conservazione indiscriminata ed indefinita dei dati relativi ai precedenti penali, effettuata dall'Irlanda del Nord, in assenza di una norma di legge chiara e dettagliata[156].

Il principio in parola è stato esteso anche alla conservazione di dati personali relativi a soggetti condannati[157]. In particolare, la Corte EDU, sulla scorta delle pronunce poc'anzi richiamate, ha censurato la conservazione dei profili DNA, impronte digitali e fotografie, ancorché riferiti ad individui colpevoli, qualora sia prevista in modo indiscriminato e generalizzato o, comunque, non trovi fondamento sulla gravità del reato o sulla necessità di una conservazione indefinita[158]. È stata altresì contestata l'assenza, per il condannato, di rimedi esperibili nei confronti della conservazione illimitata, quale l'accesso ad un'effettiva revisione della decisione sulla conservazione dei dati[159].

3.3. Il principio di limitazione della conservazione in materia di *data retention* tra la giurisprudenza della Corte di giustizia dell'UE e la normativa italiana

Nell'ultimo decennio, la limitazione del tempo di conservazione dei dati personali è stata al centro della giurisprudenza eurounitaria in materia di comunicazioni elettroniche. Segnatamente, la Corte di giustizia dell'Unione europea (CGUE) è più

[154] Cfr. Corte EDU, *M.M. c. Regno Unito*, 13 novembre 2012, n. 24029/07.
[155] *Ibidem*, par. 188.
[156] A tale riguardo, cfr. altresì Corte EDU, *Brunet c. Francia*, 18 settembre 2014, n. 21010/2010, con commento di A. SCARCELLA, *Viola la CEDU conservare in un database informazioni relative a soggetti i cui procedimenti penali non abbiano trovato sviluppo*, in *Diritto penale e processo*, 2015, 6, pp. 757 ss.
[157] Cfr. Corte EDU, *Gaughran c. Regno Unito*, 13 febbraio 2020, n. 45245/15, con commento di M. MARCIANTE, *La Corte Europea sulla raccolta e conservazione dei dati biometrici a tempo indeterminato*, in *Giurisprudenza Italiana*, 2020, p. 529, e *Trajkovski e Chipovski c. Macedonia del Nord*, 13 febbraio 2020, nn. 53205/13 e 63320/13.
[158] *Ibidem*.
[159] *Ibidem*.

volte intervenuta, in via pregiudiziale, sul bilanciamento tra la tutela della *privacy* dell'individuo e le esigenze di sicurezza pubblica.

Con la sentenza *Digital Rights Ireland e A.*[160], la CGUE ha dichiarato l'invalidità della direttiva 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[161]. In tale pronuncia, la CGUE ha riconosciuto che la conservazione dei predetti dati costituisce di per sé un'ingerenza nei diritti garantiti dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea (Carta), sul rispetto della vita privata e della vita familiare, nonché dall'art. 8 della stessa Carta, sulla protezione dei dati di carattere personale[162]. Sebbene la direttiva 2006/24/CE rispondesse ad un obiettivo di interesse generale, quale la sicurezza pubblica e la lotta contro la criminalità grave, si è rilevato come la stessa comportasse un'ingerenza nei diritti fondamentali della popolazione europea non proporzionata, *ex* art. 52, par. 1, della Carta, rispetto a tale obiettivo. La CGUE, richiamando *inter alia* il citato caso *S. e Marper c. Regno Unito* della Corte EDU, ha quindi statuito che la direttiva 2006/24/CE non prevedeva «norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta»[163]. In sintesi, è stato eccepito come la direttiva in oggetto non limitasse la conservazione dei dati alle sfere di criminalità grave e non subordinasse l'accesso ai dati personali da parte delle autorità nazionali competenti al previo controllo di un giudice o di un'autorità amministrativa indipendente, secondo condizioni sostanziali e procedurali prestabilite. Quanto alla durata del trattamento, la CGUE ha censurato il fatto che la direttiva 2006/24/CE imponesse la conservazione dei dati per almeno 6 mesi e per un massimo di 24 mesi senza alcuna distinzione tra le categorie di dati personali raccolte «a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate»[164] e senza che la durata di conservazio-

[160] Cfr. CGUE, *Digital Rights Ireland e A,* 8 aprile 2014, cause riunite C-293/12 e C-594/12. Per un commento sulla sentenza, cfr. L. Trucco, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giurisprudenza italiana*, 2014, 8-9, pp. 1850 ss.; R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d.* "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Diritto penale contemporaneo*, 2014, 2, p. 178 ss.; C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di giustizia e gli echi del* datagate, in *Nuova giurisprudenza civile commentata*, 2014, 11, pp. 1039 ss.; L. Scaffardi, "Data retention" *e diritti della persona,* in *Costituzionalismo. it,* 2017, 2, pp. 60 ss.; E. Colombo, "Data retention" *e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE*, in *Cassazione penale*, 2014, 7-8, pp. 2705-2713; M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di* "data retention", in *Diritto dell'Unione Europea*, 2014, 4, pp. 803-830. Si veda anche, in un discorso di più ampio respiro, F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 158.

[161] Per una descrizione tecnica dei dati relativi alle comunicazioni elettroniche e della *data retention*, cfr. S. Marcolini, *L'istituto della* data retention *dopo la sentenza della Corte di giustizia del 2014*, in A. Cadoppi-S. Canestrari-A. Manna (a cura di), *Cybercrime*, Torino, 2019, p. 1579 ss.

[162] Cfr. CGUE, *Digital Rights Ireland e A.*, cit., par. 29.

[163] *Ibidem*, par. 65.

[164] *Ibidem*, parr. 63-64.

ne fosse basata «su criteri obiettivi»[165] tali da garantirne la limitazione «allo stretto necessario»[166].

Due anni più tardi, la Corte di Giustizia è di nuovo intervenuta applicando alle normative nazionali i principi già enucleati con la pronuncia *Digital Rights Ireland e A*. In particolare, con la sentenza *Tele2*[167], la CGUE ha fornito un'interpretazione «costituzionalmente» orientata della direttiva 2002/58/CE[168] alla luce degli artt. 7, 8, 11 e 52, par. 1, della Carta, censurando, *inter alia*, la conservazione «generalizzata e indifferenziata» dei dati di traffico e relativi all'ubicazione delle normative nazionali esaminate per finalità di lotta alla criminalità[169]. Per quanto qui di interesse, la Corte ha ribadito la necessità che la normativa nazionale preveda un termine di conservazione limitato allo «stretto necessario»[170].

[165] *Ibidem*, parr. 63-64.

[166] *Ibidem*, parr. 63-64.

[167] Cfr. CGUE, Tele2, 21 dicembre 2016, cause riunite C/203/15 e C-698/15. Per un commento sulla sentenza, cfr. O. POLLICINO-M. BASSINI, *La Corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico. Nota a Corte Giustizia UE, sent. 21 dicembre 2016, Tele2 e Watson, cause riunite C-203/15 e C-698/15*, in *Diritto Penale Contemporaneo*, consultabile all'indirizzo https://archiviodpc.dirittopenaleuomo.org/d/5162-la-corte-di-giustizia-e-una-trama-ormai-nota-la-sentenza-tele2-sverige-sulla-conservazione-dei-dati; S. MARCOLINI, *op. cit*., pp. 1579 ss.; B. CAROTTI, *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche*, in *Giornale di diritto amministrativo*, 2017, 4, p. 479 ss.; G. TIBERI, *Il caso "Tele2 Sverige/Watson": una "iconica" sentenza della Corte di Giustizia nella saga sulla "*data retention*". Nota a CGUE Grande sezione 21 dicembre 2016 (cause riunite C-203/15 e C-698/15),* in *Quaderni costituzionali,* 2017, 2, p. 434-438; F. GUELLA, "Data retention" *e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali. Nota a CGUE Grande sezione 21 dicembre 2016 (cause riunite C-203/15 e C-698/15)*, in *DPCE online,* 2017, 2, p. 349-357; L. SCAFFARDI, *op. cit.*, pp. 68 ss.

[168] Con la caducazione della direttiva 2006/24/CE, la materia in esame risultava (e risulta tuttora) regolata dall'antecedente direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. L'art. 5 della direttiva 2002/58/CE prevede, *inter alia,* il divieto di ascoltare, captare, memorizzare e porre in essere altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, senza il consenso degli utenti, fatta eccezione, *ex* art. 15 della medesima direttiva, quando tali attività siano legalmente autorizzate «una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica».

[169] *Ibidem*, par. 112.

[170] Cfr. CGUE, *Tele2*, cit., par. 108. Inoltre, con la sentenza *Tele 2* la CGUE ribadisce gli approdi della decisione *Digital Rights Ireland*, statuendo che «L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione».

Successivamente, con la pronuncia *La Quadrature du Net*, la CGUE ha esteso le predette argomentazioni sulla proporzionalità della conservazione anche all'art. 23, par. 1, GDPR, in forza di una lettura orientata alla luce artt. 7, 8 e 11 e dell'art. 52, par. 1, della Carta[171]. In particolare, si è rilevato che, analogamente a quanto sancito per l'art. 15 della direttiva 2002/58, il potere conferito agli Stati membri dall'art. 23, par. 1, GDPR di limitare le disposizioni del regolamento europeo «può essere esercitato soltanto nel rispetto del requisito di proporzionalità, secondo cui le deroghe e le restrizioni alla tutela dei dati personali devono operare entro i limiti dello stretto necessario»[172]. Pertanto, la Corte ha ritenuto che anche la richiamata disposizione del regolamento sia contraria ad «una normativa nazionale che impone ai fornitori di accesso a servizi di comunicazione al pubblico *online* e ai fornitori di servizi di *hosting* la conservazione generalizzata e indifferenziata, in particolare, dei dati personali relativi a tali servizi»[173].

Nell'ordinamento italiano, la conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati è prevista dall'art. 132, commi 1 e 1-*bis*, del Codice rispettivamente in 24 e 12 mesi, mentre per le chiamate senza risposta è pari a 30 giorni. La disciplina risulta integrata dall'art. 24 della l. 167/2017 che, per le fattispecie di criminalità grave [«reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera *a)*, c.p.p.»], stabilisce la conservazione dei dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, in un periodo pari a 72 mesi[174]. Tale norma, adottata in via emergenziale per finalità di lotta al terrorismo, risulta oggi incardinata nella disciplina ordinaria tramite il richiamo operato dall'art. 132, co. 5-*bis*, del Codice, come da ultimo modificato dal d.lgs. 101/2018 e ss.mm.ii.

All'epoca, la disciplina italiana era stata censurata dalla dottrina la quale riteneva che l'art. 132 del Codice dovesse essere disapplicato in quanto contrario agli artt. 7, 8 e 52, par. 1, della Carta[175], presentando gli stessi vizi per i quali la direttiva 2006/24/CE era stata dichiarata invalida. In particolare, si era rilevato che l'art. 132

[171] Cfr. CGUE, *La Quadrature du Net*, cit. Quanto al rapporto tra la direttiva 2002/58/CE e il GDPR, cfr. EDPB, Parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati, 12 marzo 2019.

[172] *Ibidem*, par. 210.

[173] *Ibidem*, par. 212. Si segnala che, con tale sentenza, la CGUE ha, *inter alia*, indicato precisi parametri per la compatibilità delle misure legislative nazionali con l'art. 15, par. 1, della direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE, interpretato alla luce degli artt. 7, 8 e 11 e dell'art. 52, par. 1, della Carta. Sul punto, cfr. altresì CGUE, *Privacy International*, 6 ottobre 2020, C-623/17.

[174] Per un approfondimento sulle modifiche apportate all'art. 132 del Codice dal d.lgs 101/2018, cfr. S. Signorato, *Novità in tema di data "retention". La riformulazione dell'art. 132 codice privacy da parte del D.lgs. 10 agosto 2018, n. 101*, in *Diritto penale contemporaneo,* 2018, 11, p. 153-160.

[175] Cfr. R. Flor, *Data retention ed art. 132 cod. Privacy:* vexata quaestio *(?) Nota a Trib. Padova, ord. 15 marzo 2017, Pres. Marassi*, in *Diritto penale contemporaneo*, 2017, 3, p. 356 ss.; F. Ruggieri, "Data retention" *e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione penale*, 2017, 6, p. 2483-2488; S. Marcolini, *op. cit*., p. 1590 ss.; L. Scaffardi, *op. cit.*, p. 84.

del Codice, sia per i termini di conservazione previsti[176] che per i criteri e le modalità applicative[177], risultasse in contrasto con il principio di proporzionalità[178].

Con posizione analoga, anche il Garante italiano era intervenuto in materia giudicando eccessivo il termine di conservazione di 72 mesi e sollecitando il legislatore ad una riforma organica della disciplina in coerenza con i criteri di proporzionalità affermati dalle norme e dalla giurisprudenza comunitarie[179].

Di diverso avviso era apparsa, allora, la giurisprudenza di merito[180] e di legittimità[181] la quale riteneva che l'art. 132 del Codice fosse compatibile con il diritto sovranazionale in tema di tutela della *privacy*, come interpretato dalla giurisprudenza della Corte di giustizia dell'Unione europea. Sul punto, la Corte di Cassazione rilevava che l'Italia, a differenze degli Stati coinvolti nelle citate sentenze della CGUE, si fosse dotata di una disciplina specifica nella quale era possibile rinvenire: «l'enunciazione della finalità di repressione dei reati; la delimitazione temporale dell'attività di memorizzazione; l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati, nonché al rispetto del principio di proporzionalità in concreto»[182].

Di recente, l'art. 132 Codice Privacy è stato nuovamente riformato con d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla l. 23 novembre 2021, n. 178 nel dichiarato intento[183] di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico, per fini di indagine penale, nel rispetto dei principi enunciati dalla CGUE nella sentenza H.K. c. Prokuratuur[184]. Con tale decisione, la

[176] Cfr. S. SIGNORATO, *op. cit.*, p. 157 e S. MARCOLINI, *op. cit*., p. 1593, i quali notano che, secondo la disciplina di diritto interno, il fornitore di servizi, non potendo distinguere a priori tra criminalità grave dall'art. 24 della l. 167/2017 e non grave, è tenuto alla conservazione di tutti i dati di traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta, per 72 mesi.

[177] Cfr. R. FLOR, *Data retention ed art. 132 cod. Privacy:* vexata quaestio *(?)*, cit., p. 360.

[178] In senso parzialmente difforme, cfr. S. SIGNORATO, *op. cit.*, p. 156, la quale rileva come i termini previsti all'art. 132 del Codice risultino incompatibili con le esigenze investigative e difensive proponendo un termine di conservazione pari ad almeno 36 mesi.

[179] Cfr. *Dichiarazione di Antonello Soro, Presidente del Garante per la protezione dei dati personali, Terrorismo: Soro, troppi 6 anni conservazione dati chiamate*, Agi, 25 luglio 2017, consultabile al sito https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6651715, secondo il quale la «sorveglianza non può mai essere generalizzata e massiva ma, lo precisa la corte di giustizia nella recente sentenza tele2, deve fondarsi su requisiti individualizzanti, rivolgendosi cioè nei confronti di soggetti coinvolti, in qualche misura, in attività criminose ovvero limitandosi a specifici luoghi nei quali emergano esigenze investigative relative, sempre, a gravi reati e previa adeguata delimitazione temporale della durata della conservazione».

[180] Cfr. Trib. Padova, ord. 15 marzo 2017, con commento di R. FLOR, *Data retention ed art. 132 cod. Privacy:* vexata quaestio *(?)*, cit., p. 356 ss.; F. RUGGIERI, *op. cit.*, p. 2483-2488.

[181] Cfr. Cass., sentt. nn. 33851/18, 5741/19, 26380/19, 31994/19 e 48737/19.

[182] Cfr. Cass., sent. n. 36380/19.

[183] Cfr. CAMERA DEI DEPUTATI, Dossier 5 novembre 2021, Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP Elementi per l'esame in Assemblea, consultabile al sito https://temi.camera.it/leg18/dossier/OCD18-15887/misure-urgenti-materia-giustizia-e-difesa-nonche-proroghe-tema-referendum-assegno-temporaneo-e-irap.html.

[184] Cfr. CGUE, H. K. c. Prokuratuur, 2 marzo 2021, C-746/18, con commento di M. GIANGRECO, Data retention*, acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata*, in *Cassazione Penale*, 2022, 4, p. 1672 ss., e di C. GRECO, *Quest'acquisizione non s'ha da fare: en-*

Corte di Giustizia ha statuito, infatti, il principio che l'accesso, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, ai dati di comunicazioni elettroniche relativi al traffico o all'ubicazione, che permettano di trarre precise conclusioni sulla vita privata, è consentito soltanto per finalità di lotta contro gravi forme di criminalità o di prevenzione contro gravi minacce alla sicurezza pubblica «indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo». I Giudici di Lussemburgo hanno altresì affermato che l'accesso di un'autorità pubblica ai predetti dati di traffico e di ubicazione deve essere subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente e non dal pubblico ministero.

A seguito della menzionata riforma, il novellato comma 3 dell'art. 132 del Codice prevede che l'acquisizione dei dati di traffico possa essere effettuata solo «previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private» e per quei «reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi». L'acquisizione dei dati di traffico può essere altresì disposta dal pubblico ministero con decreto motivato soggetto a convalida entro 48 ore del giudice competente qualora ricorrano «ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini».

I termini di conservazione dei dati previsti dalla norma in commento sono, tuttavia, rimasti immutati. In tal senso, l'autorità garante, nel parere sullo schema del menzionato decreto legge che ha riformato l'art. 132 del Codice[185], ha rilevato che resta «da adeguare alla giurisprudenza di Lussemburgo la disciplina della durata della conservazione dei tabulati, considerando anzitutto che la direttiva CE 2006/24 (la quale prevedeva un termine massimo di conservazione di ventiquattro mesi) è stata invalidata dalla Corte per violazione, in particolare, del canone di proporzionalità. La legittimità dell'acquisizione dei tabulati – obiettivo perseguito dallo schema di decreto-legge, come si evince dallo stesso preambolo – esige, infatti, una parimenti legittima conservazione (alla prima preordinata), che tale potrebbe non ritenersi se incompatibile con il principio di proporzionalità, secondo cui, come chiarito dalla citata sentenza Tele2 Sverige, "le deroghe e le restrizioni alla tutela dei dati personali" devono intervenire "entro i limiti dello stretto necessario"»[186].

nesimo 'no' della Corte di Giustizia alla data retention *indiscriminata in campo penale*, in *Il diritto dell'informazione e dell'informatica*, 2021, 2, p. 235.

[185] Cfr. GPDP, Provv. 10 settembre 2021, Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale, doc. *web* n. 9704851.

[186] *Ibidem*.

Nel solco della pronuncia *La Quadrature du Net*[187], la Corte di Giustizia ha recentemente ribadito il divieto di conservazione preventiva, generalizzata ed indifferenziata dei dati di traffico e di ubicazione per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla pubblica sicurezza, nonché le relative fattispecie di deroga:

a) conservazione generalizzata ed indiscriminata dei dati relativi al traffico e all'ubicazione che sia disposta, per un periodo temporalmente limitato allo stretto necessario (ma rinnovabile), tramite ingiunzione soggetta ad un controllo effettivo e a fronte di una minaccia grave per la sicurezza nazionale;

b) conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

c) conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica;

d) conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;

e) conservazione rapida, per un periodo determinato, dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono i fornitori di servizi di comunicazione elettronica, a seguito di un'ingiunzione dell'autorità competente soggetta a un controllo giurisdizionale effettivo[188].

Gli ultimi approdi della Corte di Giustizia sanciscono il netto contrasto della conservazione «a tappeto» prevista (anche) dall'attuale versione dell'art. 132 del Codice con il diritto dell'Unione Europea. Infatti, come si è visto poc'anzi, l'intervento del legislatore italiano ha modificato solo gli aspetti procedurali della normativa, lasciando intatti sia i termini di durata della conservazione che il carattere generalizzato ed indiscriminato della stessa, elementi tutti già censurati dalla giurisprudenza eurounitaria[189].

---

[187] Cfr. CGUE, *La Quadrature du Net*, cit.

[188] Cfr.: CGUE, G.D. contro The Commissioner of the Garda Síochána e a, 5 aprile 2022, C-140/20, con commento di A. CHELO, Tabula rasa *sui tabulati? Riflessioni a margine della recente giurisprudenza della Corte di Giustizia dell'Unione Europea*, in *Cassazione Penale*, 2022, 9, p. 3268; CGUE, Bundesrepublik Deutschland c. SpaceNet AG e Telekom Deutschland GmbH, 20 settembre 2022, cause riunite C-793/19 e C-794/19, con commento di P. DI STEFANO, *La Corte di Giustizia conferma la regola del divieto, con eccezioni, di conservazione dei dati di traffico telefonico e telematico ai fini di lotta alla criminalità grave: la fine della prova a mezzo di tabulati?*, in *Cassazione Penale*, 2021, 1, p. 354; CGUE, VD e SR, 20 settembre 2022, cause riunite C-339/20 e C-397/20, con commento di V. TARTARA, *La Corte di Giustizia conferma il "divieto di conservazione generalizzata e indiscriminata" dei dati relativi al traffico delle comunicazioni elettroniche per finalità preventive di contrasto alla criminalità. Possibili ricadute nell'ordinamento italiano*, in *Sistema Penale*, 2022, 12, p. 173.

[189] In tal senso, cfr. A. CHELO, *op. cit.*, p. 3268, P. DI STEFANO, *op. cit*., p. 354, e V. TARTARA, *op. cit.*, p. 173.

3.4. Principio di limitazione della conservazione, diritto alla cancellazione e diritto all'oblio

Il principio di limitazione della conservazione risulta legato a doppio filo al diritto alla cancellazione e all'oblio che, si è detto, integra un "corollario in negativo" del principio[190]. Tale diritto costituisce segnatamente lo strumento con cui l'interessato può esercitare il potere di sindacato sull'effettivo protrarsi della conservazione da parte del titolare.

L'art. 17 GDPR[191] prevede l'obbligo per il titolare del trattamento di cancellare i dati personali dell'interessato, senza ingiustificato ritardo e su richiesta di quest'ultimo, al ricorrere delle seguenti condizioni tassative: i dati personali non sono più necessari rispetto alle finalità di trattamento[192]; è stata esercitata la revoca del consenso da parte dell'interessato[193]; è stato esercitato il diritto di opposizione al trattamento dell'interessato ai sensi dell'art. 21 GDPR[194]; il trattamento dei dati personali sia illecito[195]; la cancellazione è imposta da un obbligo di legge[196]; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1, GDPR[197] [198]. Di peculiare rilievo è la novità introdotta dal par. 2 dell'art. 17, GDPR, secondo il quale il titolare che abbia reso pubblici dati personali e che sia obbligato a cancellarli a seguito della richiesta dell'interessato deve «informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali».

---

[190] Sul diritto alla cancellazione e il diritto all'oblio, cfr. *amplius*: I.M. Alagna, *op. cit.*; A. Ricci, *op. cit.*, pp. 195 ss.; F. Di Ciommo, *op. cit.*, pp. 353 ss.; B. Meo in Art. 17. *Diritto alla cancellazione («diritto all'oblio»)*, in G.M. Riccio-G. Scorza-E. Belisario (a cura di), *op. cit.*, p. 178 ss.; M.A. Livi, *Sezione 3. Rettifica e cancellazione*, in A. Barba-S. Pagliantini (a cura di), *op. cit.*, pp. 266 ss.; V. Cuffaro, *Cancellare i dati personali. Dalla* damnatio memoriae *al diritto all'oblio*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 219 ss.; G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti alla personalità*, in *Il diritto dell'informazione e dell'informatica*, 2014, 4-5, pp. 591 ss.; G. Finocchiaro, *La memoria della rete e il diritto all'oblio*, in *Il diritto dell'informazione e dell'informatica*, 2010, 3, pp. 391 ss.; F. Pizzetti, *Il caso del diritto all'oblio*, Torino, 2013; M.R. Morelli voce *Oblio (diritto all')*, in *Enc. dir. agg. VI*, Milano, 2002; G.B. Ferri, *Diritto all'informazione e diritto all'oblio*, in *Rivista di diritto civile*, 1990, I, pp. 801 ss.; T. Auletta, *Diritto alla riservatezza e "droit à l'oubli"*, in G. Alpa-M. Bessone-L. Boneschi-G. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, pp. 127 ss.

[191] Nell'epoca antecedente al GDPR, il diritto alla cancellazione dei dati personali risultava previsto dall'art. 12, lett. *b)*, della Direttiva e dall'art. 7, co. 3, lett. *b)*, del Codice.

[192] Cfr. art. 17, par. 1, lett. *a)*, GDPR.

[193] Cfr. art. 17, par. 1, lett. *b)*, GDPR.

[194] Cfr. art. 17, par. 1, lett. *c)*, GDPR.

[195] Cfr. art. 17, par. 1, lett. *d)*, GDPR.

[196] Cfr. art. 17, par. 1, lett. *e)*, GDPR.

[197] Cfr. art. 17, par. 1, lett. *f)*, GDPR.

[198] L'esercizio del diritto alla cancellazione dei dati trova espressa deroga nelle ipotesi di cui all'art. 17, par. 3, GDPR e agli artt. 2-*undecies* e 2-*duodecies* del d.lgs. n. 196/2003, integrato con le modifiche introdotte dal d.lgs. n. 101/2018. A tale riguardo, si rinvia a F. Di Ciommo, *op. cit.*, pp. 362 ss.

Oltre al diritto alla cancellazione, la rubrica dell'art. 17, GDPR, richiama, seppur tra parentesi, il diritto all'oblio, oggetto di grande attenzione da parte della dottrina e della giurisprudenza nazionale ed europea.

Il diritto all'oblio risulta tradizionalmente definito come «il diritto di un soggetto a non vedere pubblicate alcune notizie a vicende, già legittimamente pubblicate, rispetto all'accadimento delle quali è trascorso un notevole lasso di tempo»[199]. Segnatamente, si è evidenziato che, con il trascorre del tempo, verrebbe meno l'interesse pubblico alla notizia la quale può essere riproposta solo in caso di fatti sopravvenuti che la rendano nuovamente attuale[200]. Così inteso, l'oblio, quale «nuovo profilo del diritto alla riservatezza», tutela il diritto della persona a non essere menomata nella reputazione e nell'onore, riconquistati a seguito della vicenda oggetto di notizia[201]. Il diritto all'oblio si pone, dunque, come crocevia nel bilanciamento tra il diritto di cronaca e di informazione e il diritto alla riservatezza e alla reputazione[202].

L'avvento del mondo digitale e della rete *Internet* ha comportato la permanente disponibilità per il pubblico di archivi digitali di informazioni che non risultano integrati ed aggiornati con le notizie degli eventi successivi. In questo contesto, il problema non è tanto la riproposizione di un'informazione, posto che la stessa è sempre pubblicamente accessibile, quanto la completezza e veridicità della stessa. Pertanto, il diritto all'oblio ha conosciuto una seconda accezione, quale contestualizzazione ed aggiornamento dell'informazione nel tempo rispetto agli eventi ulteriori della vicenda[203]. L'oblio risulta quindi attuabile, non solo tramite la cancellazione della notizia ripubblicata, ma anche con la rettifica ed integrazione della stessa rispetto al momento storico in cui risulta disponibile al pubblico[204].

Con la nota sentenza C-131/12 della Corte di Giustizia dell'Unione Europea (Grande Sezione), *Google Spain SL, Google Inc./Agencia de Proteccion de Datos (AEPD), Mario Costeja Gonzales*, il diritto all'oblio ha conosciuto una terza ed ulteriore accezione quale diritto alla deindicizzazione presso i motori di ricerca. Segnatamente, secondo la Corte di Giustizia, il trattamento effettuato dal gestore di un motore di ricerca può «incidere significativamente sui diritti fondamentali al rispetto

---

[199] Così G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 396. Sulla definizione del diritto all'oblio, cfr. anche G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti alla personalità*, cit., p. 592, e T. AULETTA, *op. cit.*, p. 129.

[200] Cfr. G.B. FERRI, *op. cit*., pp. 813 ss.

[201] Cfr. Cass., sent. n. 3679/98.

[202] Cfr. E. PELINO, *I diritti dell'interessato*, in L. BOLOGNINI-E. PELINO-C. BISTOLFI, *op. cit*., p. 262, secondo il quale, l'applicazione del diritto all'oblio «tiene conto di molteplici fattori, quali, senza tassatività, la gravità della notizia, il peso sociale degli eventi, il suo pregio informativo, l'attualità residua, il ruolo e la posizione pubblica dell'interessato».

[203] Cfr. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., pp. 396 ss. Cfr. anche Cass., sent. n. 5525/12: «Anche in caso di memorizzazione nella rete internet, mero deposito di archivi dei singoli utenti che accedono alla rete e cioè dei titolari dei siti costituenti la fonte dell'informazione (c.d. siti sorgente), deve riconoscersi al soggetto cui pertengono i dati personali oggetto di trattamento ivi contenuti il diritto all'oblio, e cioè al relativo controllo a tutela della propria immagine sociale, che anche quando trattasi di notizia vera, e a fortiori se di cronaca, può tradursi nella pretesa alla contestualizzazione e aggiornamento dei medesimi, e se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione».

[204] Cfr. A. RICCI, *op. cit*., p. 205.

della vita privata e alla protezione dei dati personali», posto che, tramite tali strumenti, è possibile, per qualsiasi utente di Internet, ottenere un profilo strutturato di una persona con l'elenco delle correlate informazioni reperibili su Internet, anche rispetto alla relativa vita privata[205]. Considerato, di contro, il legittimo interesse degli utenti di Internet all'accesso ai motori di ricerca, la Corte ha rilevato la necessità che il diritto all'oblio sia, di volta in volta, valutato al fine di contemperare un «giusto equilibrio» tra detto legittimo interesse ed i diritti fondamentali della persona di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea[206]. Sempre secondo la Corte, un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la disciplina europea in materia di protezione dei dati personali qualora tali dati «risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso»[207]. Ne deriva, pertanto, che l'interessato ha il diritto di chiedere direttamente ai motori di ricerca la deindicizzazione delle informazioni che lo riguardano, da intendersi come soppressione, dall'elenco dei risultati della ricerca effettuata sulla base del nome di una persona, dei link alle pagine web pubblicate da soggetti terzi contenenti informazioni su tale persona. Ciò, anche nel caso in cui il nome o le informazioni sull'interessato «non vengano previamente o simultaneamente cancellati dalle pagine *web* di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine *web* sia di per sé lecita»[208] [209].

Il diritto all'oblio così inteso risulta assimilabile, almeno in parte, al diritto alla cancellazione di cui all'art. 17 GDPR e, in questo senso, deve essere interpretato il riferimento all'oblio, contenuto, tra parentesi, nella relativa rubrica. La differenza tra i diritti in esame va, pertanto, ricercata nel fatto che «la cancellazione è un'operazione sui dati che esclude ogni ulteriore conservazione degli stessi, mentre l'oblio sembra piuttosto una finalità, che si può raggiungere con la cancellazione, ma anche con il blocco»[210]. Restano allora le perplessità evidenziate dalla dottrina sull'impropria sovrapposizione, operata dalla rubrica dell'art. 17 GDPR, tra il diritto alla cancellazione e il diritto all'o-

[205] In tal senso, cfr. CGUE (Grande Sezione), *Google Spain SL, Google Inc./Agencia de Proteccion de Datos (AEPD), Mario Costeja Gonzales*, 13 maggio 2014, C-131/12, par. 80.

[206] Su tale valutazione, *ibidem*, par. 81: «Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica».

[207] *Ibidem*, par. 93.

[208] *Ibidem*, par. 88.

[209] A tale riguardo, cfr. Gruppo di lavoro articolo 29, Linee Guida sull'attuazione della sentenza della Corte di Giustizia dell'Unione Europea nel caso C-131/12 *"Google Spain e Inc. contro Agencia Española De Protección De Datos (AEPD) e Mario Costeja González"*, 26 novembre 2014, con le quali il Gruppo di lavoro articolo 29 ha successivamente individuato i criteri per applicazione, da parte delle autorità di controllo nazionali, dei principi della sentenza C-131/12 della Corte di giustizia dell'Unione Europea, *cit*. Cfr., inoltre, EDPB, Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGPD (parte 1), 7 luglio 2020, versione 2.0.

[210] Cfr. G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti alla personalità*, cit., p. 596.

blio così inteso[211], con il rischio di appiattire quest'ultimo alla disciplina del primo senza tenere conto della citata giurisprudenza della Corte di giustizia, che il legislatore europeo avrebbe dovuto meglio tradurre, in maniera più puntuale, nelle maglie del GDPR[212].

Da ultimo, si segnala che, con il co. 1, lett. *h),* dell'art. 41, del d.lgs. n. 150 del 10 ottobre 2022, in attuazione della l. 134/2021, è stato introdotto l'art. 64-*ter* delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale che ha riconosciuto espressamente il diritto della persona, nei cui confronti siano stati pronunciati una sentenza di proscioglimento o di non luogo a procedere ovvero un provvedimento di archiviazione, di richiedere, ai sensi e nei limiti dell'art. 17 GDPR, che sia preclusa l'indicizzazione o che sia disposta la deindicizzazione, sulla rete internet, dei dati personali riportati nella sentenza o nel provvedimento. A seguito di tale richiesta, la cancelleria del Giudice che ha adottato il provvedimento provvede all'apposizione e sottoscrizione delle annotazioni indicate di cui all'art. 64-*ter,* co. 2 e 3, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale[213].

[211] Cfr. E. PELINO, *I diritti dell'interessato*, cit., p. 263.

[212] In tal senso, cfr. F. DI CIOMMO, *op. cit.*, p. 371; V. CUFFARO, *Cancellare i dati personali. Dalla* damnatio memoriae *al diritto all'oblio*, cit., p. 227 ss.; M.A. LIVI, *op. cit*., pp. 293 ss.

[213] Sul punto, cfr. GPDP, Provv. 1° settembre 2022, Parere sullo schema di decreto legislativo di attuazione della legge 27 settembre 2021 n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari, doc. *web* n. 9802612. Per un commento all'art. 64-*ter* delle norme di attuazione, di coordinamento e transitorie c.p.p., cfr. M. MARINI, *Oblio, deindicizzazione e processo penale: dal diritto eurounitario alla riforma Cartabia*, in *Sistema Penale*, 2023, 1, p 5.

Capitolo IX

Il principio di integrità e riservatezza (*rectius*, di sicurezza)

*Gian Mauro Bilotta - Daniele Sborlini - Ilaria Scarpelli**

SOMMARIO: 1. Inquadramento normativo. – 2. Portata del principio. – 2.1. Le funzioni della sicurezza in materia di trattamento dei dati personali e il *risk management approach*. – 2.2. La sicurezza del trattamento e le sue declinazioni (riservatezza, integrità, disponibilità). – 2.3. Le misure di sicurezza tecniche e organizzative ai sensi dell'art. 32 GDPR e le istruzioni ai sensi dell'art. 29 GDPR. – 2.4. La sicurezza del trattamento sin dalla progettazione e per impostazione predefinita. – 2.5. La sicurezza del trattamento in caso di violazione dei dati (*data breach*). – 2.6. La sicurezza nei trattamenti che presentano rischi elevati (DPIA). – 3. Applicazione del principio nella casistica.

1. Inquadramento normativo

Sotto il perentorio titolo «*Principi*», il Capo II del Reg. UE n. 679/2016 (di seguito GDPR), in particolare agli articoli da 5 a 11, elenca e dettaglia tutti quei precetti fondamentali che permeano e disciplinano, in via generale, il trattamento dei dati personali. Nello specifico, all'art. 5, rubricato «*Principi applicabili al trattamento dei dati personali*» viene previsto, tra gli altri, il principio di «*integrità e riservatezza*», secondo il quale «I dati personali sono (…) trattati in maniera da garantire un'adeguata *sicurezza* dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("*integrità* e *riservatezza*")» [art. 5, par. 1, lett. *f)*, GDPR].

Il principio in esame dunque, pur denominato espressamente, dal legislatore europeo, principio di «*integrità* e *riservatezza*», intende riferirsi, sostanzialmente, alla «sicurezza» dei dati personali e dei sistemi utilizzati per il loro trattamento, come si comprende sia dal tenore dell'articolo sopra riportato, sia dal *considerando* n. 39, nel quale si precisa che «(…) I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata *sicurezza* e *riservatezza*, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento»[1].

---

* Pur essendo lo scritto, nel suo complesso, frutto di riflessioni comuni, i parr. 1 e 2 sono da attribuire a Gian Mauro Bilotta e Ilaria Scarpelli, il par. 3 è da attribuire a Daniele Sborlini.

[1] Con tale precisazione il concetto di sicurezza dei dati personali viene esplicitamente riferito anche agli apparati tecnologici utilizzati per il trattamento. Viene quindi sottolineato che la sicurezza è da

A ben guardare, il linguaggio legislativo ha voluto riferirsi ai singoli elementi in cui si sostanzia la sicurezza, per indicare quest'ultima nel suo complesso: l'"*integrità*" e la "*riservatezza*", unitamente alla "*disponibilità*", sono gli aspetti in cui si traduce la "*sicurezza*" delle informazioni e dei sistemi. Sono infatti gli stessi parametri utilizzati nel metodo di analisi *risk-based* nel manuale dell'ENISA pubblicato nel 2016 e revisionato nel 2017[2].

Più precisamente, con riguardo alla *sicurezza* dei dati personali, il concetto di "*integrità*" si riferisce alla necessità di preservare i dati personali da fenomeni di distruzione o cancellazione, totale o parziale; il concetto di "*disponibilità*" fa invece riferimento alla necessità di garantire l'accesso e la fruizione dei dati personali, limitatamente a quanto occorra per gli usi legittimi del trattamento; il concetto di "*riservatezza*" si riferisce invece alla necessità di precludere l'accesso ai dati personali, così come ogni altra operazione di trattamento, a quanti non siano legittimati.

Nell'art. 5, par. 1, lett. *f)*, GDPR, dunque, il termine «*riservatezza*» – così come quello di «*integrità*» – va inteso in senso tecnico, quale *connotato della sicurezza*. Il legislatore europeo, nel richiamare l'integrità e la riservatezza come principio, ha chiaramente voluto affermare, nella disposizione ora citata, la necessità di garantire la "*sicurezza*" dei dati personali, unitariamente considerata in tutte le sue componenti e per l'intero ciclo di vita del trattamento.

La "sicurezza" dei dati richiede che il trattamento sia presidiato da adeguate misure tecniche e organizzative, da predisporre prima ancora che il medesimo venga svolto. Deve inoltre essere assicurata già in fase di progettazione del trattamento e deve garantire il rispetto dei diritti e delle libertà dell'interessato per impostazione predefinita, mediante ulteriori misure tecniche e organizzative. Deve infine presidiare il trattamento anche in caso di violazione dei dati.

Il principio in esame trova dunque una sua specificazione innanzitutto nella Sezione 2 del Capo IV del GDPR, intitolata «*Sicurezza dei dati personali*», nella

intendersi riferibile con riguardo non solo ai dati personali in sé ma anche alle attrezzature impiegate per il trattamento.

[2] ENISA, *Manuale sulla Sicurezza nel trattamento dei dati personali*, 2017, *passim*. Ivi, con riferimento al GDPR, viene altresì rimarcato, a p. 6, che «Ai sensi del Regolamento, uno degli obblighi fondamentali per tutte le imprese, comprese le PMI, che agiscono in qualità di Titolari o di Responsabili del trattamento, è quello della *sicurezza* nel trattamento dei dati personali. In particolare, secondo il GDPR, la sicurezza è una tematica che *include* anche quelle della *riservatezza*, *integrità* e *disponibilità* dei dati e dovrebbe essere considerata seguendo un *approccio basato sul rischio*: più alto è il rischio e più rigorose devono essere le misure che il Titolare o il Responsabile del trattamento devono considerare (per gestire il rischio). Anche se questo approccio basato sul rischio non è un nuovo concetto, sono stati presentati solo alcuni specifici quadri di valutazione del rischio per la *privacy*, focalizzandosi principalmente sulla valutazione del rischio sui dati personali e sull'adozione di adeguate misure di sicurezza pertinenti».

quale assumono un ruolo centrale l'art. 32[3] GDPR, rubricato «*Sicurezza del trattamento*», gli artt. 33[4] e 34[5], dedicati alla disciplina del *data breach* e l'art.

[3] L'art. 32 del GDPR, rubricato «*Sicurezza del trattamento*», stabilisce che «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

[4] L'art. 33 del GDPR, rubricato «*Notifica di una violazione dei dati personali all'autorità di controllo*», stabilisce che «1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo».

[5] Ai sensi dell'art. 34 del GDPR, rubricato «*Comunicazione di una violazione dei dati personali all'interessato*», «1. Quando la violazione dei dati personali è suscettibile di presentare un rischio

35[6], dedicato alla valutazione d'impatto, secondo l'approccio del *risk management*.

elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere *b)*, *c)* e *d)*.
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta».

[6] L'art. 35 GDPR, rubricato «*Valutazione d'impatto sulla protezione dei dati*», dispone che «1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
7. La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

Il principio in parola trova altresì una sua specificazione anche nell'art. 25[7] in tema di *privacy by design* e *by default*, contenuto nella Sezione 1 del medesimo Capo, dedicata agli «*Obblighi generali*»[8].

La sicurezza deve però coinvolgere anche tutti i soggetti che, per conto del titolare, effettuano il trattamento dei dati personali. Tenendo conto di ciò ulteriori

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere *c)* o *e)*, trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento».

[7] L'art. 25 del GDPR, rubricato «*Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*», stabilisce che «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo».

[8] Sull'art. 25 GDPR e sul principio di *privacy by design* e *by default* si veda, *amplius*, F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 775-854; nonché F. Bravo, *Data Management Tools and Privacy by Design and by Default*, in R. Senigaglia-C. Irti-A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Springer, 2022, pp. 85-95; R. D'orazio, *Protezione dei dati* by default *e* by design, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della* privacy, Milano, 2016, pp. 79 ss. Si veda altresì, nel presente volume, S. Faillace, *Il principio di* privacy by design *e* by default (Capitolo XII).

riferimenti alla sicurezza, nelle sue diverse dimensioni, sono presenti nell'art. 28 del GDPR, in tema di responsabile del trattamento, incluso l'obbligo – previsto nell'art. 28, par. 3, lett. *b)* e *c)*, GDPR – di garantire «che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza» e di adottare «tutte le misure richieste ai sensi dell'art. 32»[9]. In questa prospettiva va letto anche l'art. 29 GDPR, ove si prevede che «Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

L'impostazione seguita nel GDPR è innovativa: ripercorrendo l'evoluzione normativa in materia di protezione dei dati personali che ha interessato gli aspetti dell'«integrità e riservatezza» – ovvero, più in generale, della "sicurezza" – si avverte il passaggio, nel susseguirsi delle differenti disposizioni legislative europee e nazionali, da mero "obbligo" a vero e proprio "principio cardine" di sistema, per quanto riguarda la tutela dei dati personali[10].

In tal senso si potrebbe riconoscere un primo riferimento nell'omologo art. 5 dalla Convenzione di Strasburgo n. 108 del 1981 del Consiglio d'Europa, aggiornata recentemente con il Protocollo emendativo del 18 maggio 2018. La Convenzione n. 108, nel momento della sua emanazione, costituiva uno dei più importanti e lungimiranti strumenti normativi posti a tutela delle persone fisiche a garanzia dei possibili abusi connessi al trattamento di dati personali, se svolto con mezzi (in tutto o in parte) automatizzati. La Convenzione n. 108 costituiva a quei tempi, infatti, l'unico strumento internazionale giuridicamente vincolante in materia di protezione dei dati personali e si applicava a tutti i trattamenti di dati personali effettuati sia nel settore privato che nel pubblico e, in tale ambito, anche a quelli effettuati da autorità giudiziarie e di polizia. La sua emanazione si è collocata nel solco dell'art. 8 della

---

[9] Rispetto alle previsioni dell'art. 28 GDPR, si evidenzia che l'obbligo del titolare del trattamento di avvalersi unicamente di responsabili «che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento (…)» (art. 28, par. 1, GDPR) riguarda anche i profili legati alla sicurezza, come emerge dal *considerando* n. 81 del GDPR, il quale prevede espressamente che il responsabile debba presentare «garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, *anche per la sicurezza del trattamento*».
Si consideri inoltre che il responsabile del trattamento, oltre a dover «adottare tutte le misure richieste dall'art. 32» [art. 28, par. 3, lett. *c),* GDPR], è anche tenuto ad assistere il titolare nel garantire il rispetto degli obblighi previsti, tra l'altro, dall'32 GDPR [art. 28, par. 3, lett. *f)*, GDPR]. Come evidenziato dall'EDPB, quest'obbligo è distinto da quello stabilito alla lett. *c)* richiamata poc'anzi, in quanto riferito alle misure di sicurezza del titolare e non a quelle che il responsabile stesso deve adottare (cfr. EDPB, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, ver. 2.0, adottate il 7 luglio 2021, p. 42, punto 135).

[10] Sulla transizione dell'obbligo di adozione di misure di sicurezza adeguate da specifica regola a principio, si veda ad es. F. RESTA, *Principi applicabili al trattamento di dati personali*, in G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, pp. 60-61.

Convenzione europea dei diritti dell'uomo del 1950, dedicato al diritto al rispetto della vita privata e familiare[11].

Tra le prescrizioni della Convenzione n. 108 del 1981 si riscontra, all'art. 7, l'obbligo di adottare «idonee misure di sicurezza (…) per la protezione dei dati a carattere personale registrati nelle collezioni automatizzate contro la distruzione accidentale o non autorizzata, o la perdita accidentale, nonché contro l'accesso, la modificazione o la diffusione non autorizzati».

Si nota chiaramente la declinazione degli obblighi di *sicurezza* nei diversi aspetti volti a preservarne sia l'*integrità* e la *disponibilità* dei dati, contro le ipotesi di distruzione, modificazione e perdita dei dati medesimi, sia la *riservatezza*, contro le ipotesi di accesso e diffusione non autorizzati.

Le disposizioni della Convenzione di Strasburgo hanno funzionato da modello per l'emanazione, in seno all'allora Comunità europea, della Direttiva "madre" 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, in materia di protezione dei dati personali.

Tale direttiva non individuava la «sicurezza» (e le sue declinazioni in termini di "integrità, disponibilità e riservatezza") nei «*Principi relativi alla qualità dei dati*» (a cui è dedicata la Sezione I, in cui si trova il solo art. 6). Veniva invece disciplinata al di fuori del novero dei "principi", all'interno di un'apposita sezione intitolata «*Riservatezza e sicurezza dei trattamenti*» (Sezione VIII), composta dagli artt. 16 e 17, rubricati rispettivamente «*Riservatezza dei trattamenti*» e «*Sicurezza dei trattamenti*».

Mentre nel primo di tali articoli veniva stabilito che «*Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law*», nel successivo art. 17 veniva ribadito l'obbligo, per gli Stati membri, di imporre al titolare del trattamento l'adozione di misure di sicurezza tecniche e organizzative adeguate a proteggere i dati personali contro eventi che potessero comprometterne l'integrità, la riservatezza e la disponibilità[12].

---

[11] Già nel preambolo del testo originario della Convenzione n. 108 del 1981, poi parzialmente modificato dal protocollo addizionale del 2018, si rimarcava infatti che «è auspicabile estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica». Nel testo attuale della Convenzione (108+) si pone maggiore enfasi sulla protezione dei dati personali. Nel preambolo aggiornato si rimarca che «*it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data*», che «*the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression*» e che «*it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people*».

[12] L'art. 17 della Direttiva 95/46/CE, rubricato «*Sicurezza dei trattamenti*», prevedeva che «1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizza-

Venivano individuati quegli obblighi che sarebbero, con il GDPR, assurti anche al rango di "principio" nell'art. 5, par. 1, lett. *f)* (principio di «integrità e riservatezza»).

In attuazione della Direttiva 95/46/CE, venne in Italia emanata inizialmente la l. 31 dicembre 1996, n. 675 che all'art. 15 (rubricato «*Sicurezza dei dati*») prevedeva, come da indicazioni impartite nel testo comunitario, l'obbligo di predisporre misure di sicurezza per il trattamento dei dati personali, volte a ridurre al minimo i rischi idonei a compromettere l'integrità, la disponibilità e la riservatezza dei dati[13]. Nell'ambito di tali misure la scelta legislativa era stata poi quella di individuarne altre più circoscritte, definite "misure minime di sicurezza", la cui omissione avrebbe comportato anche una responsabilità di natura penale, ai sensi dell'art. 36.

---

tive appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.
Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.
2. Gli Stati membri dispongono che il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure.
3. L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:
– che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento;
– che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.
4. A fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti concernenti le misure di cui al paragrafo 1 sono stipulati per iscritto o in altra forma equivalente».

[13] L'art. 15 della l. n. 675/1996 stabiliva che «1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
2. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante.
3. Le misure di sicurezza di cui al comma 2 sono adeguate, entro due anni dalla data di entrata in vigore della presente legge e successivamente con cadenza almeno biennale, con successivi regolamenti emanati con le modalità di cui al medesimo comma 2, in relazione all'evoluzione tecnica del settore e all'esperienza maturata.
4. Le misure di sicurezza relative ai dati trattati dagli organismi di cui all'articolo 4, comma 1, lettera b), sono stabilite con decreto del Presidente del Consiglio dei ministri con l'osservanza delle norme che regolano la materia».

Quando la l. n. 675/1996 venne sostituita, successivamente e dopo alcune modifiche, con il d.lgs. n. 196 del 2003 (Codice in materia di protezione dei dati personali), rimase la distinzione tra le due categorie di misure di sicurezza, previste rispettivamente all'art. 31[14], rubricato «*Obblighi di sicurezza*» e all'art. 33[15], rubricato «*Misure minime*», che trovava specificazione sia nei successivi artt. 34, 35 e 36, sia in un allegato tecnico al Codice (il c.d. Disciplinare tecnico, All. B), poi abrogato[16].

L'impianto normativo è stato poi rivoluzionato dalle successive scelte del legislatore europeo, con l'emanazione del Reg. (UE) n. 679/2016 (GDPR), direttamente applicabile in tutti i Paesi dell'UE dal 25 maggio 2018, a seguito della quale l'Italia ha provveduto ad emendare le norme di diritto interno, abrogando le sopra citate disposizioni del Codice in materia di protezione dei dati personali in forza dell'intervento di riforma avutosi con il d.lgs. n. 108 del 2018.

Nello stesso anno, a seguito del constatato bisogno di modificare il testo normativo della Convenzione 108 per adeguarlo al mutato contesto sociale e tecnologico, oltre che per adattarlo alle disposizioni contenute nel GDPR, il Consiglio d'Europa ha adottato un Protocollo di modifica alla predetta Convenzione (c.d. Convenzione 108+) che fornisce un quadro giuridico più forte e incisivo, ma allo stesso tempo più versatile e flessibile, per agevolare il flusso dei dati attraverso le "frontiere" degli Stati aderenti.

L'aggiornamento normativo ha portato ad una riformulazione delle disposizioni in materia di sicurezza, ad iniziare dall'art. 7, rubricato «*Data security*», al cui primo comma viene ora stabilito che «*Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data*», mentre al secondo comma si esplicita la disciplina del *data breach*, prevedendo che «*Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects*».

---

[14] L'art. 31 del d.lgs. n. 196 del 2003, rubricato «*Obblighi di sicurezza*», poi abrogato, stabiliva che «1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta».

[15] Ai sensi dell'abrogato art. 33 del d.lgs. n. 196 del 2003, rubricato «*Misure minime*», veniva previsto che «1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali».

[16] Relativamente agli obblighi di sicurezza previsti dalle abrogate disposizioni del d.lgs. n. 196/2003, si vedano P. Troiano, *Sicurezza dei dati e dei sistemi*, in C.M. Bianca-F.D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196*, Padova, 2007, pp. 682 ss.; P. Perri, *Le misure di sicurezza*, in J. Monducci-G. Sartor (a cura di), *Il Codice in materia di protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003 n. 196*, Padova, 2004, pp. 137 ss.

Si registra dunque, a livello internazionale, un'esportazione del modello delineato nel GDPR, con un'acquisita centralità del principio di sicurezza.

2. PORTATA DEL PRINCIPIO

2.1. Le funzioni della sicurezza in materia di trattamento dei dati personali e il *risk management approach*

Per comprendere meglio la portata del principio in parola non si può non ripercorrere, seppur brevemente e senza pretese di esaustività, l'approccio che si è originariamente avuto in ambito europeo e nazionale in materia di sicurezza e protezione dei dati personali e come esso sia mutato nel tempo[17].

Va ricordato, in particolare, che l'approccio alla gestione del rischio di fronte al trattamento dei dati personali entra e si sviluppa nelle diverse normative che, dalla fine degli anni '60 in poi, si succedettero in materia di tutela dei dati personali[18]. I primi interventi normativi, infatti, furono molto influenzati dai "timori" connessi alla raccolta massiccia di informazioni personali che gli Stati avevano iniziato ad accumulare in poderosi archivi, sebbene ancora non del tutto meccanizzati e informatizzati, nel periodo del dopoguerra e con l'inizio della "guerra fredda"[19]. La paura suscitata dall'ancora troppo vivido ricordo delle dittature che avevano portato l'Europa a scatenare il secondo conflitto mondiale, spinsero verso un concetto di *data protection*, infatti, non solo come una derivazione del tradizionale *right to privacy* di Bostoniana memoria[20], bensì come reazione al possibile "rischio sociale" e conseguente potenziale pregiudizio della società civile e dei singoli cittadini riconducibile, grazie allo sviluppo dell'informatica che si affacciava in maniera preponderante e sempre più pervasiva alla fine degli anni settanta, all'evidente maggiore capacità

[17] In materia si vedano, tra gli altri, G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Milano, 2003; P. PERRI, *Privacy, diritto e sicurezza informatica*, Milano, 2007; P. PERRI, *Protezione dei dati e nuove tecnologie. Aspetti nazionali, europei e statunitensi*, Milano, 2007; A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 287 ss., nonché A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, pp. 473 ss.

[18] Cfr. A. MANTELERO, *La gestione del rischio*, cit., p. 477.

[19] *Ibidem*, pp. 477 ss., ove viene ricordata l'impostazione ed il pensiero di S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, pp. 25 ss. e 50 ss. L'accumulo dei dati personali da parte dei pubblici poteri, concernenti i cittadini, comportava l'accentramento in mano pubblica di nuovi poteri di controllo, nei cui confronti, a partire dagli anni '60, vennero rivendicate istanze di tutela a fronte dei rischi connessi alla "schedatura di massa". Nel corso del tempo, il fenomeno dell'accentramento dei dati e del relativo potere si è esteso dai soggetti pubblici a quelli privati (si pensi ai *Big Player* del settore IT, per lo più multinazionali americane).

[20] S. WARREN-L. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review,* 15 December 1890, 4.

tecnologica che rendeva possibili forme sempre più invasive, e non controllabili, di schedatura di massa[21] o, più pervasivamente, di sorveglianza di massa[22].

Si assiste pertanto ad una spinta nella direzione di elaborare normative che garantiscano ai cittadini di operare un sempre maggior controllo sull'acquisizione delle informazioni che li riguardano, resa possibile sempre di più dalla capacità di messa in relazione delle diverse banche dati ad opera degli Stati nazionali, ma anche di organismi privati accentratori di un forte potere, connesso all'utilizzo di tecnologie informatiche sempre più evolute[23].

Alla pretesa di tutela in termini di trasparenza, avanzata da parte dei soggetti interessati dal trattamento dei dati, le legislazioni nazionali e sovranazionali hanno risposto fornendo progressivamente norme sempre più evolute implicanti la disciplina della raccolta e dell'elaborazione dei dati personali, in una prospettiva di bilanciamento di contrapposti interessi, sicché le tecniche di tutela finirono progressivamente con l'essere incentrate non tanto sulla difesa della vita privata contro indebite intrusioni ad opera di soggetti pubblici o privati, ma sul nuovo diritto alla protezione dei dati personali, inteso come un diritto a controllare che il trattamento dei dati personali sia svolto in maniera corretta, lecita e conformemente alle prescrizioni imposte dalla normativa di settore, a protezione degli interessati[24].

Si viene ad affermare, in altre parole, una nuova prospettiva circa il rapporto fra informazione e persona, fondato non tanto – o, meglio, non soltanto – sul diritto alla tutela della propria sfera di intimità connessa allo svolgimento della vita privata, limite invalicabile che anche "i re avrebbero dovuto rispettare"[25], bensì su esigenze

---

[21] Cfr. A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. valutazione d'impatto e consultazione preventiva (artt. 32-39)*, cit., pp. 287 ss., nonché A. Mantelero, *La gestione del rischio*, cit., pp. 473 ss.

[22] Su «L'utilizzo delle tecnologie per sorvegliare il cittadino» si vedano le pagine di G. Ziccardi, *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Milano, 2008, II, pp. 150 ss., nonché, sul medesimo tema, A. Bellavista, *Società della sorveglianza e protezione dei dati personali*, in *Contratto e impresa*, 1996 e P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020; si veda anche D. Lyon, *The electronic eye: the rise of surveillance society*, Minneapolis, 1994 e più recentemente, Id., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2003; Id., *La cultura della sorveglianza*, Roma, 2020.

[23] A tal riguardo si veda A. Mantelero, *La gestione del rischio*, cit., p. 478, per il quale «è proprio la domanda di conoscenza ad affiorare nelle prime prese di posizione da parte dei cittadini, intimoriti dalla concentrazione di questo nuovo potere che si stava realizzando nelle mani della pubblica amministrazione, laddove l'informatizzazione dei diversi servizi apriva nuovi scenari in cui il cittadino veniva "messo a nudo" grazie all'incrocio fra le molteplici informazioni conservate nelle diverse banche dati pubbliche, da quelle fiscali a quelle sanitarie a quelle dei servizi sociali ed assistenziali, fino a quelle di polizia. Tale istanza andrà poi rafforzandosi nel tempo quando accanto alle grandi burocrazie saranno anche le imprese a diventare collettori di dati personali, consentendo di disvelare nuovi aspetti della vita di ciascuno, dalle abitudini di consumo ai dati sanitari, alle opinioni personali».

[24] *Ibidem*, p. 478.

[25] «(…) il più povero degli uomini può, nella sua casetta lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina». Così Lord Chatham,

di protezione che, nella prospettiva del bilanciamento di diritti confliggenti, facciano salve le pretese legittime alla raccolta e all'uso dei dati, divenuti presupposto ineliminabile di ogni attività[26]. Si assiste alla nascita del diritto al corretto trattamento dei dati personali degli interessati ed a ricevere protezione avverso i *rischi* che i trattamenti possono comportare per i diritti e le libertà degli interessati[27].

Le normazioni nazionali ed europee in tema di tutela dei dati personali, seguendo tale approccio, si arricchirono anche di specifiche prescrizioni in ordine a precisi obblighi in materia di sicurezza del trattamento, richiedendo specifica attenzione anche agli aspetti tecnici e procedimentali connessi al trattamento dei dati personali, di cui si vede un esempio chiaro già nella Convenzione del Consiglio d'Europa n. 108 del 1981.

Il concetto di *rischio* che gli obblighi di sicurezza mirano ad affrontare in tale materia, per la verità, è da intendere in una duplice direzione: da un lato, come rischio contro minacce che possano comportare una "violazione dei dati" (*data breach*), causata generalmente, ma non necessariamente, da attività illecita; dall'altro lato, come rischio avverso possibili conseguenze negative correlate all'utilizzo, di per sé "lecito", di informazioni di carattere personale, correttamente acquisite e lecitamente trattate, ma il cui trattamento potrebbe essere non gradito all'interessato (ad es., ove effettuato dalla controparte per la tutela di un diritto in sede giudiziaria) o comunque, se voluto, implicante un'esposizione a rischi che il titolare è chiamato a gestire (ad es., nel caso di trattamenti svolti dal datore di lavoro, per la gestione della sicurezza negli ambienti in cui viene espletata l'attività lavorativa dei dipendenti o, ancora, in caso di tracciamento *online* mediante *cookies* espressamente accettati dall'interessato, nell'ambito di attività di profilazione, per utilizzi nel settore della pubblicità *online* o per altre ragioni). Sicché la gestione del rischio impone che il trattamento venga effettuato facendo di tutto per escludere – o quantomeno per ridurre al minimo – ogni possibile pregiudizio derivante da fattori esterni o interni alla struttura che si occupa del trattamento.

In questa ottica, già nella Direttiva "madre" 95/46/CE la gestione del rischio connesso al trattamento e la sua pratica attenuazione si incentravano chiaramente sulla sicurezza – soprattutto informatica[28] – e sulla conseguente esplicita necessità di

---

Discorso al Parlamento Inglese del 1766, in M. IASELLI-S. GORLA (a cura di), *Storia della Privacy*, Roma, 2015, pp. 27.

[26] Sul rilievo giuridico della pretesa di fare uso dei dati personali altrui, si veda l'approfondita analisi di F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018 (in particolare, sul carattere imprescindibile delle attività di trattamento dei dati personali nell'attuale contesto socio-politico, si vedano le pp. 42 ss.).

[27] V. FROSINI*, Diritto alla riservatezza e calcolatori elettronici*, in AA.Vv., *Il riserbo e la notizia. Atti del convegno di Studio di Macerata*, 5-6 marzo 1982, Napoli.

[28] Sulle caratteristiche della gestione del rischio prevista dalla citata Direttiva e, in particolare, sulla circostanza che tale normativa considerava il rischio essenzialmente nel contesto di un'ottica fondata sulla sicurezza informatica, si veda A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, cit., pp. 298 ss.; F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, pp. 277 ss.

adottare, come si legge nel *considerando* n. 46[29], misure di protezione dei dati e delle libertà personali da attuarsi con l'adozione di misure di sicurezza volte a prevenire anche quei trattamenti non autorizzati e illeciti; gestione del rischio esplicitamente ripresa, poi, anche nell'art. 17 della Direttiva cit.[30].

Venendo a tempi più recenti occorre evidenziare che il Reg. UE n. 679/2016 si può leggere in assoluta continuità, per quanto riguarda le tematiche connesse alla sicurezza del trattamento dei dati, con la citata Direttiva 95/46/CE, anche se, sullo specifico tema della gestione del rischio, il GDPR mostra caratteri distintivi e un approccio innovativo[31], facendo assurgere la *sicurezza* da mero obbligo a vero e proprio "principio cardine", che permea e informa l'intera normativa europea, accompagnato da obblighi di maggior dettaglio, che mirano a rendere effettiva la sua applicazione, in molteplici direzioni.

Il principio in analisi, "*integrità e riservatezza*" – enunciato dall'art. 5, par. 1, lett. *f)* del GDPR – infatti, si sostanzia e specifica, nel dettato del Regolamento, nel generale e pervasivo *principio di sicurezza*, nel rispetto del quale tutti i dati personali devono essere obbligatoriamente trattati in maniera tale da assicurare un'adeguata sicurezza dei dati personali, compresa la protezione, mediante l'adozione di *adeguate* misure tecniche e organizzative, da trattamenti non autorizzati o illeciti, e dalla perdita, dalla distruzione o dal danno accidentali, così come precisamente stabilito dalla disposizione poc'anzi citata e ulteriormente chiarito dal correlato *considerando* n. 39.

Trattandosi di principio, esso ha un ruolo "ordinante" rispetto agli istituti e alle norme che nel GDPR incentrano gli adempimenti proprio sulla sicurezza dei dati personali.

Il principio in questione fa riferimento a misure "adeguate", sicché la normativa europea impone al titolare e al responsabile di garantire, nel trattamento posto in essere, un livello di sicurezza non tanto "assoluto" e aprioristicamente predefinito, ma parametrato sulla base degli effettivi rischi che potrebbero insistere sul trattamento, dovendosi, in tale valutazione, tenere in debito conto di tutti quegli elementi, espressamente indicati dall'art. 32, par. 1, GDPR, dedicato alla sicurezza del trattamento[32]. Sotto l'aspetto della valutazione del rischio, allora, diventerà assolutamente

---

[29] Nel *considerando* n. 46 della Direttiva 95/46/CE viene infatti messo in evidenza «che la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato (…)» e «(…) che spetta agli Stati membri accertarsi che il responsabile del trattamento osservi tali misure; che queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere».

[30] Cfr., *supra*, nota n. 12.

[31] Su continuità e differenze tra la gestione del rischio prevista dalla Direttiva madre e il GDPR, si veda A. Mantelero, *La gestione del rischio*, cit., pp. 475 ss.; F. Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, cit., pp. 277 ss.

[32] Su portata e contenuti dell'obbligo di adozione di misure di sicurezza "adeguate", si veda ad es. G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679*

necessario evidenziare la natura, il contesto, le finalità del trattamento entro la cui cornice potrebbe verificarsi e rappresentarsi un eventuale rischio, unitamente alla esatta determinazione della probabilità e gravità di accadimento del medesimo rischio, da leggersi in rapporto alle dirette conseguenze per i diritti e le libertà degli interessati, persone fisiche i cui dati sono oggetto di trattamento.

Il principio di sicurezza va però anche in altre innovative direzioni. L'evoluzione normativa citata evidenzia con chiarezza come l'approccio al rischio, in generale, e alla sua gestione mediante un sistema in grado di realizzare a tutto tondo la sicurezza del trattamento e dei dati personali, permei, ora, tutto il Regolamento, tant'è che, travalicando l'obbligo delineato dall'art. 32 GDPR, la gestione della sicurezza è delineata a tutti i livelli del trattamento e attinge a collaudate tecniche di analisi dei rischi tipicamente utilizzate in altri contesti disciplinari.

Le misure tecniche e organizzative fanno da sfondo all'applicazione dell'intera disciplina nella prospettiva dell'*accountability* (art. 24 GDPR) e sono state affermate dal legislatore europeo anche nell'iniziale fase di progettazione del trattamento e di protezione dei dati per impostazione predefinita (art. 25 GDPR).

Ancora, il Regolamento europeo ha introdotto, tra gli strumenti da applicare per una corretta gestione del rischio, anche una nuova e generale logica per cui il *risk assessment*, quindi la valutazione del rischio, diviene parte integrante e fondamentale della disciplina del trattamento dei dati, chiaramente improntata alle tecniche del *risk management*, applicato nel contesto della *data protection*: a differenza delle precedenti normative, adesso il *risk assessment* viene richiesto in modo esplicito dalla normativa europea, che introduce chiaramente un'attenzione precisa alla gestione del rischio per la messa in sicurezza dei dati personali, con particolare riguardo ai trattamenti esposti a rischi specifici (art. 35 GDPR).

2.2. La sicurezza del trattamento e le sue declinazioni (riservatezza, integrità, disponibilità)

Il concetto di sicurezza del trattamento, soprattutto con riferimento alla sicurezza informatica, viene analizzato partendo dai tre elementi di base sui quali lo stesso può essere declinato e cioè le tre caratteristiche fondamentali di cui si compone la sicurezza medesima ossia la *riservatezza*, l'*integrità* e la *disponibilità* delle informazioni[33], conosciute anche come «*CIA Triad*», dall'acronimo ricavato dalla corrispondente terminologia inglese (*confidentiality*, *integrity*, *availability*)[34]. Si tratta dunque di concetti fondamentali, tanto che anche la metodologia ENISA in

e d.lgs. 10 agosto 2018, n. 101, cit., pp. 17 ss.; C. BISTOLFI, *Adozione obbligatoria di strumenti per la sicurezza del trattamento: adozione di specifici strumenti*, in L. BOLOGNINI-E. PELINO-C. BISTOLFI, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, pp. 400 ss.

[33] Si veda, al riguardo, P. PERRI, *Protezione dei dati e nuove tecnologie. Aspetti nazionali, europei e statunitensi*, cit., p. 108, che si riferisce alla *riservatezza*, all'*integrità* e alla *disponibilità* quali «componenti essenziali idonee a costruire una moderna nozione di sicurezza applicata alle tecnologie dell'informazione».

[34] S. BROOKS-E. NADEAU, *Privacy Risk Management for Federal Information Systems, Information Technology Laboratory – NIST*, Gaithersburg, 2015; A. BOURKA-P. DROGKARIS, *Security meets data*

materia di valutazione preventiva del rischio connesso al trattamento li indica precisamente come fattori chiave per la valutazione di impatto (*Data Protection Impact Assessment*, DPIA), che vedremo più avanti[35].

La sicurezza è quindi da intendere in maniera strumentale alla protezione dei dati personali, innanzitutto per le esigenze di tutela dei diritti e delle libertà fondamentali dell'interessato[36], ma anche per assicurare il raggiungimento delle finalità del trattamento decise dal *data controller*[37].

Esaminando allora, brevemente, le sue componenti nel dettaglio, va rimarcato che la «*riservatezza*», così intesa, «si ottiene impedendo che le informazioni siano rivelate senza autorizzazione»[38] ed impone di non rendere accessibili o conoscibili i dati a chiunque non svolga, o possa svolgere, legittimamente su quegli stessi dati operazioni di trattamento. Anche i soggetti individuati dal titolare e/o dal responsabile quali soggetti che possono trattare dati personali per loro conto, dovranno essere comunque tenuti all'obbligo di riservatezza. Diventano inoltre fondamentali,

---

protection: from risk management to systems engineering, in *15 years of ENISA: A Success story*, Publications Office of the European Union, 2019, pp. 125-135.

[35] ENISA, *Online platform for security of personal data processing. Reinforcing trust and security in the area of electronic communications and online services*, dicembre 2019, p. 6 e pp. 9 ss., documento disponibile sul sito istituzionale dell'ENISA all'indirizzo https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform (consultato da ultimo in data 5 aprile 2023).

[36] La connessione tra sicurezza e tutela del diritto alla protezione dei dati personali, come diritto fondamentale, è costantemente riconosciuta in dottrina, anche al cospetto della legislazione previgente. Si rinvia, ad es., a D. Liantonio, *La legge sulla privacy e la sicurezza dei dati*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, vol. I, pp. 751 ss.; R. Motroni, *La sicurezza dei dati e dei sistemi*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, pp. 221 ss. In maniera più specifica, con riguardo al GDPR, si veda, invece, A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 1, pp. 144 ss. e, *ivi*, spec. p. 155 ss., in cui viene evidenziato un ampliamento della nozione di rischio accolta nel GDPR rispetto all'impianto normativo precedente, più circoscritto ai soli profili inerenti alla protezione dei dati e alla riservatezza dell'interessato, che invece viene ora estesa, nel GDPR, ad ulteriori diritti e libertà fondamentali, sicché la sicurezza nella disciplina *de qua* finisce per essere funzionale ad essi. Sul punto, si veda anche M.S. Esposito, *Sicurezza dei dati personali (comm. art. 32 GDPR)*, in R. D'Orazio-G. Finocchiaro-O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Milano 2021, p. 507. Nella medesima direzione s'è affermato che la sicurezza costituisce «il fondamento del rispetto dei diritti e delle libertà degli interessati», suffragando tale affermazione con quanto previsto dal *considerando* n. 83 del GDPR, che «parla di valutazione dei rischi per la sicurezza "che potrebbero cagionare in particolare un danno fisico, materiale o morale" all'interessato» (L. Bolognini, *Principi del trattamento*, in L. Bolognini-E. Pelino-C. Bistolfi, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, cit., pp. 114-115).

[37] In questo senso esplicito è F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 799, secondo cui la sicurezza va letta «in funzione di esigenze plurime, non solo a tutela del diritto alla protezione dei dati personali, considerando che obiettivo delle misure tecniche e organizzative in materia di protezione dei dati personali è anche quello di realizzare le finalità del trattamento stabilite dal titolare e dichiarate nell'informativa da rendere agli interessati. Sicché, le misure di sicurezza, oltre a proteggere i dati personali dell'interessato e le connesse situazioni giuridiche soggettive, assolvono contestualmente anche all'ulteriore funzione di garantire il corretto raggiungimento delle finalità del trattamento volute dal titolare o che il titolare è tenuto a raggiungere nello svolgimento di funzioni pubbliche o di compiti di pubblico interesse».

[38] P. Perri, *op. ult. cit*., p. 108.

a questo proposito, le istruzioni impartite dal titolare e dal responsabile del trattamento a coloro che, su incarico di quest'ultimi, pongono in essere le operazioni di trattamento (art. 29 GDPR).

Quanto all'«*integrità*», in dottrina è stato efficacemente rimarcato «che si ottiene impedendo che le informazioni siano modificate senza autorizzazione»[39], ovvero salvaguardate da azioni, volontarie o involontarie, che possano comportare, in tutto o in parte, la distruzione, la perdita o l'alterazione dei dati personali oggetto di trattamento. Ha trovato esplicitazione, oltre che nel GDPR, anche nella normativa previgente, se si pensa che nell'art. 11 del Codice *privacy*, rubricato «*Modalità del trattamento e requisiti dei dati*», poi abrogato, si indicava che «I dati personali oggetto di trattamento sono: (…) *c)* esatti e, se necessario, aggiornati; *d)* pertinenti, completi (…)»[40].

Nel settore delle comunicazioni elettroniche il Garante si era già espresso sul principio di integrità, con particolare riguardo al rispetto delle caratteristiche di accuratezza, completezza e affidabilità dei dati nel corso dell'intero loro ciclo di vita. Nel provvedimento sulla «Sicurezza dei dati di traffico telefonico e telematico», reso dall'*Authority* il 17 gennaio 2008, in riferimento alla conservazione separata dei dati di traffico per esclusive finalità di accertamento e repressione dei reati (ad oggi avente termini di 6 anni, come definito nell'art. 24 della l. 20 novembre 2017, n. 167, c.d. "Legge europea 2017", in tema di *data retention*)[41] erano stati espressamente indicati gli accorgimenti e le misure prescritte a tal fine, tra i quali figurano, al punto 7.6 (intitolato «*Altre misure*»)[42], gli *audit log*, nei cui confronti era già sancito, quale garan-

---

[39] P. PERRI, *op. ult. cit*., p. 108.

[40] Più precisamente, l'intero art. 11 del Codice *privacy* prevedeva che «1. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati».

[41] L'art. 24 della l. n. 167/2017, rubricato «*Termini di conservazione dei dati di traffico telefonico e telematico*», ha stabilito che «In attuazione dell›articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera *a)*, del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-*bis*, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-*bis*, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196».

[42] Nel punto n. 7.6 cit., rubricato «*Altre misure*», con riguardo agli *audit log* si prevede che «Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati

zia di corretta conservazione, l'immodificabilità delle registrazioni, esplicitandone anche la necessaria implementazione attraverso idonee procedure informatiche che potessero garantire l'integrità e, dunque, inalterabilità dei dati. Il requisito di integrità nella conservazione dei dati risulta inoltre già presente, sempre con riferimento alla registrazione degli accessi, nel provvedimento del Garante dedicato alle «Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema» del 27 novembre 2008 (così modificato in base al provvedimento del 25 giugno 2009)[43].

Infine, per quanto concerne il requisito di «*disponibilità*» del dato, deve essere garantito l'accesso e l'usabilità del medesimo, «impedendo che l'accesso alle informazioni o alle risorse sia negato senza autorizzazione»[44] al soggetto legittimato a porre in essere operazioni di trattamento.

---

di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di *audit log* devono garantire la completezza, l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi devono essere adottati, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter,* sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.

Le misure di cui al presente paragrafo sono adottate nel rispetto dei princìpi in materia di controllo dei lavoratori sull'uso di strumenti elettronici, con particolare riguardo all'informativa agli interessati (cfr. Provv. 1° marzo 2007, doc. *web* n. 1387522)».

[43] Al punto 2, lett. *f)*, e al punto 4.5 del citato provvedimento del Garante sugli amministratori di sistema è specificato che per gli *access log* relativi alle attività degli amministratori di sistema deve essere possibile verificarne l'integrità. Il provvedimento in questione pone un'attenzione specifica sulla necessità di individuare una figura che possa contribuire fortemente a garantire l'integrità dei dati, anche nel senso della completezza e dell'inalterabilità degli stessi. In maniera più dettagliata, nelle FAQ nn. 4, 12 e 13, rese a corredo del provvedimento sugli amministratori di sistema, si trovano le indicazioni sull'implementazione di tale requisito. Viene infatti indicato che per le postazioni *client* la registrazione dei dati di accesso può avvenire a livello locale (forse da leggere "deve avvenire"), sempre con sufficienti garanzie di integrità, secondo le valutazioni del titolare, mediante l'utilizzo di strumenti più sofisticati quali dispositivi non riscrivibili o tecniche crittografiche per la verifica dell'integrità delle registrazioni. Il discorso sulle modalità per garantire l'inalterabilità dei *log*, ovvero il mantenimento dell'integrità dei dati raccolti, non viene tuttavia affrontato in maniera dettagliata sotto gli aspetti tecnici; piuttosto viene posto l'accento sui termini di raccolta e conservazione, lasciando ogni valutazione specifica al titolare, in base al contesto operativo.

[44] P. Perri, *op. ult. cit.*, p. 108.

2.3. Le misure di sicurezza tecniche e organizzative ai sensi dell'art. 32 GDPR e le istruzioni ai sensi dell'art. 29 GDPR

Quello relativo alla sicurezza è un tema complesso che, come affermato da autorevole dottrina[45], riguarda l'intero flusso informativo ed abbraccia, mettendole in stretta correlazione, più aree di competenza, inclusa l'informatica, giuridica e organizzativa[46].

Il Codice in materia di protezione dei dati personali, prima dell'intervento di riforma del 2018 dovuto all'esigenza di coordinamento con il GDPR, prevedeva sia l'obbligo di adozione delle misure minime di sicurezza, all'art. 33, la cui violazione comportava responsabilità anche di natura penale, sia l'obbligo di adozione di misure adeguate ai livelli di rischio incombenti sul trattamento, all'art. 31.

Con l'entrata in vigore del GDPR cambia radicalmente l'approccio all'adozione delle misure di sicurezza tecniche ed organizzative: viene abbandonata la previsione di misure «minime» (prima esplicitate nell'allegato B del Codice *privacy*), utilizzate troppo spesso nella prassi quale livello standard a cui uniformare la sicurezza del trattamento, insistendo solamente sulle misure adeguate al rischio, la cui determinazione è rimessa al titolare – anche sulla scorta del principio di *accountability* – ed al responsabile del trattamento, secondo valutazioni rigorose, che attingono all'analisi dei rischi con tecniche di *risk management*.

In dottrina è stato posto l'accento sulla regola di «appropriatezza del livello di sicurezza rispetto ai rischi presentati dal trattamento»[47]. Anche in questo caso occorre che l'intervento tecnico-organizzativo sia commisurato alla situazione concreta, secondo parametri che fanno riferimento all'evoluzione tecnologica del tempo (il c.d. "stato dell'arte") ed ai relativi costi di attuazione, tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento a cui si applicano le misure di sicurezza. Il menzionato criterio della misurazione dei costi di attuazione delle misure, invero, apre la porta a scenari connotati da incertezze e criticità, in quanto potrebbe apparire strettamente connesso alla tipologia di *business* in cui il tratta-

---

[45] G. FINOCCHIARO, Privacy *e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 249-253.

[46] Sulla necessità di un approccio multidisciplinare agli obblighi in materia di sicurezza previsti dal GDPR, si veda, segnatamente, G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., p. 18. Si veda anche L. BOLOGNINI, *Principi del trattamento*, cit., p. 113.

[47] G.G. CODIGLIONE, Risk-based approach *e trattamento dei dati personali*, in S. SICA-V. D'ANTONIO-G.M. RICCIO (a cura di), *La nuova disciplina europea della* privacy, Milano, 2016, pp. 67 s., il quale precisa altresì che l'art. 32 cit., al par. 1, «indica un modello di condotta ed organizzazione adeguato a garantire gli obiettivi di sicurezza, basato sulla "spersonalizzazione" dei dati attraverso procedura di pseudonimizzazione e cifratura e, ancora, sulla garanzia di riservatezza, integrità, disponibilità e resilienza dei servizi di trattamento, sulla loro capacità di ripristino a seguito di incidente fisico o tecnico e infine rimesso all'attuazione periodica di procedure di *testing*, verifica e valutazione dell'efficacia complessiva delle misure». L'A. cit. ricorda poi che l'art. 32, in chiusura, contiene altresì «un incentivo all'adozione di codici di condotta o meccanismi di certificazione approvati, intesi come elementi validi per dimostrare l'adeguatezza delle misure» e, sia per il titolare che per il responsabile, «un obbligo generale di rendere edotto sulle regole di sicurezza qualunque soggetto che, operando sotto la propria autorità, abbia accesso ai dati personali trattati».

mento viene posto in essere, alla remuneratività dell'attività svolta, spesso frutto di un affidamento in *outsourcing*, nonché alla disponibilità economica del titolare del trattamento o del responsabile del trattamento ad affrontare lo sforzo economico connesso all'adozione delle misure di sicurezza. Ove però fossero questi i parametri di valutazione del criterio di adeguatezza delle misure tecniche ed organizzative da selezionare in vista della loro adozione, si finirebbe per avere un sostanziale svuotamento dei livelli di garanzia che, al contrario, il GDPR mostra di individuare con un approccio più rigoroso. L'interpretazione dell'art. 32 GDPR, sul punto, non può che essere decisamente restrittiva[48].

2.4. La sicurezza del trattamento sin dalla progettazione e per impostazione predefinita

L'adozione di idonee ed adeguate misure tecniche ed organizzative necessarie per la tutela dei dati personali riflette, inoltre, un altro corollario del citato principio di sicurezza: quello introdotto dall'art. 25 GDPR che, in particolare, enuncia l'altrettanto innovativo approccio concettuale alla sicurezza attraverso l'obbligo di adozione di misure tecniche e organizzative (ulteriori rispetto a quelle di cui all'art. 32 GDPR), improntate a realizzare la c.d. *privacy by design* e *privacy by default*[49]. Qui si impone ai titolari del trattamento l'obbligo di prevedere in fase progettuale (fin dall'iniziale fase di ideazione) tutti i più idonei e necessari strumenti e le conseguenti corrette impostazioni atte a garantire un'appropriata tutela dei dati personali.

Sul rapporto tra sicurezza e "architettura" del trattamento, la dottrina si è espressa evidenziando, altresì, l'abbandono dell'approccio "difensivo", da parte del legislatore, verso gli strumenti tecnologici di trattamento, non più visti solamente come fonti di minacce per i diritti e le libertà dell'interessato: si percorrono ora nuove strade, a favore di un approccio volto a coltivare l'uso della tecnologia anche a

[48] Al riguardo, risulta opportuno richiamare le indicazioni fornite dall'EDPB nel diverso contesto della *privacy by design* e *by default*, rispetto al quale il GDPR si riferisce allo "stato dell'arte" e ai "costi di attuazione" con formulazione analoga a quella ivi in esame (art. 25, par. 1, GDPR). L'EDPB ha indicato che «il costo di attuazione rappresenta un fattore di cui tenere conto nel realizzare la protezione dei dati fin dalla progettazione, e non già un motivo per astenersi dal realizzarla» e che «[l] e misure individuate devono pertanto garantire che l'attività di trattamento prevista dal titolare non comporti trattamenti di dati personali in violazione dei principi, indipendentemente dal costo di tali misure. I titolari devono essere in grado di gestire i costi complessivi per poter attuare efficacemente tutti i principi e, di conseguenza, tutelare i diritti» (EDPB, *Linee guida 4/2019 sull'articolo 25. Protezione dei dati fin dalla progettazione e per impostazione predefinita*, v. 2.0, 20 ottobre 2020, p. 9). Si evidenzia inoltre che, relativamente alla normativa previgente e, segnatamente, al riferimento ai «costi dell'applicazione» come criterio al quale il titolare del trattamento doveva attenersi per l'adozione delle misure di sicurezza (art. 17, Direttiva 95/46/CE), autorevole dottrina sottolineò che «il titolare non può addurre la gravosità del costo delle misure per giustificare la loro mancata adozione» (G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 332).

[49] Sul rapporto tra sicurezza del trattamento e obblighi in materia di *privacy by design* e *by default*, si veda ad es. L. Greco, *L'organigramma privacy: i soggetti del trattamento*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 324 ss., nonché F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 789 ss.

supporto delle esigenze di tutela degli interessati, facendo in modo che la tecnologia, se ben congegnata in fase di progettazione, possa rafforzare la protezione delle persone fisiche a cui i dati si riferiscono (si pensi, ad esempio, alle *Privacy Enhancing Technologies*, PET)[50].

2.5. La sicurezza del trattamento in caso di violazione dei dati (*data breach*)

Il principio di sicurezza del trattamento ha un ruolo centrale anche con riguardo alla disciplina relativa al *data breach*, di cui agli artt. 33 e 34 GDPR.

Preliminarmente va tenuto presente che una sicura conservazione dei dati è alla base della minimizzazione dei rischi causata da una violazione, mediante misure tecniche ed organizzative quali la cifratura o la pseudonimizzazione. La cifratura del dato permette di tenerlo al sicuro dai rischi connessi ad accessi non autorizzati (perché senza una chiave per decrittografare, il dato risulta illeggibile), mentre la pseudonimizzazione dei dati, che richiede specifiche misure tecniche e organizzative volte a rendere gli interessati non (immediatamente) identificabili[51], consente di minimizzare l'impatto sugli interessati nel caso in cui vengano appresi i loro dati personali[52].

In materia di *data breach* il principio di sicurezza impone di adottare non solo misure di carattere preventivo, ma anche quelle volte a gestire e fronteggiare la violazione in atto, quando la minaccia considerata nel rischio viene a realizzarsi, e a mitigare le conseguenze pregiudizievoli che vengono a concretizzarsi per i diritti e le libertà dell'interessato[53].

È in quest'ottica che possono leggersi anche gli obblighi – di notifica al Garante, di comunicazione agli interessati e di documentazione delle violazioni – imposti al titolare del trattamento dagli artt. 33 e 34 GDPR[54].

---

[50] F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 789 ss. e, ivi, spec. pp. 814 ss.

[51] Ai sensi dell'art. 4, par. 1, n. 5, GDPR, la pseudonimizzazione è definita come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile».

[52] Interessante è il contributo di D'Orazio riguardo alla "riservatezza" garantita attraverso misure di "oscuramento" dei dati, come la citata pseudonimizzazione, piuttosto che il renderli anonimi (R. D'ORAZIO, *Protezione dei dati* by default *e* by design, cit., pp. 79 ss.). Se ne deduce che non è sempre dovuta l'anonimizzazione (che di fatto comporta l'impossibilità assoluta di risalire all'identità dell'interessato) potendosi ricorrere a tecniche di pseudonimizzazione che consentono il trattamento dei dati personali per le finalità per cui è posto, rendendo invece impossibile risalire all'identità dell'interessato solamente per chi non è legittimato a trattare dati identificativi. Questa tecnica agevola quindi l'implementazione di più livelli di accesso, in aderenza anche al principio di minimizzazione, che opera congiuntamente con il principio di sicurezza dei dati, ed al contempo rende più robusta la base di dati rispetto ad eventuali *data breach*. Anche sotto questo aspetto, afferma D'Orazio nel contributo citato, il GDPR richiama ad uno stretto legame tra l'innovazione tecnologica e la tutela dei dati personali.

[53] Sugli adempimenti imposti in caso di verificazione di un *data breach* quali obblighi di adozione di misure di sicurezza *ex post*, si veda ad es. F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, cit., pp. 279 ss.

[54] Sul punto si veda S. VIGLIAR, Data breach *e sicurezza informatica*, in S. SICA-V. D'ANTONIO-G.M. RICCIO (a cura di), *La nuova disciplina europea della* privacy, cit., pp. 240 ss. e, ivi, spec. pp. 252 ss.

Si consideri infatti – a mero titolo esemplificativo – che, nella notifica al Garante, il titolare deve indicare espressamente, tra l'altro, quali misure di sicurezza siano state adottate e quali siano state proposte per porre rimedio alla violazione dei dati personali e per mitigarne o temperarne gli effetti pregiudizievoli per l'interessato, consentendo così al Garante, ove ne ravvisi la necessità, di intervenire controllando l'idoneità dell'intervento di reazione al *data breach* e, se del caso, prescrivendo ulteriori misure. Anche la documentazione delle violazioni è misura che si inserisce nella logica del principio di sicurezza, perché, oltre a consentire una verifica da parte dell'Autorità, consente al titolare di tenere traccia dello storico delle violazioni, per analizzare le vulnerabilità del proprio sistema di gestione dei trattamenti, al fine di incrementare i livelli di sicurezza.

2.6. La sicurezza nei trattamenti che presentano rischi elevati (DPIA)

Un'ulteriore articolazione del principio di sicurezza (ovvero, di «integrità e riservatezza») si riscontra quando l'analisi propedeutica all'individuazione delle misure preventive di sicurezza *ex* art. 32 GDPR fa emergere la presenza di un possibile rischio elevato per i diritti e le libertà dell'interessato, in particolare in un trattamento in cui si faccia uso di «nuove tecnologie»: in questo caso il titolare, prima di procedere al trattamento, deve attivarsi per effettuare un'ulteriore e preventiva «valutazione dell'impatto sulla protezione dei dati» (la c.d. *Data Protection Impact Assessment*, DPIA) secondo quanto previsto e specificamente predisposto all'art. 35 del GDPR.

Al riguardo, il Garante ha pubblicato un elenco della tipologia di trattamenti per cui la DPIA risulterebbe obbligatoria[55].

L'impatto da analizzare rimane pur sempre quello sui diritti e le libertà dell'interessato, secondo l'approccio tipico del Regolamento europeo in tale materia. Su tale aspetto è stato rilevato «come, ad oggi, manchi ancora una consolidata elaborazione in tema di analisi dei rischi concernenti l'impatto sulle libertà ed i diritti, impatto che risulta essere ben difficile da misurare di quello tradizionalmente considerato, inerente alla sicurezza dei dati. Mentre, infatti, in quest'ultimo caso i parametri di probabilità e di entità del rischio possono risultare agevolmente prevedibili, ben più complesso è valutare l'incidenza potenziale su "i diritti e le libertà delle persone fisiche", stante l'ampiezza della categoria in questione e la mancanza di indici misurabili. A ciò si aggiunga la presenza di elementi di vaghezza nel dettato normativo, quali ad esempio il riferimento alle "nuove tecnologie", categoria a-tecnica e potenzialmente assai estesa e variabile»[56].

---

[55] GPDP, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento UE n. 2016/679*, Allegato n. 1 al Provv. 11 ottobre 2018, doc. *web* n. 9058979.

[56] Così A. Mantelero, *La gestione del rischio*, cit., pp. 496 s. Per un'analisi della disciplina in materia di valutazione di impatto si veda anche: R. Torino, *La valutazione d'impatto (Data Protection Impact Assessment)*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit. pp. 855 ss.; F. Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, cit., pp. 285 ss.; L. Bolognini, *Adozione obbligatoria di strumenti per la sicurezza del trattamento: le attività preparatorie*, cit., pp. 378 ss.

Nella disciplina sulla valutazione di impatto il principio di sicurezza viene attuato facendo leva su uno strumento di analisi complesso, i cui contenuti sono stabiliti dall'art. 35, par. 7, GDPR: non si richiede solamente di effettuare un'analisi dei rischi e di predisporre le relative misure di sicurezza, ma, prima ancora, si impone di parametrare l'analisi sia alle finalità ed alle caratteristiche del trattamento, sia alla «valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità», secondo quanto previsto dall'art. 35, par. 7, lett. *a)* e *b)*, GDPR[57].

L'attuazione del principio di sicurezza, in particolare là dove il trattamento presenta rischi elevati, passa dunque per un'analisi complessa che richiede la concorrente applicazione dei principi di necessità e di proporzionalità, in grado di ridurre a monte l'esposizione al rischio a cui sono sottoposti i dati, prima ancora di intervenire con la previsione di misure di sicurezza per fronteggiare la probabilità e la gravità delle minacce[58].

Ove la valutazione effettuata dal titolare, con il coinvolgimento del *Data Protection Officer*, se designato, faccia emergere un rischio residuo elevato, si rende obbligatorio il coinvolgimento della competente autorità di controllo, a cui il titolare deve rivolgersi richiedendo la c.d. «valutazione preventiva» di cui all'art. 36 GDPR.

3. Applicazione del principio nella casistica

La prassi applicativa del Garante per la protezione dei dati personali dimostra una rilevante attenzione per il rispetto del principio di "integrità e riservatezza" (ovvero di "sicurezza"). Nel seguito, senza pretese di esaustività, si evidenzieranno alcuni passaggi dei provvedimenti del Garante che, a giudizio di chi scrive, meglio consentono di comprendere il significato di tale principio e le modalità con cui l'Autorità ne ha fatto applicazione.

Il carattere innovativo del principio di "integrità e riservatezza" e dei correlati obblighi di sicurezza previsti dal GDPR emerge con chiarezza dalle considerazioni svolte dal Garante nel parere del 24 febbraio 2022 sullo schema di «*Linee guida di* design *per i siti internet e i servizi digitali della PA*», predisposto dall'AgID[59].

Lo schema di queste linee guida prevedeva la necessità di assicurare «almeno il livello base di sicurezza stabilito dalle "Misure minime di sicurezza ICT per le pubbliche amministrazioni", ove non sia specificamente richiesto un livello superio-

[57] Per la valutazione del rischio l'ENISA ha fornito un valido strumento (ENISA, *Securing Personal Data: a risk-based approach*, su cui si veda il documento consultabile all'url https://www.enisa.europa.eu/news/enisa-news/securing-personal-data-a-risky-business alla cui stesura ha partecipato anche il Garante). La metodologia dell'ENISA è definita nelle sue «*Guidelines for SMEs on the security of personal data processing*» (2016) e nel «*Manuale sulla Sicurezza nel trattamento dei dati personali*» (2017).

[58] Sul punto, si veda A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, cit., pp. 310-311.

[59] GPDP, Provv. 24 febbraio 2022, doc. *web* n. 9753209. Nel medesimo senso, si v. anche GPDP, Provv. 30 gennaio 2020, doc. *web* n. 9283857; Provv. 13 febbraio 2020, doc. *web* n. 9283921 e Provv. 29 ottobre 2020, doc. *web* n. 9487928.

re dal citato documento»[60]. Il Garante ha statuito che il rinvio a tali "misure minime", contenute nella circolare AgID n. 2/2017, non sia sufficiente «ad assicurare l'adozione di misure di sicurezza del trattamento "adeguate", in conformità al Regolamento, a norma del quale, occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati»[61]. Per questa ragione, l'adozione di tali misure minime «non è di per sé idonea a soddisfare in tutti i casi i requisiti previsti dagli artt. 5, par. 1, lett. *f)*, e 32 del Regolamento»[62], in quanto «una valutazione in tal senso deve essere effettuata, in maniera puntuale, dai titolari del trattamento»[63].

Il Garante mostra così di accogliere il concetto di sicurezza «dinamico e relazionale»[64] previsto dal Reg. UE n. 679/2016, il quale, secondo l'approccio basato sul rischio che informa l'intero regolamento, impedisce soluzioni di sicurezza di tipo "statico", sciolte cioè dalle caratteristiche del trattamento nel caso concreto e dal rischio posto dal medesimo per i diritti e le libertà degli interessati[65].

Questo parere, inoltre, evidenzia un aspetto che, come si vedrà, risulta comune alla quasi totalità dei provvedimenti adottati dal Garante in riferimento al principio in esame: l'accertamento circa la conformità del trattamento all'art. 5, par. 1, lett. *f)*, GDPR è normalmente accompagnato dalla contestuale considerazione dell'art. 32 GDPR, il quale, con ogni evidenza, reca le prescrizioni che ne costituiscono la principale specificazione. Il rispetto del principio di sicurezza, in tal senso, non appare conseguibile senza l'idonea implementazione del complesso di misure tecniche e organizzative previste dal predetto art. 32 GDPR. L'applicazione del principio è poi sovente accompagnata anche da riferimenti alla valutazione di impatto e alla relativa analisi dei rischi, ove richiesta ai sensi dell'art. 35 GDPR.

Il rilievo dei processi di gestione del rischio rispetto al principio di sicurezza emerge anche nel provvedimento adottato nei confronti dell'Azienda USL Toscana Sud Est in data 17 dicembre 2020, relativo ai trattamenti svolti nell'ambito della c.d. sanità di iniziativa[66].

Per realizzare questo modello assistenziale, detta Azienda aveva previsto un'articolata procedura che i medici di medicina generale dovevano seguire per trasmettere alla stessa le informazioni sui pazienti arruolati (nella specie: salvataggio da parte dei MMG di un *file* su *pen drive* di loro proprietà; consegna di tale supporto al medico di distretto; salvataggio del *file* sul pc di quest'ultimo e invio dello stesso

[60] GPDP, Provv. 24 febbraio 2022, cit. Il documento recante le suddette «*Misure minime di sicurezza ICT per le pubbliche amministrazioni*» è costituito dalla Circolare AgID del 18 aprile 2017, n. 2.

[61] GPDP, Provv. 24 febbraio 2022, cit.

[62] *Ibidem*.

[63] *Ibidem*.

[64] Cfr. G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., p. 18.

[65] Non a caso, le norme in materia di misure minime di sicurezza contenute nel d.lgs. n. 196/2003 erano già state abrogate a opera del d.lgs. n. 101/2018, in sede di adeguamento dell'ordinamento interno al GDPR (sul punto, si veda quanto indicato nei paragrafi precedenti).

[66] GPDP, Provv. 17 dicembre 2020, doc. *web* n. 9529527.

via *e-mail* al medico referente per area provinciale; successivo invio via *e-mail* dei *file* ricevuti da tutti i medici di distretto alla società incaricata quale responsabile del trattamento). Al riguardo, l'Autorità ha ritenuto che l'Azienda non avesse posto in essere «misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio»[67]; le anzidette modalità di trattamento «non rispondono, infatti, ai principi e criteri di sicurezza descritti dagli artt. 5, par. 2, lett. *f)* e 32 del Regolamento» e «mettono in luce l'assenza di una *valutazione dei rischi* del trattamento che si sarebbe dovuta effettuare nell'ambito della *valutazione di impatto* che invece non risulta essere stata effettuata»[68].

Il rispetto del principio di integrità e riservatezza impone pertanto l'adozione di misure proporzionate al rischio, in quanto tali da individuarsi previa valutazione dei rischi. Ivi, in particolare, visti i rischi elevati posti dal trattamento, il *risk assessment* avrebbe dovuto essere condotto nel contesto di una valutazione d'impatto[69], ritenuta obbligatoria dall'Autorità a fronte della natura dei dati trattati (di tipo sanitario) e della numerosità degli interessati coinvolti.

Il Garante, inoltre, innanzi alla mancata adozione del registro delle attività di trattamento (art. 30 GDPR), ha precisato come la tenuta di tale documento costituisca «un elemento essenziale per il governo dei trattamenti e per l'efficace individuazione di quelli a maggior rischio»[70], così evidenziando come detto adempimento abbia una specifica funzione nel complessivo processo di *risk management* necessario, tra l'altro, per garantire il livello di sicurezza previsto dal principio di integrità e riservatezza[71].

Questione di interesse è quella degli effetti derivanti dall'introduzione, a opera del GDPR, del principio di integrità e riservatezza rispetto agli obblighi di sicurezza previsti in provvedimenti approvati nel contesto della normativa previgente. Al riguardo, si richiama il provvedimento adottato il 26 maggio 2022 nei confronti dell'Azienda sanitaria universitaria Friuli Centrale, inerente al c.d. *dossier* sanitario[72].

Il caso è scaturito della notifica di due *data breach*, cagionati da accessi non autorizzati ai *dossier* sanitari di taluni pazienti da parte del personale sanitario. L'Ufficio del Garante ha rilevato come la configurazione del sistema di gestione del *dossier* sanitario stabilita dal titolare individuava un profilo di accesso unico, così consentendo a tutto il personale sanitario di accedere, peraltro senza limitazioni temporali, ai *dossier* di qualsiasi paziente presente in Azienda, a prescindere dalla

---

67 *Ibidem*.

68 *Ibidem*.

69 Sul rapporto tra il principio in esame e la valutazione d'impatto, si veda *supra*, par. 2.6.

70 *Ibidem*.

71 Il tema è stato successivamente ripreso in GPDP, Provv. 7 aprile 2022, doc. *web* n. 9768363, descritto *infra*, dal quale emerge che il registro ha carattere strumentale rispetto alla valutazione del rischio, nel più ampio contesto del principio di responsabilizzazione. Il Garante ha infatti indicato che «[l] a tenuta del registro (…) è funzionale al rispetto del principio di "responsabilizzazione" del titolare (art. 5, par. 2, del Regolamento), in quanto costituisce uno strumento idoneo a fornire un quadro aggiornato dei trattamenti (…). Ciò risulta particolarmente rilevante con riguardo alle attività di valutazione e di analisi del rischio, costituendo, pertanto, un adempimento preliminare rispetto a tali attività».

72 GPDP, Provv. 26 maggio 2022, doc. *web* n. 9790365.

circostanza che lo stesso fosse in cura presso la persona che effettuava l'accesso. Detta configurazione, inoltre, permetteva a tutto il personale di effettuare, attraverso il *dossier*, le medesime attività di trattamento.

Il Garante ha affrontato il caso richiamando le misure in materia di sicurezza previste dalle «*Linee guida in materia di* Dossier *sanitario*» adottate nel contesto della normativa previgente[73], ritenendo queste ultime compatibili con il GDPR ai sensi dell'art. 22, co. 4, d.lgs. n. 101/2018[74]. Dette linee guida impongono specifiche prescrizioni sull'adozione di sistemi di autenticazione e autorizzazione del personale avente necessità di accesso ai *dossier* sanitari, la cui violazione, nel caso in esame, a giudizio del Garante aveva causato i suddetti *data breach*. La mancata implementazione di tali misure, per questa ragione, è stata giudicata in contrasto con il principio di integrità e riservatezza, nonché con altre norme rilevanti nel caso scrutinato[75].

Ne emerge che le puntuali prescrizioni in materia di sicurezza contenute nei provvedimenti adottati anteriormente all'applicazione del GDPR, laddove compatibili con quest'ultimo, possono ritenersi quali specificazioni, in contesti circoscritti, del principio di integrità e riservatezza[76]. Di conseguenza, la mancata aderenza a queste prescrizioni di fonte amministrativistica rende applicabili le sanzioni amministrative pecuniarie di maggiore gravità previste dall'art. 83, par. 5, lett. *a)*, GDPR per la violazione dei «principi di base del trattamento», come avvenuto nel caso in esame.

Proseguendo oltre, il provvedimento in considerazione appare rilevante anche per apprezzare il rilievo della cifratura, quale misura di sicurezza espressamente

---

[73] GPDP, Provv. 4 giugno 2015, doc. *web* n. 4084632.

[74] L'art. 22, co. 4, d.lgs. n. 101/2018 dispone che «[a] decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto».

[75] Il titolare aveva sostenuto, a sua difesa, che non fosse possibile fissare in anticipo regole temporali sull'accessibilità ai dati per finalità di cura, in ragione del fatto che «il processo di cura del paziente può essere caratterizzato dalla prestazione di servizi molto diversi, resi in tempi e luoghi diversi e da professionisti appartenenti a diverse discipline» (GPDP, Provv. 26 maggio 2022, cit.). Il Garante, tuttavia, ha giudicato dette circostanze insufficienti «per derogare alla necessaria individuazione temporale del periodo di validità del profilo di accesso al *dossier*, atteso che quanto riferito non appare essere una condizione che esima il titolare dall'applicazione dei principi generali del trattamento o una caratteristica unica di codesta Azienda» (*Ibidem*).

[76] Sempre sul rilievo delle prescrizioni delle linee guida in materia di *dossier* sanitario rispetto al principio di sicurezza, si consideri anche che, nel caso in esame, l'Autorità ha rilevato come il *dossier* sanitario, nonostante quanto stabilito dalle citate linee guida in merito ai sistemi di *audit log,* non prevedesse «un sistema per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, ovvero l'utilizzo di indicatori di anomalie (c.d. *alert*) volti ad individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dai soggetti autorizzati al trattamento (es. numero degli accessi eseguiti, tipologia o ambito temporale degli stessi), utili per orientare successivi interventi di *audit* in violazione dei principi di integrità e riservatezza dei dati personali (artt. 5, par. 1, lett. *f),* e 32 GDPR)» (in senso conforme, v. altresì GPDP, Provv. 10 novembre 2022, doc. *web* n. 9819792). Sul tema, si v. anche GPDP, Provv. 11 marzo 2021, doc. *web* n. 9583597, nel quale il Garante ha ritenuto violati gli artt. 5, par. 1, lett. *f),* e 32 GDPR in relazione al mancato rispetto degli specifici termini di conservazione dei *file* di *log* previsti nelle anzidette linee guida per la tracciabilità degli accessi e delle operazioni effettuate.

prevista dall'art. 32, par. 1, GDPR, rispetto all'obiettivo di garantire la sicurezza "adeguata" cui tende il principio di integrità e riservatezza[77].

Nel caso esaminato, l'Azienda utilizzava per i trattamenti relativi ai *dossier* sanitari il protocollo di rete "*http*" (*hypertext transfer protocol*). A giudizio del Garante, detto protocollo «oltre a non garantire la riservatezza e l'integrità dei dati scambiati tra il *browser* dell'utente e il *server* che ospita l'applicazione, non consente agli utenti di verificare l'autenticità del *server* con cui colloquiano. Tenuto conto della natura, dell'oggetto e della finalità del trattamento, nonché dei rischi che insistono sui dati e della possibile "clonazione" del sistema in questione per l'acquisizione dei dati trasmessi per fini illeciti, la soluzione adottata dall'Azienda non può essere considerata una misura tecnica idonea a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, che prevede la trasmissione di dati, anche relativi alla salute, su una rete pubblica di comunicazioni»[78].

Valorizzando le specifiche caratteristiche del trattamento e i rischi posti dal medesimo per gli interessati, il Garante giunge alla conclusione che il «mancato utilizzo di tecniche crittografiche per il trasporto dei dati configura (…) una violazione dell'art. 5, par. 1, lett. *f)*, e dell'art. 32 del Regolamento, che peraltro al par. 1, lett. *a)*, individua espressamente la cifratura dei dati come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio (sul punto, cfr. anche il *considerando* n. 83 del Regolamento nella parte in cui prevede che "il titolare del trattamento (…) dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura")»[79].

L'Autorità, nella specie, ha provveduto all'applicazione del principio di sicurezza in combinazione con quello della *privacy by design* (art. 25, par. 1, GDPR), indicando che il titolare «avrebbe, infatti, dovuto mettere in atto, fin dalla progettazione del proprio servizio, misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, tra cui il principio di "integrità e riservatezza", provvedendo ad adottare un protocollo di rete sicuro, quale il protocollo "*https*" (*hypertext transfer protocol over secure socket layer*), nell'ambito del sistema in esame»[80].

Sull'importanza della cifratura dei dati quale misura per assicurare il rispetto del principio di sicurezza, il Garante si è espresso in più occasioni[81]. Di particolare

---

[77] Rispetto alla cifratura dei dati, le linee guida in materia di *dossier* sanitario si limitano a prescrivere la necessità di determinare «i criteri per la cifratura dei dati sensibili (ad es., attraverso l'applicazione anche parziale di tecnologie crittografiche a *file system* o *database*), al fine di rendere gli stessi inintelligibili» (GPDP, Provv. 4 giugno 2015, cit., Allegato A, p. 34).

[78] GPDP, Provv. 26 maggio 2022, cit.

[79] *Ibidem*.

[80] *Ibidem*.

[81] Si richiamano, in particolare, GPDP, Provv. 23 gennaio 2020, doc. *web* n. 9269618; Provv. 10 giugno 2021, doc. *web* n. 9685922 e Provv. 10 giugno 2021, doc. *web* n. 9685947, relativi a trattamenti svolti nel contesto di un sistema di gestione della segnalazione di illeciti, rispetto ai quali il Garante, valorizzando caratteristiche e rischi dei trattamenti effettuati in tale contesto, ha ritenuto necessaria l'adozione di misure di cifratura sia per il trasporto sia per la successiva conservazione dei dati. Sulla cifratura dei dati, si v. inoltre GPDP, Provv. 24 marzo 2022, doc. *web* n. 9767635 e Provv. 2 dicembre 2021, doc. *web* n. 9734934.

rilievo risulta quanto stabilito nel provvedimento adottato il 27 gennaio 2022 nei confronti dell'Azienda socio sanitaria territoriale Nord di Milano[82], in riferimento all'utilizzo del protocollo "*http*" nel sito *web* previsto da tale Azienda per la prenotazione delle prestazioni sanitarie.

Sul punto, il Garante ha riscontrato una violazione del principio di sicurezza e dell'art. 32 GDPR in base ad argomentazioni sostanzialmente analoghe a quelle richiamate nel provvedimento esaminato in precedenza, aggiungendo tuttavia un'importante specificazione: «allo stato dell'arte, l'utilizzo di tecniche crittografiche è una delle misure comunemente adottate per proteggere, in particolar modo, i dati personali degli utenti di un servizio *online* durante la loro trasmissione su rete Internet»[83].

Anche il provvedimento adottato nei confronti dell'Azienda ospedaliera di Perugia in data 7 aprile 2022, relativo ai modelli per la gestione della segnalazione di illeciti (c.d. "*whistleblowing*")[84], risulta particolarmente indicativo della sensibilità del Garante rispetto alla corretta attuazione del principio di sicurezza.

Nel caso in questione, l'applicativo per l'acquisizione e la gestione delle segnalazioni di condotte illecite, fornito da una società terza designata responsabile del trattamento, risultava implementato in modo da essere esposto su rete pubblica, ma raggiungibile esclusivamente da postazioni di lavoro attestate alla rete aziendale; l'accesso alla rete pubblica da tali postazioni avveniva mediante sistemi *firewall* che memorizzavano nei *file* di *log* le operazioni di navigazione effettuate.

Il Garante ha rilevato che «la registrazione e la conservazione, nei *log* degli apparati *firewall*, delle informazioni relative alle connessioni all'applicativo in questione consente la tracciabilità dei soggetti che utilizzano tale applicativo, tra i quali

[82] GPDP, Provv. 27 gennaio 2022, doc. *web* n. 9746448.

[83] *Ibidem*. Sul rilievo delle tecniche crittografiche quali misure di sicurezza richieste dallo "stato dell'arte" (art. 32, par. 1, GDPR) per garantire il rispetto del principio di integrità e riservatezza, si richiama inoltre GPDP, Provv. 10 febbraio 2022, doc. *web* n. 9751194, adottato nei confronti dell'ISTAT. Il caso ha riguardato un *data breach* scaturito da un attacco informatico che aveva comportato l'esfiltrazione e il potenziale accesso non autorizzato a dati personali comprendenti, tra gli altri, le credenziali di autenticazione a determinati portali gestiti dall'ISTAT. L'Autorità accertava la violazione degli artt. 5, par. 1, lett. *f),* e 32 GDPR a fronte della circostanza che l'Istituto «in qualità di titolare del trattamento e detentore di ingenti banche dati, esposte per loro stessa natura ad un'elevata probabilità di attacco, non disponeva, tenuto anche conto dello stato dell'arte tecnologico, di misure tecniche idonee a garantire su base permanente la sicurezza e la riservatezza dei dati trattati (…)» (*Ibidem*). In particolare, «(…) la conservazione mediante l'utilizzo di tecniche crittografiche allo stato dell'arte è una delle misure comunemente adottate per proteggere le *password* degli utenti di un servizio *online*, mentre l'Istat conservava, rispetto ai richiamati servizi, le *password* in chiaro o mediante un algoritmo non robusto allo stato dell'arte tecnologico» (*Ibidem*). In senso conforme, si v. anche GPDP, Provv. 6 ottobre 2022, doc. *web* n. 9817058, nel quale l'Autorità ha altresì evidenziato gli «elevati rischi» presentati dal trattamento delle credenziali di autenticazione ai servizi *online*, «anche in ragione dell'abitudine di molti utenti a riutilizzare la stessa *password*, o comunque una *password* molto simile, per l'accesso a diversi servizi *online*», specificando come l'uso di un protocollo di comunicazione cifrato possa mitigare, segnatamente, i rischi di «furto di identità, di possibile clonazione del sito *web* a scopo di *phishing* e di acquisizione delle credenziali di autenticazione per fini illeciti (…)».

[84] GPDP, Provv. 7 aprile 2022, cit.

i segnalanti. Ciò, considerato anche l'esiguo numero di connessioni all'applicativo in questione, rende inefficaci le altre misure adottate per tutelare la riservatezza dell'identità dei segnalanti. Per tali ragioni, la registrazione e la conservazione, all'interno dei *log* degli apparati *firewall*, di informazioni direttamente identificative degli utenti dell'applicativo in questione non risulta conforme alle disposizioni di cui all'art. 5, par. 1, lett. *f)*, e all'art. 32 del Regolamento (…)»[85].

Emerge allora che il principio di sicurezza, considerato anche dall'angolo prospettico dei principi di *privacy by design* e *by default*, impone di valutare il complesso degli elementi che compongono il sistema informativo nel quale si intende introdurre un determinato applicativo, in modo da verificare anche gli impatti sulla sicurezza derivanti dalla combinazione tra i vari elementi del sistema. Questa valutazione deve considerare altresì le possibili distorsioni che possono derivare dall'applicazione di una misura di sicurezza (nel caso in esame, il sistema *firewall*) a processi aventi peculiari caratteristiche (ivi, quello per la gestione della segnalazione di illeciti, per cui le norme di settore prevedono specifiche garanzie di riservatezza)[86].

Tale decisione, inoltre, rende manifesto che la sicurezza "adeguata" richiesta dal GDPR, come rimarcato nei paragrafi precedenti, può essere raggiunta solo dalla virtuosa convergenza di competenze informatiche, giuridiche e organizzative[87].

Di interesse, sotto molteplici profili, risulta anche il provvedimento adottato nei confronti di Crèdit Agricole Italia S.p.a. e Crèdit Agricole FriulAdria S.p.a. il 14 gennaio 2021[88].

Il caso origina dalle notifiche di un *data breach* incidente sulla riservatezza dei dati: un dipendente del responsabile del trattamento incaricato aveva inviato tramite PEC degli estratti conto a clienti diversi dagli intestatari dei rapporti bancari cui tali estratti si riferivano. Le violazioni, nella specie, erano state causate da un malfunzionamento *software* riconducibile a una esecuzione parziale dei test sulle modifiche che avevano interessato l'applicativo di invio delle PEC, in spregio delle procedure aziendali in materia di "*IT change management*".

---

[85] *Ibidem*. Sul punto, l'Autorità ha precisato che, ai fini della complessiva valutazione della conformità agli obblighi di sicurezza del trattamento, non rileva la circostanza che detti *log* non registrassero informazioni sulle attività svolte nel sistema, né che la consultazione degli stessi fosse consentita al solo amministratore di sistema. La registrazione delle sopra citate informazioni nei *log* del *firewall*, inoltre, è stata ritenuta non conforme ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR), i quali, secondo il Garante, impongono al titolare di effettuare una valutazione dei rischi funzionale all'idonea configurazione del sistema anche in caso di fruizione di prodotti o servizi forniti da terzi.

[86] Si veda quanto stabilito dalla l. 30 novembre 2017, n. 179, recante «*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*», nonché dalla Dir. UE 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e dal d.lgs. 10 marzo 2023, n. 24 attuativo di quest'ultima.

[87] Cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., p. 18; F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, cit., p. 261.

[88] GPDP, Provv. 14 gennaio 2021, doc. *web* n. 9582744.

Il Garante, pur ritenendo il suddetto processo aziendale di "*IT change management*" «una soluzione tecnicamente idonea a garantire una corretta gestione delle modifiche ai sistemi informatici»[89], ha statuito che tale soluzione non fosse «adeguatamente assistita da efficaci strumenti di rilevazione di anomalie, errori operativi e/o violazioni dolose»[90]. In particolare, a fronte dell'obbligo «di garantire "l'integrità e la riservatezza" dei dati personali (artt. 5, par. 1, lett. *f)* del Regolamento)» che grava sui titolari del trattamento «nell'ambito del più generale principio di responsabilizzazione di cui agli artt. 5, par. 2 e 24 del Regolamento», i titolari sono tenuti a verificare «l'effettiva rispondenza delle *policy* adottate ai principi di cui all'art. 32, par. 2, del Regolamento, con particolare riferimento a quanto previsto alle lett. *b)* e *d)*»[91]. A tali fini, il Garante ha ingiunto ai titolari «di prevedere (…) l'esecuzione di mirate attività di controllo volte a verificare la rispondenza delle specifiche procedure adottate per la gestione e l'esecuzione delle modifiche ai sistemi informatici (c.d. *IT change management*) alle più generali misure di sicurezza, tecniche e organizzative definite dalle società (…)»[92].

Questi passaggi pongono in risalto il peculiare significato del principio di "integrità e riservatezza" (ovvero di "sicurezza"), peraltro nell'ambito dei più ampi doveri di *accountability*[93]. L'approccio basato sul rischio – elemento intrinsecamente mutevole – rende indispensabile il monitoraggio continuo delle misure di sicurezza approntate[94]; a tali fini, occorre adottare specifiche procedure per testare, verificare e valutare regolarmente la loro efficacia [art. 32, par. 1, lett. *d)*, GDPR], misure, queste ultime, che i titolari sono tenuti a implementare anche in conformità al principio di responsabilizzazione.

Il caso in esame consente altresì di comprendere la portata del principio di sicurezza relativamente alle misure da adottare rispetto agli amministratori di sistema, onde contenere i rischi connessi ai trattamenti svolti da tali figure (cfr. *supra*, par. 2.2.).

L'Autorità, nel provvedimento del 14 gennaio 2021 da ultimo richiamato, ha evidenziato come il rilascio del suddetto *software* nell'ambiente di produzione era stato effettuato da un incaricato attraverso un'utenza tecnica assegnata ad altro di-

---

89 *Ibidem*.

90 *Ibidem*.

91 *Ibidem*.

92 *Ibidem.* L'Autorità, nella specie, ha ingiunto l'implementazione di tali misure «nell'ambito delle attività di *audit* interno previste dal provvedimento del Garante n. 192 del 12 maggio 2011 "in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie", (punto 4.3.2)» (*Ibidem*).

93 Sul principio di responsabilizzazione o "*accountability*" (art. 5, par. 2, GDPR), si veda ad es. G. Finocchiaro, *Il principio di accountability*, in *Giur. it.*, 2019, 12, pp. 2778-2783, nonché F. Albanese-I. Cardinali, *Il principio di responsabilizzazione (*accountability*)*, Cap. XIII del presente volume.

94 In tal senso, si veda G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., p. 18. Sulla "circolarità" del processo di gestione del rischio per garantire la permanenza degli standard di sicurezza imposti dal GDPR, si veda F. Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, cit., p. 281, che sul punto richiama A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, cit., p. 301.

pendente. Sul punto, è stata riscontrata una violazione del principio di "integrità e riservatezza" e degli obblighi previsti dall'art. 32 GDPR, in quanto «l'utilizzo di un'utenza tecnica da parte di più soggetti (i.e. il legittimo assegnatario e il dipendente in questione) impedisce di attribuire le azioni compiute in un sistema informatico a un determinato soggetto, con pregiudizio anche per il titolare e il responsabile, privati della possibilità di controllare l'operato di coloro che agiscono sotto la loro autorità; inoltre, allorquando un'utenza tecnica con privilegi amministrativi, come quella in questione, venga utilizzata da più soggetti, possono determinarsi situazioni in cui non c'è coerenza tra i profili di autorizzazione attribuiti e le effettive esigenze di operatività per la gestione dei sistemi, rendendo possibile a un soggetto non autorizzato di operare, in assenza di una specifica volontà del titolare o del responsabile, nell'ambito dei sistemi e dei servizi di trattamento, come in effetti è accaduto nel caso di specie»[95].

Sul versante sanzionatorio, è opportuno evidenziare come il Garante abbia considerato la violazione dell'art. 32 GDPR esclusivamente nel contesto della più grave violazione del principio di "sicurezza", posto che «la violazione dell'art. 32 del Regolamento», nel caso in esame, era «riferita a principi ricompresi nella disposizione, di portata generale, di cui all'art. 5 del Regolamento e inerenti l'"integrità e riservatezza" del trattamento (art. 5, par. 1, lett. *f)*, del Regolamento)»[96]. Di conseguenza, l'Autorità ha applicato la sanzione prevista dall'art. 83, par. 5, lett. *a),* GDPR, ma non anche quella stabilita dall'art. 83, par. 4, lett. *a)*, GDPR.

Il provvedimento in esame, in ultimo, consente di apprezzare il rilievo del principio di "sicurezza" nel caso di trattamenti esternalizzati a un responsabile del trattamento. Secondo l'Autorità, ai titolari del trattamento è «(…) attribuita la "responsabilità generale" del trattamento che essi abbiano posto in essere direttamente o che altri abbiano effettuato per loro conto»[97]; in tal senso, «(…) sebbene le violazioni in questione si siano verificate nell'ambito dell'operatività di CA Group Solutions, responsabile del trattamento (i cui dipendenti hanno agito in parziale violazione delle istruzioni ricevute), purtuttavia CA Italia e CA FriulAdria, quali titolari del trattamento (…) hanno omesso di verificare, in relazione alla natura, al contesto, alle finalità e ai rischi del trattamento realizzato nell'ambito del processo di *IT Change Management*, l'effettiva conformità dello stesso ai principi di integrità e riservatezza di cui all'art. 5, par. 1, lett. *f)* e degli obblighi in materia di sicurezza del trattamento di cui all'art. 32, par. 1 e 2, lett. *b)* e *d)* del Regolamento»[98].

Il titolare del trattamento è pertanto tenuto a svolgere le attività di verifica che, a seconda delle caratteristiche del trattamento e dei rischi presentati da quest'ultimo nel singolo caso, devono ritenersi necessarie per assicurare che il responsabile inca-

[95] GPDP, Provv. 14 gennaio 2021, cit. Sulla questione dell'attribuzione individuale delle utenze con privilegi amministrativi, già disciplinata nel provvedimento relativo agli amministratori di sistema del 27 novembre 2008, si vedano anche GPDP, Provv. 10 giugno 2021, doc. *web* n. 9685947 e Provv. 4 aprile 2019, doc. *web* n. 9101974.

[96] GPDP, Provv. 14 gennaio 2021, cit.

[97] *Ibidem*.

[98] *Ibidem*.

ricato tratti i dati in conformità al principio di "integrità e riservatezza" e ai correlati obblighi di sicurezza[99].

A ogni modo, anche il responsabile del trattamento è specifico destinatario delle prescrizioni derivanti dal principio di "sicurezza". Il Garante si è mostrato particolarmente attento a questi profili, come emerge dal provvedimento adottato nei confronti di Brav s.r.l. in data 24 marzo 2022[100].

Il caso è relativo a una violazione dei dati personali causata da un accesso abusivo alla piattaforma fornita dal responsabile del trattamento Brav s.r.l. al Comune di Genova, utilizzata dalla Polizia locale di tale Comune per la gestione delle contravvenzioni al Codice della Strada. La violazione era stata cagionata dalla condotta degli stessi agenti, i quali avevano divulgato le credenziali di accesso alla piattaforma (rimaste invariate rispetto a quelle assegnate per il primo accesso).

Il Garante, pur rilevando che l'accesso abusivo era avvenuto a causa del comportamento del personale della polizia, ha ritenuto che «la società avrebbe comunque dovuto adottare misure tecniche e organizzative volte ad assicurare che le *password* dei soggetti autorizzati rispettassero criteri di qualità e fossero obbligatoriamente modificate al primo utilizzo»[101] e, conseguentemente, ha accertato in capo alla società la violazione del principio di "sicurezza" ("integrità e riservatezza") di cui all'art. 5, par. 1, lett. *f)*, e degli obblighi di cui all'art. 32 GDPR.

In particolare, l'Autorità ha ricordato che «taluni obblighi sono posti direttamente anche a carico dello stesso responsabile il quale, in base anche alle competenze tecniche specifiche, deve collaborare, anche manifestando un'autonomia propositiva, nell'adozione di misure adeguate e nella verifica sistematica dell'efficacia delle stesse, soprattutto nel caso in cui fornisca servizi a una pluralità di titolari del trattamento che coinvolgono un numero elevato di interessati, come nel caso in esame»[102]. In sostanza, la società responsabile, «in ragione della sua esperienza nel settore, era tenuta a verificare costantemente l'efficacia delle misure poste a presidio della piattaforma fornita alla Polizia Locale del Comune di Genova per la gestione delle contravvenzioni (…)»[103].

Risulta opportuno rimarcare che l'Autorità ha reputato di non dover adottare alcun provvedimento nei confronti del Comune titolare del trattamento, «(…) in quanto si è tenuto conto che nell'atto di nomina a responsabile del trattamento ai sensi dell'art. 28 del Regolamento, il Comune di Genova ha esplicitamente previsto, tra

---

[99] Sul punto, si veda l'art. 28. par. 3, lett. *d)*, GDPR, il quale dispone che l'atto giuridico volto a disciplinare il rapporto tra titolare e responsabile del trattamento preveda che quest'ultimo «metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato». Rispetto alla responsabilità imputabile al titolare del trattamento per *culpa in vigilando* sul responsabile del trattamento, cfr. C. Bistolfi, *Adozione obbligatoria di strumenti per la sicurezza del trattamento: adozione di specifici strumenti*, cit., pp. 402 ss.

[100] GPDP, Provv. 24 marzo 2022, doc. *web* n. 9767635. Sul medesimo tema, si v. GPDP, Provv. 11 febbraio 2021, doc. *web* n. 9562831 e Provv. 22 luglio 2021, doc. *web* n. 9698597.

[101] GPDP, Provv. 24 marzo 2022, cit.

[102] *Ibidem*.

[103] *Ibidem*.

l'altro, l'obbligo, per la società, in ragione della sua esperienza tecnica nel settore, di mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio inclusa una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento»[104].

Ne emerge, dunque, che l'entità degli adempimenti discendenti dal principio di "sicurezza" in capo a titolare e responsabile del trattamento può essere modulata mediante un'attenta definizione dei contenuti dell'atto giuridico previsto dall'art. 28, par. 3, GDPR; ciò, fino al punto di determinare, come avvenuto nel caso in esame, un'esclusione di responsabilità del titolare – sotto il profilo dell'illecito amministrativo sanzionabile *ex* art. 83 GDPR – per condotte materialmente poste in essere dal proprio personale autorizzato, lasciando fermo, per il responsabile del trattamento, l'obbligo di adottare le misure idonee ad evitare tali violazioni, di cui anch'egli è diretto destinatario ai sensi dell'art. 32 GDPR.

Ulteriori indicazioni per garantire il rispetto del principio di sicurezza mediante misure di protezione da trattamenti non autorizzati o illeciti si rivengono nel provvedimento adottato l'11 febbraio 2021 nei confronti di Roma Capitale, inerente al sistema previsto per la verifica dei permessi per l'accesso e la sosta nelle zone a traffico limitato ("Z.T.L.") di Roma[105].

L'Autorità, ivi, ha riscontrato la violazione degli artt. 5, par. 1, lett. *f)*, e 32 GDPR in quanto i sopra citati permessi, da esporre sui veicoli, riportavano un *QR code* che permetteva a chiunque, tramite una generica *app* di decodifica dei *QR code*, di accedere ai dati personali relativi ai loro titolari e utilizzatori. L'illecita diffusione dei dati è stata imputata alla mancata adozione di sistemi di autenticazione e autorizzazione idonei a garantire un livello di sicurezza adeguato al rischio e tali da limitare l'accesso ai medesimi «al solo personale effettivamente autorizzato al trattamento necessario per la finalità di interesse pubblico funzionale al controllo della validità dei permessi (…)»[106].

Di conseguenza, il Garante ha ingiunto al titolare l'adozione di misure «che garantiscano un livello di sicurezza adeguato ai rischi presentati dal trattamento concernenti: *i)* la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le *password* relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di *password* "deboli" e che le medesime *password* siano modificate almeno al primo utilizzo; *ii)* la capacità di contrastare efficacemente attacchi informatici di tipo *brute force* sul sistema di autenticazione *online*, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione»[107].

---

[104] *Ibidem*. In aggiunta, il Garante ha dato atto della circostanza che il Comune avesse già ripristinato le misure di sicurezza adeguate al rischio e svolto attività di sensibilizzazione verso il proprio personale autorizzato.

[105] GPDP, Provv. 11 febbraio 2021, doc. *web* n. 9562852.

[106] *Ibidem*.

[107] *Ibidem*. Le indicazioni fornite dal Garante nel provvedimento in esame coincidono, soltanto in parte, con quelle relative ai sistemi di autenticazione e autorizzazione previste all'interno dell'abrogato All. B al d.lgs. n. 196/2003. Sulla violazione del principio di sicurezza per la mancata implementa-

Rispetto alle misure di *audit log*, si richiama il provvedimento adottato verso TPER (Trasporto Passeggeri Emilia Romagna S.p.A.) in data 28 ottobre 2021[108].

Il caso ha riguardato il trattamento dei dati personali degli operatori addetti al *call center* svolto da tale società mediante un sistema di gestione delle telefonate di assistenza all'utenza. Detto sistema, nella specie, consentiva la registrazione delle chiamate e dei relativi metadati associati ai nominativi dei dipendenti.

Al di là dei profili inerenti alle riscontrate violazioni delle norme in materia di controllo a distanza dell'attività lavorativa e di altre disposizioni in materia di protezione dei dati personali, preme ivi evidenziare i rilievi relativi alla misura di sicurezza della tracciatura degli accessi alle telefonate registrate.

Il Garante ha giudicato il sistema di tracciatura adottato dal titolare non conforme al principio di "sicurezza" e all'art. 32 GDPR, in quanto tale sistema non permetteva la registrazione nei *log file*: *i)* delle operazioni svolte dai tecnici della società incaricata quale responsabile del trattamento; *ii)* delle operazioni di creazione e cancellazione delle utenze e di cancellazione delle chiamate registrate. Al riguardo, «tali mancate registrazioni non consentono pertanto al titolare del trattamento di avere contezza, con certezza e in modo esaustivo, di tutti gli accessi alle telefonate registrate né lo rendono in grado di documentare tali accessi»[109].

Sul punto, si ravvisa anche in tal caso un'applicazione del principio in esame in combinazione con quello di responsabilizzazione (art. 5, par. 2, GDPR). Secondo l'Autorità, infatti, la doverosità dell'adozione di idonei strumenti di tracciatura deriva «(…) dall'obbligo di adottare misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato anche rispetto al rischio di divulgazione non autorizzata o accesso illecito ai dati (art. 32 del Regolamento) e dal correlato obbligo di comprovarne l'adeguatezza (artt. 5, par. 2, e 24 Regolamento). In ragione della "responsabilità generale" del titolare del trattamento (art. 5, par. 2 del Regolamento) lo stesso è, infatti, tenuto a "mettere in atto misure adeguate ed efficaci [e] (…) dimostrare la conformità delle attività di trattamento con il (…) Regolamento, compresa l'efficacia delle misure" (cfr. *considerando* 74 nonché artt. 24 e 25 del Regolamento), fornendo a tal fine le necessarie indicazioni al fornitore del servizio (art. 28 del Regolamento)»[110].

---

zione di idonei sistemi di autenticazione e autorizzazione, si v. anche GPDP, Provv. 7 aprile 2022, cit., nel quale è stata sottolineata la necessità di disattivare tempestivamente le credenziali di autenticazione in caso di perdita delle qualità che consentono al personale autorizzato di accedere ai dati, onde evitare trattamenti non autorizzati – misura, questa, già prevista dall'abr. All. B al d.lgs. n. 196/2003.

[108] GPDP, Provv. 28 ottobre 2021, doc. *web* n. 9722661.

[109] *Ibidem*.

[110] *Ibidem*. Sull'implementazione di un sistema di *audit log* conforme al principio di sicurezza si richiama inoltre GPDP, Provv. 18 dicembre 2019, doc. *web* n. 9283040. Ivi, negli *access log* degli amministratori di sistema risultavano registrate, in chiaro, le credenziali di autenticazione immesse dagli amministratori. Per l'Autorità, tale circostanza «costituisce di per sé una grave violazione degli obblighi di sicurezza di cui all'art. 32 del GDPR in quanto compromette la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, sia quando tali credenziali consentono di trattare direttamente dati personali, sia quando le stesse sono utilizzate per amministrare e gestire i sistemi informatici coinvolti nel trattamento (cfr.

Utile per comprendere la portata del principio in esame rispetto alle varie declinazioni della sicurezza (cfr. *supra*, par. 2.2.) è il provvedimento del 14 gennaio 2021 che ha interessato l'Agenzia Regionale Protezione Ambientale Campania (ARPAC), scaturito dalla notifica di un *data breach* relativo al furto di un *hard disk* esterno contenente dati personali[111].

La violazione, ivi, incideva sia sulla riservatezza dei dati, posto che il dispositivo non era protetto da misure quali, ad esempio, la cifratura, sia sulla disponibilità, in quanto il *backup* dei dati memorizzati nell'*hard disk* non era andato a buon fine. Il Garante, accertando l'illiceità del trattamento per violazione degli artt. 5, par. 1, lett. *f)*, e 32 GDPR, ha evidenziato che la violazione era stata resa possibile in ragione dell'assenza di misure tali da garantire un livello di sicurezza adeguato al rischio. In particolare, oltre alla mancanza di «accorgimenti necessari a consentire la continuità, su base permanente, e il ripristino della disponibilità dei dati personali sottratti»[112] e di «procedure idonee a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento»[113], è stata accertata la carenza di «tecniche in grado di assicurare la non identificabilità degli interessati ai quali i dati personali contenuti nel dispositivo si riferivano, per limitare il rischio della loro consultazione da parte di soggetti non debitamente autorizzati (come la pseudonimizzazione o la cifratura dei dati), tenuto anche conto che, presso il locale in cui era custodito il dispositivo sottratto, poteva accedere qualsiasi dipendente»[114].

In conclusione, è indispensabile richiamare l'attenzione sull'ampia casistica riguardante *data breach* avvenuti in ambito sanitario, segnatamente a causa di operazioni di comunicazione di dati sanitari a terzi non autorizzati al trattamento[115].

---

anche art. 5, § 1, lett. *f)*, del GDPR)» (*Ibidem*). L'Autorità ha dunque ritenuto «che riportare all'interno dei file di *log* informazioni non indispensabili per le finalità di controllo e sicurezza connesse al tracciamento degli accessi e delle operazioni compiute su un sistema informatico e sui dati in esso contenuti, determini una duplicazione di dati personali oggetto di trattamento nell'ambito del predetto sistema che risultano così esposti a maggiori rischi di trattamenti non autorizzati o illeciti, e, quindi, non sia conforme ai principi di minimizzazione e di riservatezza di cui all'art. 5, § 1, lett. *c)* e *f)*, del GDPR» (*Ibidem*).

[111] GPDP, Provv. 14 gennaio 2021, doc. *web* n. 9538748.

[112] *Ibidem*.

[113] *Ibidem*.

[114] *Ibidem*.

[115] Queste fattispecie comprendono, ad esempio, la consegna di copie della cartella clinica a persone non autorizzate a riceverle (cfr. GPDP, Provv. 16 settembre 2021, doc. *web* n. 9718851) o di copie della cartella recanti la documentazione sanitaria di altri pazienti (cfr. GPDP, Provv. 27 gennaio 2021, doc. web n. 9544092; Provv. 11 febbraio 2021, doc. *web* n. 9561792 e Provv. 8 luglio 2021, doc. *web* n. 9691011), la comunicazione di informazioni sullo stato di salute di una persona in violazione delle indicazioni del paziente (cfr. GPDP, Provv. 27 gennaio 2021, doc. *web* n. 9544504) o del diritto di oscuramento in materia di Fascicolo Sanitario Elettronico (cfr. GPDP, Provv. 29 aprile 2021, doc. *web* n. 9676172), l'invio postale di documentazione sanitaria ad erroneo destinatario (cfr. GPDP, Provv. 27 gennaio 2021, doc. *web* n. 9544457 e Provv. 11 febbraio 2021, doc. *web* n. 9567489), l'inserimento di un referto clinico nel FSE di un terzo (cfr. GPDP, Provv. 9 luglio 2020, doc. *web* n. 9440117), l'invio di *e-mail* a un gruppo di pazienti inserendo gli indirizzi dei destinatari nel campo "copia conoscenza" in luogo di quello "copia conoscenza nascosta" (cfr. GPDP, Provv. 28 aprile 2022, doc. *web* n. 9779057 e Provv. 16 settembre 2021, doc. *web* n. 9722297).

Al riguardo, preme rimarcare alcuni profili emergenti dalla complessiva prassi applicativa in materia, i quali forniscono utili indicazioni circa gli elementi da considerare per garantire il rispetto del principio di "integrità e riservatezza" in tale ambito.

Anzitutto, l'osservanza del principio in esame e degli obblighi di sicurezza previsti dal GDPR «(…) si impone, ancor più, con riferimento ai dati personali relativi alla salute»[116], in quanto «tali dati meritano una maggiore protezione dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali (Cons. n. 51)»[117]. Particolare attenzione, poi, deve essere prestata alle norme di settore applicabili in tale ambito (anche ai sensi dell'art. 75 del d.lgs. n. 196/2003)[118], le quali possono evidenziare elementi di rischio o esigenze di tutela che è indispensabile considerare per approntare misure di sicurezza proporzionate al rischio[119]. In ultimo, come espressamente evidenziato dal Garante, «(…) il continuo verificarsi di casi analoghi nel settore della sanità, in generale, dovrebbe portare i titolari del trattamento a stimare come altamente probabile il verificarsi di rischi simili»[120].

Dal complesso di queste circostanze emerge pertanto la necessità, nel contesto sanitario, di implementare più efficaci misure per assicurare il rispetto del principio di sicurezza e, più ampiamente, dei diritti e delle libertà degli interessati.

[116] GPDP, Provv. 14 ottobre 2021, doc. *web* n. 9717745.

[117] *Ibidem*.

[118] L'art. 75 del d.lgs. n. 196/2003, rubricato «*Specifiche condizioni in ambito sanitario*», dispone che «[i]l trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere *h)* ed *i)*, e 3 del GDPR, dell'articolo 2-*septies* del presente codice, nonché nel rispetto delle specifiche disposizioni di settore».

[119] Si richiamano, ad esempio, le norme in materia di interruzione volontaria della gravidanza (l. n. 174/1978), le quali richiedono «che venga assicurato al più alto livello il rispetto della dignità e della riservatezza della donna» (cfr. GPDP, Provv. 27 gennaio 2021, doc. *web* n. 9544504); le norme in materia di prevenzione e lotta all'AIDS di cui alla l. n. 135/1990, che prevedono specifiche garanzie a tutela dei diritti e della dignità della persona (cfr. GPDP, Provv. 16 settembre 2021, doc. *web* n. 9722297); il d.l. n. 179/2012 di istituzione del Fascicolo Sanitario Elettronico e il relativo d.p.c.m. n. 178/2015, circa le garanzie di riservatezza dell'assistito in caso di esercizio del diritto di oscuramento (cfr. GPDP, Provv. 29 aprile 2021, doc. *web* n. 9676172).

[120] Cfr. GPDP, Provv. 24 marzo 2022, doc. *web* n. 9767077.

Capitolo X
Il principio di necessità

*Cristina Chilin - Daniele Sborlini**

Sommario: 1. Inquadramento normativo. – 1.1. Premessa su diritto alla protezione dei dati personali e principio di necessità. – 1.2. Il principio di necessità e il suo inquadramento normativo: dal Codice della *privacy* al GDPR. – 1.3. Il principio di necessità nella Convenzione 108/81 e nella Convenzione 108+. – 2. Portata del principio. – 2.1. Il principio di necessità nel Codice della *privacy*. – 2.2. (*segue*): Rapporto tra principio di necessità e principio di pertinenza e non eccedenza nel Codice della *privacy*: endiadi o duplicazione? – 2.3. Il principio di necessità alla luce del GDPR. – 2.4. (*segue*): Il principio di necessità nel bilanciamento tra diritto alla protezione dei dati e libera circolazione degli stessi (art. 1, part. 3, GDPR). – 2.5. (*segue*): Principio di necessità e condizioni di liceità del trattamento diverse dal consenso. – 2.6. (*segue*): Principio di necessità e principio di minimizzazione dei dati nel GDPR. – 2.7. (*segue*): Principio di necessità e valutazione d'impatto *ex* art. 35 GDPR. – 2.8. Il principio di necessità e *privacy by design* e *by default* nel GDPR. Il consolidamento nell'ordinamento europeo dell'originaria accezione del «principio di necessità» già emergente *ex* art. 3 del Codice della *privacy*. – 3. Applicazione del principio nella casistica.

1. Inquadramento normativo

1.1. Premessa su diritto alla protezione dei dati personali e principio di necessità

In attuazione della Dir. 95/46/CE, il legislatore italiano, con il d.lgs. 30 giugno 2003, n. 196[1], recante il «*Codice in materia di protezione dei dati personali*», aveva codificato espressamente nel nostro ordinamento giuridico il diritto di protezione dei dati personali[2], facendone menzione nell'art. 1 («Chiunque ha diritto alla protezione

---

* Pur essendo lo scritto frutto di riflessione comune, i par. 1 e 2 sono da attribuire a Cristina Chilin, il par. 3 è da attribuire a Daniele Sborlini.

1 Il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) è stato pubblicato nella G.U. 29 luglio 2003, n. 174 ed è entrato in vigore il 1° gennaio 2004. È stato successivamente modificato dal d.lgs. 10 agosto 2018, n. 101 (recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e da altri più recenti interventi normativi.

2 Il diritto alla protezione dei dati personali era già disciplinato nell'ordinamento italiano dalla l. 31 dicembre 1996, n. 675, che statuiva la tutela delle persone e di altri soggetti al trattamento dei dati personali, pubblicata in G.U. 8 gennaio 1997, n. 5, in attuazione della Dir. 95/46/CE. Tale diritto trova riconoscimento anche nell'ordinamento europeo all'art. 8 della Carta dei diritti fondamen-

dei dati personali che lo riguardano»), poi abrogato in forma del d.lgs. n. 101/2018, per esigenze di coordinamento con il Reg. UE n. 679/2016 (GDPR)[3].

Si tratta di un diritto fondamentale[4] in base al quale ogni individuo può pretendere che i propri dati personali siano raccolti e trattati soltanto con il proprio consenso o sulla base di altro presupposto legittimo individuato per legge, nel rispetto delle regole previste dalle leggi, nazionali ed europee, nonché in conformità ai diritti e alle libertà fondamentali[5] e ai principi generali[6] in tema di trattamento dei dati. Proprio con riferimento ai principi, elementi essenziali per comprendere la normativa, il legislatore italiano aveva dedicato nel Codice della *privacy* un intero titolo: il primo.

Per converso, in ambito europeo e precisamente nel Reg. UE n. 679/2016 il legislatore, relativamente ai principi, ha individuato un solo articolo, in cui ha riorganizzato l'enunciazione dei «Principi applicabili al trattamento di dati personali». Specificatamente, all'art. 5, par. 1, del Reg. cit. il legislatore individua i principi di "liceità", "correttezza" e "trasparenza", "limitazione delle finalità", "esattezza", "limitazione della conservazione", "integrità e riservatezza" (sicurezza e confidenzialità), e il principio di "minimizzazione dei dati", a sua volta declinato nei canoni della necessità, pertinenza e non eccedenza rispetto alle finalità, a cui si aggiunge, al par. 2, il principio di responsabilizzazione (*accountability*).

Il principio di necessità, pur connesso con il principio di minimizzazione, presenta tuttavia una propria autonomia con riferimento al trattamento dei dati personali.

Partendo da queste premesse, il presente contributo avrà ad oggetto l'analisi del principio di necessità del trattamento dei dati al fine di rimarcare non solo le connessioni con altri principi, ma anche il suo autonomo rilievo e il suo ambito applicativo, sia sul piano teorico che su quello della casistica.

---

tali dell'Unione Europea e all'art. 16, par. 1, del trattato sul funzionamento dell'Unione europea (TFUE), nonché al *considerando* n. 1 e all'art. 1 del Reg. UE n. 679/2016.

[3] Il Reg. UE n. 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) è stato pubblicato in G.U.U.E. il 4 maggio 2016, l. 119/1 ed è entrato in vigore il 24 maggio 2016 con applicazione diretta agli Stati membri a far data dal 25 maggio 2018.

[4] Si veda, ora, l'art. 8 della Carta dei diritti fondamentali dell'UE, espressamente dedicato al «Diritto alla protezione dei dati personali».

[5] L'art. 2 del Codice della *privacy*, abrogato nel 2018 per esigenze di coordinamento con il GDPR, prevedeva espressamente che «Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento». Con l'entrata in vigore del Reg. UE n. 679/2016 il legislatore europeo ha ivi precisato al *considerando* n. 4 che «il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero e di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

[6] I principi generali applicabili al trattamento dei dati si rinvenivano all'art. 1, lett. *a),* l. 31 dicembre 1996, n. 675, agli artt. 3 e 11 del d.lgs. 30 giugno 2003, n. 196 e attualmente all'art. 5 GDPR.

In tale direzione, sotto il profilo metodologico, appare utile indagare l'evoluzione del principio di necessità e della sua portata applicativa, nel passaggio che si è registrato dalla disciplina previgente a quella attuale, avutasi a seguito della definitiva applicazione del Reg. UE n. 679/2016 e dell'intervento di modifica al Codice in materia di protezione dei dati personali (effettuato, per esigenze di coordinamento, con il d.lgs. 101/2018).

In primis, si provvederà ad individuare l'inquadramento normativo del principio di necessità nella disciplina in materia di protezione dei dati personali: dalla sua codificazione nell'ordinamento normativo italiano *ex* art. 3 del Codice *privacy* sino alla sua collazione nel Reg. cit. agli artt. 5, 6, 25 e 35, oltre che all'art. 1, par. 3. Si analizzerà anche la portata applicativa di tale principio, prestando particolare attenzione alle tecniche di bilanciamento tra diritto alla protezione dei dati personali e libera circolazione degli stessi[7].

In particolare, ci si chiederà come il principio di necessità possa operare, indipendentemente dal principio di minimizzazione dei dati, per dirimere il rapporto tra l'uno e l'altra, alla luce dell'art. 1, par. 3 del reg. cit. in cui sembra che il legislatore europeo riconosca come preminente il diritto alla libera circolazione dei dati rispetto al trattamento dei dati personali, là dove afferma che «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»[8].

Per procedere a tale analisi si prenderà in considerazione anche l'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE, che consente una limitazione alla portata dei principi e dei diritti soltanto laddove sia necessaria e risponda effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Infine, nell'ultimo paragrafo, si esamineranno i principali casi in cui il principio di necessità è stato più volte richiamato e applicato in concreto nei provvedimenti nazionali dell'Autorità garante per la protezione dei dati personali, tenendo altresì conto degli orientamenti espressi dal Gruppo di lavoro *ex* Art. 29, dall'*European*

---

[7] Nell'ambito dell'Unione Europa la base giuridica sulla libera circolazione dei dati si rinviene all'art. 16, par. 2, del Trattato sul funzionamento dell'Unione Europea (TFUE) in base al quale le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati sono demandate al Parlamento europeo e al Consiglio. Per quel che concerne la disciplina normativa in ambito *privacy* il diritto di libera circolazione dei dati trovava una prima collocazione nella Dir. 95/46/CE all'art. 1, par. 2, in cui non era consentito agli Stati membri vietare o restringere la libera circolazione dei dati per motivi connessi alla tutela dei diritti e delle libertà fondamentali delle persone fisiche ed ora è previsto all'art. 1, par. 3, del Reg. UE n. 679/2016.

[8] Tale concetto si trova più volte ribadito nei *considerando* del Reg. UE n. 679/2016: tra i più degni di nota si evidenziano il *considerando* n. 13, in base al quale «per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici», ed ancora il *considerando* n. 170, in cui si prevede che «poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma (…) può essere meglio conseguito a livello di Unione».

Data Protection Board (EDPB), dall'*European Data Protection Supervisor* (EDPS), nonché dalla Corte di Giustizia UE.

1.2. Il principio di necessità e il suo inquadramento normativo: dal Codice della *privacy* al GDPR

Nel nostro ordinamento giuridico il principio di necessità in materia di protezione dei dati personali ha trovato espressa previsione normativa con il Codice della *privacy* all'art. 3[9], poi abrogato con la riforma del 2018[10].

Specificatamente, in tale articolo – rubricato «*Principio di necessità nel trattamento dei dati*» – si prevedeva che i sistemi informativi e i programmi informatici dovessero essere configurati in modo da garantire sia che l'utilizzazione dei dati personali[11] o di quelli identificativi[12] venisse ridotta al minimo, sia che il trattamento dei dati dovesse escludersi quando le medesime finalità potessero essere conseguite con dati anonimi[13] o con modalità che permettessero di identificare l'interessato solo in caso di necessità.

---

[9] Va precisato che nell'ordinamento italiano, con riguardo allo specifico settore della protezione dei dati personali, il principio di necessità ha trovato la sua prima collocazione nell'art. 3, co. 3, d.lgs. 11 maggio 1999, n. 135, norma con portata applicativa circoscritta al trattamento di dati sensibili da parte di soggetti pubblici. Tale comma prevedeva che i soggetti pubblici dovevano verificare periodicamente, tra i vari adempimenti, anche la necessità del trattamento dei dati rispetto alle finalità perseguite. Ed ancora ai co. 4 e 5 del medesimo articolo si precisava che «I dati che, anche a seguito delle verifiche, risultano (…) non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti». Si tratta di norme che raffiguravano il principio di necessità come principio privo di autonomo rilievo. Cfr. D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali* in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, Torino, 2007, p. 19.

[10] Nel Codice della *privacy* si potevano rinvenire altri riferimenti al principio di necessità, ad esempio in tema di trattamenti in ambito giudiziario, all'art. 48 («banche dati di uffici giudiziari»), nell'ambito del trattamento dei dati da parte di forze di polizia, all'art. 54 («modalità di trattamento *e* flussi di dati»), nonché in ambito di trattamento di dati sanitari, all'art. 91 («dati trattati mediante carte»).

[11] Segnatamente, per «dato personale» si intende, ai sensi e per gli effetti dell'art. 4, par. 1, n. 1), GDPR, «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato") (…)». Anche nel Codice della *privacy*, all'art. 4, co. 1, lett. *a),* si rinveniva una simile definizione, nella quale originariamente, tuttavia, a differenza di quanto previsto più recentemente nella medesima normativa (a seguito di interventi modificativi) e successivamente nell'attuale disciplina europea, si prevedeva che il dato personale potesse riguardare non solo la persona fisica ma anche la persona giuridica.

[12] In particolare, il Codice della *privacy*, all'art. 4, co. 1, lett. *b)*, definiva i «*dati identificativi*» come quei «dati personali che permettono l'identificazione diretta dell'interessato». Nel regolamento europeo, l'art. 4, par. 1, n. 1), stabilisce che «(…) si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[13] Segnatamente per «*dato anonimo*» si intende «il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile»: in tal senso si esprimeva l'abrogato art. 4, co. 1, lett. *c)*, Codice della *privacy*. Nel GDPR non si rinviene alcuna definizione esplicita di dato anonimo all'interno delle disposizioni normative. La nozione è tuttavia evincibile da quanto ivi

Quanto appena esposto, sembra non trovare riscontro alcuno nella normativa europea. Difatti, se si analizza l'art. 6 della Dir. 95/46/CE[14], in cui si sostanzia la Sezione I (intitolata «Principi relativi alla qualità dei dati»)[15] del Capo II (dedicato alle «Condizioni generali di liceità dei trattamenti di dati personali»), il principio di necessità non risulta declinato espressamente. Ve ne era menzione tuttavia all'art. 7, contenuto nella Sezione II («Principi relativi alla legittimazione del trattamento dei dati»), nella parte in cui si richiedeva, per le ipotesi diverse dal consenso dell'interessato, che il trattamento fosse pur sempre «necessario» rispetto alla condizione via via individuata per la sua liceità[16]. Si tratta di soluzione replicata anche nell'impianto del GDPR. Non vi era, però, una disposizione normativa che contemplasse in via autonoma il «principio di necessità» nel trattamento dei dati. Nell'ordinamento italiano, dunque, l'art. 3 del Codice rappresentava un'innovazione di particolare rilievo.

A seguito dell'abrogazione della già menzionata direttiva, il legislatore europeo con il GDPR ha ritenuto opportuno percorrere la strada già intrapresa dal legislatore italiano, dando maggior enfasi al principio di necessità, che si rinviene declinato – talvolta esplicitamente, talvolta implicitamente – in più norme.

Il principio di necessità nella disciplina europea può qualificarsi come l'elemento costitutivo ed insopprimibile di altri principi applicabili al trattamento dei dati personali.

Si pensi, ad esempio, all'art. 5 GDPR, ove il principio di necessità costituisce uno dei canoni[17] – assieme all'adeguatezza e alla pertinenza e non eccedenza[18] – del principio di minimizzazione dei dati[19].

---

affermato al *considerando* n. 26, ove si trova ribadito che «I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell›interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca».

[14] La Dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pubblicata in G.U.U.E. l. n. 281 del 23 novembre 1995, è stata abrogata dal Reg. UE n. 679/2016.

[15] Si noti come al *considerando* n. 11 della Dir. 95/46/CE si prevedeva che i principi generali ivi contenuti «precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale». Tuttavia, nella Convenzione n. 108/81 non vi era alcun rifermento esplicito al principio di necessità.

[16] Per un maggior approfondimento si veda Gruppo di lavoro ex art. 29, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014, p. 16.

[17] Risulta pacifico in dottrina che il principio di necessità costituisca espressione del principio di minimizzazione. A tal riguardo si veda: F. Resta, *Comm. all'art. 5. Principi applicabili al trattamento dei dati personali*, in G.M. Riccio-G. Scorza-E. Belisario (a cura di), *GDPR e normativa privacy. Commentario al Regolamento (UE) 2016/679,* Milano, 2018, p. 57; G. Cristofari-F. Sartore, *Comm. art. 5 GDPR* (*Principi applicabili al trattamento di dati personali)*, in L. Bolognini-E. Pelino (a cura di), *Codice della disciplina privacy*, Milano, 2019, p. 88.

[18] Il principio di pertinenza e non eccedenza stabilisce che i dati personali potranno essere registrati ed elaborati soltanto se necessari alle finalità perseguite. Cfr. art. 11, co. 1, lett. *d)*, Codice della *privacy* e art. 6, par. 1, lett. *c)*, Dir. 95/46/CE e art. 5, par. 1, lett. *c)*, GDPR.

[19] Il principio di minimizzazione è espressamente menzionato sia al *considerando* n. 156, sia all'art. 5, par. 1, lett. *c)*, GDPR, il quale stabilisce che i dati devono essere «adeguati, pertinenti e limitati a

Si consideri, altresì, l'art. 35 GDPR, ove il principio di necessità assume un ruolo rilevante, in relazione al principio di responsabilizzazione (*accountability*)[20], anche nella valutazione d'impatto sulla protezione dei dati (DPIA)[21], in relazione alla quale il titolare del trattamento, dovrà procedere alla valutazione del rischio (c.d. *risk based*) quando l'uso di nuove tecnologie potrebbe presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati.

Ancora, da una lettura attenta della normativa europea, si può ravvisare una trasposizione del principio di necessità – quale delineato nell'art. 3, poi abrogato, del Codice – nell'obbligo di protezione dei dati fin dalla progettazione (*privacy by design*) e nell'obbligo di protezione per impostazione predefinita (*privacy by default*), previsti ora all'art. 25 del Reg. cit., ove il titolare del trattamento, nell'adottare le misure tecniche e organizzative, deve tener in debita considerazione il principio di necessità del trattamento[22].

Nelle maglie del regolamento europeo il principio di necessità, così come già avvenuto per la Dir. 95/46/CE, emerge anche con riguardo alle condizioni di liceità alternative al consenso, richiedendosi sempre che il trattamento sia in rapporto di «necessità» con il presupposto individuato *ex lege*.

1.3. Il principio di necessità nella Convenzione 108/81 e nella Convenzione 108+

Il principio di necessità ha trovato applicazione, in ambito internazionale, con la «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale», anche nota come Convenzione 108[23].

Si tratta di un vero e proprio trattato internazionale che in Italia è entrato in vigore il 1° luglio 1997 e che costituisce uno strumento internazionale giuridicamente

quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati")».

[20] Il principio dell'*accountability* mira alla responsabilizzazione del titolare, comportando l'obbligo di adozione di misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR, che include anche il principio di necessità (artt. 5, par. 2, e 24, GDPR).

[21] Il Reg. UE n. 679/2016 all'art. 35 introduce l'obbligo di effettuare la valutazione di impatto o *Data Protection Impact Assessment* (DPIA). La DPIA «*is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them*» in GRUPPO DI LAVORO EX ART. 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev. 01, on 13 October 2017.

[22] Sull'importanza del ruolo del principio di necessità in riferimento al principio di *privacy by design* e *by default* si veda EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* on 20 October 2020.

[23] Il Consiglio d'Europa il 28 gennaio 1981 ha emanato la Convenzione 108 del Consiglio d'Europa o anche Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STCE n. 108, 1981, ratificata in Italia con l. 21 gennaio 1989 n. 98.

vincolante[24], che fornisce protezione suppletiva all'ambito europeo, assicurando una pervasiva e uniforme disciplina sulla protezione di dati personali[25].

Orbene, da una prima lettura della Convenzione sembrerebbe che il principio di "necessità" non sia contemplato, né nella sua originaria formulazione, risalente al 1981, né in quella più recente, avutasi a seguito dell'introduzione del protocollo modificativo del 2018. Difatti, analizzando l'originario art. 5 della Convenzione, rubricato «Qualità dei dati»[26], che disciplinava in che modo i dati personali oggetto di elaborazione automatica dovevano essere trattati, parrebbe assente un autonomo ed esplicito riferimento alla "necessità". Altrettanto dicasi per l'attuale formulazione del medesimo articolo della Convenzione 108+, ora rubricato «Legittimità dell'elaborazione dei dati e qualità dei dati», ove s'è abbandonato il riferimento esclusivo all'elaborazione in forma automatica ed è stato ribadito il principio di proporzionalità e l'obbligo del ricorso ad una base giuridica del trattamento, da individuarsi nel consenso o in altra condizione di liceità individuata dalla legge, in sintonia con quanto previsto dall'art. 8 della Carta dei diritti fondamentali dell'UE e dagli artt. 6 e 9 del GDPR.

In entrambe le versioni dell'art. 5 cit., è tuttavia possibile rinvenire un richiamo al principio di necessità all'interno del principio della conservazione dei dati *ex* art. 5, lett. *e)*, della Convenzione, ove il legislatore ha affermato che i dati di carattere personale oggetto di elaborazione automatiche dovranno essere «conservati in una forma che consenta l'identificazione delle persone interessate per un periodo non superiore a quello necessario agli scopi per i quali tali dati sono trattati»[27].

A fronte di ciò, se il legislatore internazionale ha intenzionalmente inserito la "necessità" nello s*tep* finale di gestione del dato (nella determinazione del periodo ultimo di conservazione), si può ritenere ragionevolmente che essa sia insita sin dalla fase iniziale di raccolta del dato.

L'importanza e la forza cogente del principio di necessità è stata recentemente ribadita e rafforzata con l'avvento del citato protocollo di modifica della Convenzione 108 (c.d. Convenzione 108+), con cui, come già precisato, s'è provveduto

---

[24] Agenzia dell'Unione europea per i diritti fondamentali, Consiglio d'Europa, Corte europea dei diritti dell'uomo, Garante europeo della protezione dei dati, *Manuale sul diritto europeo in materia di protezione dei dati personali*, 2018, p. 19.

[25] Si veda il Preambolo della Convenzione 108 in cui il legislatore afferma che lo scopo di tale trattato consiste nel realizzare un'unione «più stretta tra i suoi membri, nel rispetto in particolare della prevalenza del diritto nonché dei diritti umani e delle libertà fondamentali» ed ancora, sempre nel Preambolo, si prevede che gli Stati firmatari di tale Convenzione riconoscono «la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli».

[26] L'art. 5 della Convenzione 108, nella sua formulazione originaria, prevedeva che «I dati a carattere personale oggetto di elaborazione automatica devono essere: *a)* ottenuti ed elaborati lealmente e legalmente; *b)* registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini; *c)* adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati; *d)* esatti e, se necessario, aggiornati; *e)* conservati sotto una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati».

[27] Cfr. art. 5, par. 4, lett. *e)*, Conv. 108+, di contenuto analogo all'art. 5, par. 1, lett. *e)*, Conv. 108 del 1981.

ad estendere anche ai trattamenti non automatizzati la disciplina della Convenzione e, al contempo, s'è provveduto ad aggiornare l'impianto normativo al fine di tener conto sia del progresso tecnologico, sia delle più recenti soluzioni normative adottate dall'UE con il GDPR[28].

Grazie al processo di modernizzazione di tale Convenzione, il legislatore internazionale ha recepito nuovi principi, previsti nel GDPR, come quello di minimizzazione e di *privacy by design* e *by default*, lasciando più ampi margini all'applicazione del principio di necessità. Si consideri, ad esempio, l'art. 10, par. 2, della Convenzione 108+, rubricato «*Ulteriori aggiuntivi*», ove il titolare del trattamento e il responsabile, prima di iniziare la raccolta del dato, deve prevenire o ridurre al minimo il rischio di interferenza con i diritti e le libertà fondamentali dell'interessato: ma per ottenere tale risultato occorrerà che venga svolto un *test* di effettiva "necessità" del trattamento, valutando anche il bilanciamento tra l'interferenza causata dal trattamento (posto in essere dal titolare per il raggiungimento di finalità legittime) e i diritti fondamentali dell'interessato (che il trattamento rischia di comprimere)[29].

2. Portata del principio

2.1. Il principio di necessità nel Codice della *privacy*

Come si è già avuto modo di rimarcare, il principio di necessità al trattamento dei dati trovava collocazione nell'ordinamento italiano all'art. 3 del Codice della *privacy*[30], secondo il quale «i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità».

Prima di analizzare nel dettaglio tale norma, è opportuno comprendere il contesto normativo nel quale essa viene inserita.

Com'è noto, il legislatore italiano, nell'accordare ampia tutela con riguardo alla protezione dei dati personali, ha preso in debita considerazione anche i tratta-

[28] Il Comitato dei ministri del Consiglio d'Europa ha portato a termine il processo di modernizzazione della Convenzione 108 con il Protocollo di Modifica del 18 maggio 2018, noto come Conv. 108 + STCE n. 223, ratificato dall'Italia il 5 marzo 2019.

[29] L'art. 10, par. 2, Conv. 108+ stabilisce, testualmente, che «Ciascuna Parte dispone che i titolari del trattamento e, se del caso, i responsabili del trattamento, esaminino il probabile impatto dell'elaborazione dei dati prevista sui diritti e le libertà fondamentali delle persone interessate prima dell'inizio di tale trattamento e definiscano il trattamento dei dati in modo da prevenire o minimizzare il rischio di interferenze con tali diritti e libertà fondamentali». Sul punto si rinvia, *amplius*, al par. 2.4. del presente capitolo.

[30] Tale articolo è stato abrogato dal d.lgs. 10 agosto 2018, n. 101 recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE».

menti di dati personali effettuati dal titolare attraverso *software*, *database*, *computer* e altri dispositivi interconnessi in reti di comunicazioni sempre più complessi. Tali sistemi informatici possono portare, tra l'altro, alla costruzione di enormi archivi digitali di dati che incrementano esponenzialmente i rischi per i diritti e le libertà dell'interessato, soprattutto laddove tali dati dovessero essere successivamente utilizzati per finalità diverse rispetto a quelle sussistenti al momento della raccolta.

Pertanto, per contenere tali rischi, il legislatore aveva introdotto, con l'art. 3 (poi abrogato) del Codice, una norma che fosse in grado di tutelare *ex ante* l'interessato, riducendo al minimo l'utilizzazione dei suoi dati mediante sistemi informativi e programmi informatici, qualora le modalità d'uso di tali tecnologie non dovessero risultare "necessarie"[31] in relazione alle finalità di trattamento legittimamente perseguite. Tale norma conteneva un principio, di natura innovativa[32], dotato di rilevanza autonoma[33], messo in risalto anche dalla rubrica dell'articolo, intitolata appunto «*Principio di necessità nel trattamento dei dati*».

Si tratta di un principio destinato a fronteggiare la rapida obsolescenza normativa delle regole di dettaglio di fronte all'incessante progresso tecnologico degli strumenti informatici[34], facendo in modo che venga recepito come "principio normativo", ciò che in realtà sia da considerarsi, prima ancora, un «principio di buon senso»[35].

Quella di cui all'art. 3 del Codice della *privacy* è norma di rango primario e di ordine generale[36], la cui forza cogente si rinviene già dalla sua collocazione all'inter-

---

[31] In verità, l'art. 3 del Codice della *privacy* è stato riferito dalla dottrina sia ai sistemi informatici, che a qualunque strumento e/o procedura anche non informatizzata. Cfr. G. D'Orazio, *Protezione dei dati by default e by design*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano 2016, p. 79; N. Miniscalco, *Uno, nessuno o centomila? Minimizzazione e privacy by default nel primo provvedimento del Garante dopo il GDPR*, in *Dir. inf.*, 2018, 4-5, p. 782.

[32] La dottrina è concorde nell'affermare che il «principio di necessità» sia un «principio» di carattere "innovativo". *Ex multiis*: A. Del Ninno, *La Tutela dei dati personali. Guida pratica al codice della privacy (d.lg. 30.6.2003, n. 196)*, Padova, 2006, p. 23; G. Buttarelli, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, in C.M. Bianca-D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno, 196 ("Codice della privacy")*, cit., p. 33.

[33] Con riguardo alla rilevanza del «principio di necessità», Rodotà ha affermato che tale principio «non individua soltanto un preciso limite alle attività dei soggetti pubblici e privati, ma indica un essenziale criterio per l'accettazione istituzionale delle tecnologie e dell'informazione e della comunicazione» (S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, in *Eur. e dir. priv.*, 2004, 1, p. 7).

[34] Cfr. G. Buttarelli, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., pp. 32 e 33.

[35] Cfr. F. Modafferi, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu.com, 2015, p. 122.

[36] Si tratta di una norma di carattere generale che è stata mutuata dalla legislazione tedesca: si rinviene all'art. 3(a) del *Bundesdatenschutzgesetz* tedesco del 2001, ove si prevede «Parsimonia e misura nell'utilizzo dei dati personali. La configurazione e la scelta di sistemi di elaborazione dati devono avere come obiettivo quello di evitare o ridurre quanto più possibile la raccolta, il trattamento o l'utilizzazione di dati personali. In particolare, occorre fare uso delle opportunità all'anonimizzazione e dalla pseudonimizzazione nella misura in cui ciò sia possibile ed il loro impiego risulti proporzionato alle finalità di protezione perseguite». Cfr. Relazione Parlamentare di accompagnamento al testo del "Codice in materia di protezione dei dati personali", p. 7; G. Buttarelli, *Comm. art. 3*

no della «terna dei tre *top principle*»[37]. Il legislatore aveva inserito intenzionalmente il «principio di necessità» nella Parte I («Disposizioni generali») del Titolo I («Principi generali») del Codice, accanto al diritto fondamentale di protezione dei dati personali[38] e alle finalità del Codice[39], proprio per sottolineare la sua portata generale e la sua rilevanza sistematica[40]. Efficacemente s'è detto che con «il principio di necessità, il legislatore ha in sostanza codificato nella protezione dei dati il principio di precauzione che si affaccia in altri contesti normativi»[41].

Orbene, rileggendo il Codice della *privacy* si può facilmente rilevare come la locuzione «necessità» (o «necessario») venga più volte utilizzata dal legislatore, non solo all'art. 3, ma anche in altre disposizione, come quelle rese in tema di condizioni

(Principio di necessità nel trattamento dei dati), cit., p. 34; D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali*, cit., p. 20, nota 6.

37 Cfr. G. BUTTARELLI, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., p. 33.

38 Nel Codice della *privacy*, antecedentemente alla riforma del 2018, il diritto di protezione dei dati personali era enunciato all'art. 1, che riproduceva alla lettera il primo comma dell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea: «Chiunque ha diritto alla protezione dei dati personali che lo riguardano». L'art. 3 del Codice è stato modificato dal d.lgs. 10 agosto 2018, n. 101 nel seguente modo: «il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito "Regolamento", e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona».

39 Le «finalità» del Codice in materia di protezione dei dati personali erano previste all'art. 2, ove si trovava affermato che: «1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. 2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento». Oggi tale articolo, per esigenze di coordinamento con il GDPR, è stato sostituito dal d.lgs. 10 agosto 2018, n. 101 nel seguente modo «il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento».

40 Sulla collocazione sistematica del «*Principio di necessità*» nel Codice della *privacy* è stato significativamente rimarcato come il legislatore italiano avesse voluto «sottolineare non solo la sua propedeuticità rispetto a molti altri canoni basilari della protezione dei dati, ma, soprattutto, il suo valore portante e significativo di un più ampio approccio di tutela sostanziale che il Codice intende offrire anche in via preventiva: una guida innovativa per gli operatori che guarda all'innovazione tecnologica (...)». Così G. BUTTARELLI, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., p. 33.

41 Cfr. G. BUTTARELLI, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., p. 33.

di liceità del trattamento dei dati personali comuni[42] e sensibili [43] diverse dal consenso dell'interessato, nonché in ambito di trasferimenti dei dati all'estero[44].

Si tratta, in verità, di concetti completamente distinti, che portano ad evidenziare come il principio di necessità assuma significati differenti a seconda dei molteplici ambiti in cui viene declinato.

Infatti, il principio di "necessità", con riguardo al trattamento dei dati, esprime il principio di "precauzione" in relazione alle modalità ed ai mezzi del trattamento, sicché, prima di procedere al trattamento dei dati personali attraverso sistemi informatici, si dovrà verificare se tale trattamento possa essere ridotto al minimo, prediligendo, in tutti quei casi in cui le finalità del trattamento non richiedano o impongano un trattamento di dati personali, l'utilizzazione di dati anonimi o di opportune modalità che consentano di non identificare l'interessato, nonché, in ogni caso, un'apposita "configurazione" dei sistemi informatici con riduzione al minimo dell'utilizzazione di dati personali e identificativi.

Altro significato assume il principio di "necessità" ancorato alle condizioni di liceità del trattamento diverse dal consenso dell'interessato: anche qui la norma si colloca in un momento precedente a quello della raccolta del dato, ma il principio in parola si discosta dal principio di minimizzazione, perché in quest'ultimo la "necessità" del trattamento è rapportata alle finalità perseguite, mentre, con riguardo alla condizione di liceità diversa dal consenso, la "necessità" del trattamento è rapportata al presupposto legittimo del trattamento come individuato *ex lege*, a prescindere dalle finalità concretamente perseguite dal titolare. In quest'ultimo contesto, infatti, viene ad essere applicato al fine di valutare l'aderenza o meno del trattamento rispetto

[42] Ci stiamo riferendo all'art. 24 del Codice della *privacy*, rubricato «*Casi nei quali può essere effettuato il trattamento senza consenso*», poi abrogato dal d.lgs. 10 agosto 2018, n. 101. Il legislatore disciplinava, ivi, i casi in cui il titolare poteva effettuare un trattamento legittimo senza il consenso dell'interessato, ovvero quando tale trattamento fosse necessario per adempiere a un obbligo di legge, di un regolamento e norma comunitaria [lett. *a)*]; per eseguire obblighi derivanti da un contratto [lett. *b)*]; per salvaguardare la vita o l'incolumità fisica di un terzo [lett. *c)*]; per investigazioni difensive *ex* l. 7 dicembre 2000, n. 397 o per far valere o difendere un diritto in sede giudiziaria [lett. *f)*]; in altri casi individuati dal Garante [lett. *g)*]; per scopi scientifici o statistici o storici presso archivi privati [lett. *i)*].

[43] L'art. 26 del Codice della *privacy*, anch'esso abrogato dal d.lgs. 10 agosto 2018, n. 101, disciplinava le garanzie per i dati sensibili, prevedendo, al co. 4, che questi potessero essere oggetto di trattamento, senza il consenso dell'interessato, in specifiche ipotesi di eccezione, come ad esempio qualora il trattamento fosse necessario per la salvaguardia della vita o dell'incolumità di un terzo [lett. *b)*], oppure per le investigazioni difensive *ex* l. 7 dicembre 2000, n. 397 o per far valere o difendere un diritto in sede giudiziaria [lett. *c)*] o, ancora, per adempiere a specifici obblighi o compiti previsti dalla legge [lett. *d)*].

[44] L'art. 43 del Codice della *privacy*, anch'esso abrogato dal d.lgs. 10 agosto 2018, n. 101, individuava le ipotesi in cui erano consentiti i trasferimenti in Paese terzi dei dati personali oggetto di trattamento, ovvero quando il trasferimento fosse *necessario* per l'esecuzione di obblighi derivanti da un contratto [lett. *b)*], oppure per la salvaguardia dell'interesse pubblico [lett. *c)*], della vita o dell'incolumità fisica di un terzo [lett. *d)*], per investigazioni difensive *ex* l. 7 dicembre 2000, n. 397 o per far valere o difendere un diritto in sede giudiziaria [lett. *e)*] e infine scopi scientifici o statistici o storici presso archivi privati [lett. *g)*].

alla condizione di liceità ovvero al fondamento legittimo previsto per il trattamento dei dati personali, svincolandolo dalle finalità del trattamento.

Analogo discorso vale con riguardo al trasferimento dei dati nei Paesi terzi, ove l'art. 43 del Codice, nel testo precedente alla riforma del 2018, richiedeva che il trattamento avvenisse con il consenso dell'interessato o che fosse comunque "necessario" in relazione ai presupposti legittimi (ovvero, alle condizioni di liceità) ivi previsti[45].

L'art. 3 del Codice è una norma impersonale[46], nella quale non vengono esplicitamente identificati i soggetti attivi tenuti a rispettare il «principio di necessità» ivi delineato. Infatti, la norma genericamente si riferisce ai mezzi di trattamento dei dati personali (ovverosia «i sistemi informativi e i programmi informatici sono configurati…»), utilizzando un costrutto in forma passiva, nel quale non trovano menzione i destinatari dell'obbligo in essa contenuto. Si può tuttavia ritenere che il principio sia rivolto a un'ampia platea di soggetti[47]. Tra questi rientrano certamente chi tratta o chi intende trattare i dati, individuando finalità, mezzi e modalità del trattamento, ossia il titolare del trattamento, nonché chi è da questi preposto a trattare i dati personali, ossia il responsabile del trattamento.

Si ritiene, tuttavia, che l'osservanza del principio di necessità – così come delineato nel Codice della *privacy* – dovesse inevitabilmente essere rispettata anche da altri soggetti che, pur non trattando direttamente i dati personali, si ponevano comunque in rapporto con gli strumenti tecnologici di trattamento, incidendo sulle loro funzionalità tecniche, in sede di realizzazione, di implementazione o di controllo. Ci stiamo riferendo ai produttori ed ai programmatori di *software* e *hardware* e agli organismi di certificazione ed alle associazioni rappresentative, che nello svolgimento della loro attività sarebbe opportuno che si interrogassero, prima di consegnare il prodotto al titolare del trattamento, se questi sia conforme e corrispondente al principio di necessità[48].

Pertanto, secondo un'interpretazione estesa (che pone tuttavia grandi problemi in sede applicativa), non solo il titolare ed il responsabile del trattamento, ma anche i produttori e i programmatori degli strumenti tecnologici usati per il trattamento dei dati erano chiamati a svolgere, *ex* art. 3 del Codice della *privacy*, una valutazione preventiva per verificare il rispetto del principio di necessità. In tale prospettiva, la rilevanza normativa del principio di necessità, anche alla luce della disciplina in materia di sicurezza adottata del trattare i dati personali, imponeva che il titolare del trattamento dovesse richiedere al fornitore il rilascio di un'apposita dichiarazione di conformità dei prodotti, con conseguenti ripercussioni sul regime di responsabilità in caso di non corrispondenza.

Occorre rimarcare che il principio di cui si tratta opera inevitabilmente in tutte le fasi del trattamento ed infatti qualora, per qualsiasi ragione, il trattamento dei dati

---

[45] Cfr., *supra*, nota n. 45.

[46] *Ex multis*: G. BUTTARELLI, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., p. 34; D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali*, cit., p. 20.

[47] L'interpretazione estensiva è proposta da G. BUTTARELLI, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., p. 34.

[48] Cfr. G. BUTTARELLI, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., p. 34.

si discostasse dal principio di necessità in una fase successiva a quella di iniziale raccolta dei dati, ci troveremo di fronte a un trattamento illecito di dati.

Pertanto, ai sensi della disposizione in esame il titolare del trattamento non si doveva limitare a verificare se il trattamento dei dati fosse stato eseguito in conformità al principio di necessità, ma avrebbe dovuto controllare che quest'ultimo venisse rispettato anche nella fase di conservazione dei dati dell'interessato e, in generale, in tutte le fasi e operazioni di trattamento.

Alla luce di quanto sin qui detto, c'è da chiedersi cosa comporti l'eventuale violazione o la mancata applicazione del principio di necessità di cui all'art. 3 cit.

Nel Codice della *privacy* non vi era alcuna norma che sanzionasse espressamente tale violazione, né sul piano penale, né su quello amministrativo. Tuttavia, secondo concorde dottrina, il principio di necessità di cui all'art. 3 del Codice si poneva quale obbligo giuridico inserito in una norma imperativa, sicché la sua violazione si collocava senz'altro nella sfera dell'illiceità e, al di là dell'eventuale rilievo sul piano risarcitorio, avrebbe potuto comportare la comminazione anche di una sanzione penale qualora si ricollegasse, sul piano sistematico, ad altre disposizioni idonee a tipizzare l'illecito (come ad esempio quelle previste in materia di trattamento di dati sensibili, che, sotto l'egida del Codice, dovevano essere trattati, fra l'altro, anche sulla base di un'autorizzazione del Garante)[49].

L'importanza prescrittiva del principio, infatti, è stata sottolineata espressamente dal Garante per la protezione dei dati personali nelle varie autorizzazioni generali, nelle quali ha inserito un'apposita indicazione relativa al rispetto del principio di necessità di cui all'art. 3 del Codice[50]. A tal riguardo, l'Autorità garante aveva evidenziato come il mancato rispetto del principio di necessità comportava l'adozione da parte della stessa autorità di provvedimenti di natura correttiva, volti a sospendere e/o a bloccare i trattamenti considerati "non necessari" e a rendere i dati raccolti dal titolare inutilizzabili[51].

---

[49] Cfr. G. Buttarelli, *Profili generali del trattamento dei dati personali*, in G. Santaniello (a cura di), *La protezione dei dati personali*, in *Trattato di diritto amministrativo*, Padova, 2005, vol. XXXVI, pp. 78-79; G. Buttarelli, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., pp. 35 e 36, il quale aveva rilevato che il principio di necessità era comunque richiamato nelle autorizzazioni generali rese ai sensi dell'originario art. 26, par. 2, del Codice e che pertanto, almeno per i trattamenti rientranti nell'ambito di applicazione di tali autorizzazioni, la sua violazione avrebbe comportato l'applicazione della sanzione penale, ai sensi dell'originario art. 170 del Codice (che puniva come reato l'inosservanza dei provvedimenti del Garante, incluse le autorizzazioni), anche se, precisava l'A., «non è la dimensione penale che dovrebbe fungere da traino per una sentita attuazione di questo tipo di *privacy enhancing technology*» (*Ibidem*).

[50] Il Garante per la protezione dei dati personali ha sempre ritenuto, sotto la vigenza della norma ora in esame, che il trattamento dei dati con sistemi informativi e programmi informatici dovesse essere configurato nel rispetto del principio di necessità di cui all'art. 3 del Codice della *privacy*. *Ex multiis* si vedano le autorizzazioni pubblicate in G.U. n. 190 del 14 agosto 2004; G.U. n. 196 del 24 agosto 2007 e G.U. n. 303 del 29 dicembre 2016.

[51] Infatti, il Garante, tra i vari provvedimenti, ha vietato, ai sensi dell'art. 154, co. 1, lett. *d)*, del Codice, che il datore di lavoro effettuasse un trattamento dei dati sui propri dipendenti per mere finalità di controllo degli stessi durante lo svolgimento del rapporto di lavoro. Ad esempio, con riferimento ai dati biometrici il Garante ha vietato l'uso della biometria – nel caso di specie si trattava di un sistema di rilevazione di impronte digitali – per mere finalità di accertamento della presenza sul

S'è però già chiarito che il principio di necessità operava nell'impianto del Codice anche con riferimento alle condizioni di liceità alternative al consenso e, in modo analogo, pure per i trasferimenti di dati verso Paesi terzi, sicché la violazione del principio di necessità in tali contesti avrebbe potuto comportare le sanzioni previste per violazione degli artt. 24 e 43 del Codice, in quanto, in tali casi, la violazione del principio di necessità finiva per essere inquadrata come violazione dei presupposti di liceità del trattamento.

Le disposizioni sopra considerate, contemplanti il principio di necessità (artt. 3, 24 e 43 del Codice), come noto, sono state abrogate dal legislatore con l'emanazione del d.lgs. n. 101/2018[52], che ha adeguato la normativa nazionale all'entrata in vigore del GDPR. Occorre pertanto indagare in quale misura l'assetto normativo previsto dal Codice della *privacy* sul principio di necessità sia sopravvissuto nella normativa europea e in quali norme lo ritroviamo.

2.2. (*segue*): Rapporto tra principio di necessità e principio di pertinenza e non eccedenza nel Codice della *privacy*: endiadi o duplicazione?

Alla luce di quanto sin qui detto, è doveroso prendere in considerazione anche il rapporto che sussiste tra il principio di necessità e quello di pertinenza e non eccedenza.

Ebbene, quest'ultimo era previsto all'art. 11, lett. *d)*, del Codice della *privacy* e prevedeva che il trattamento dei dati personali dovesse essere, oltre che volto a "minimizzare" l'utilizzazione dei dati personali, anche pertinente, completo e non eccedente rispetto alle finalità per le quali i dati medesimi sono raccolti o trattati[53].

Pertanto, alla luce di tale definizione, occorre domandarsi se, nell'impianto del Codice, il principio di pertinenza e non eccedenza costituisse un'endiadi o una duplicazione del principio di necessità, ciò anche al fine di trarre elementi interpretativi utili per la lettura critica delle successive norme contenute nel GDPR.

---

posto di lavoro e dei tempi di lavoro del dipendente. Cfr. GPDP, Provv. 15 ottobre 2009, doc. *web.* n. 1664257 (v. anche GPDP, Provv. 21 luglio 2005, doc *web.* n. 1150679). Ed ancora il Garante ha vietato, ai sensi dell'art. 154, co. 1, lett. *c)* e *d)*, del Codice, a una società l'utilizzo di dati per finalità di *marketing* sia degli utenti non iscritti al sito sia degli utenti che si erano cancellati dalla *mailing list*, in quanto tale condotta risultava contraria al principio di necessità. Cfr. GPDP, Provv. 20 luglio 2017, doc. *web*. n. 6955363.

[52] Il d.lgs. 10 agosto 2018, n. 101 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE n. 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) è stato pubblicato in G.U. Serie Generale n. 205 del 4 settembre 2018.

[53] Anche l'art. 11 del Codice della *privacy* è stato abrogato dal d.lgs. 10 agosto 2018, n. 101. Tuttavia, quanto in esso riportato – ed in particolare, ai fini del nostro discorso, la previsione di cui alla lett. *d)*, concernente i requisiti di pertinenza, completezza e non eccedenza dei dati rispetto alle finalità della loro raccolta e del loro successivo trattamento – si trova trasposto, seppur in parte, nei contenuti dell'art 5, lett. *c)*, GDPR: la pertinenza e la non eccedenza, segnatamente, divengono elementi o canoni del principio di «minimizzazione» dei dati.

A ben vedere, analizzando la portata applicativa dei due principi, si può pacificamente affermare che il principio di pertinenza e non eccedenza costituiva e/o costituisce un corollario del principio di necessità.

A tal proposito nella Relazione Parlamentare di accompagnamento al testo del Codice in materia di protezione dei dati personali, il legislatore ha chiaramente affermato che i due appena citati principi non possono considerarsi una mera duplicazione, difatti il principio di necessità di cui all'art. 3 del Codice «integra e completa, con riferimento alla configurazione stessa dell'ambiente in cui i dati sono trattati, il principio di pertinenza e non eccedenza dei dati trattati già operante in relazione al trattamento dei medesimi dati»[54].

Il principio di pertinenza e non eccedenza costituisce un'endiadi del principio di necessità, difatti se i dati personali dell'interessato non sono più "necessari" al titolare per perseguire le finalità del trattamento, questi non potrà continuare la sua attività, in quanto i dati trattati risulterebbero non pertinenti, incompleti ed eccedenti rispetto allo scopo del trattamento[55].

Il principio di pertinenza e non eccedenza continua a costituire un'endiadi del principio di necessità anche nella disciplina europea, e più precisamente all'art. 5 del Reg. UE n. 679/2016. La portata applicativa del principio di necessità nell'attuale disciplina in materia di protezione dei dati personali, tuttavia, si colloca in un ambito più ampio, che meglio si coglie nell'impianto del nuovo regolamento europeo (GDPR).

2.3. Il principio di necessità alla luce del GDPR

In materia di protezione dei dati personali il Reg. UE n. 679/2016 ha adottato un approccio differente rispetto al d.lgs. n. 196/2003[56], ad iniziare dalla responsabilizzazione del titolare del trattamento (*accountability*)[57].

Entrambe le discipline sono incentrate sulla tutela del diritto alla protezione dei dati personali quale diritto fondamentale dell'interessato, in cui si sostanzia l'accezione moderna del diritto alla *privacy*, originariamente inteso come "diritto di esser lasciato solo"[58]. Tuttavia, nel nuovo regolamento europeo è profondamente cambiato, tra l'altro, il rapporto tra *privacy* e libera circolazione dei dati, nonché il grado di coinvolgimento del titolare nell'applicazione della disciplina normativa in esso delineata, come ben si evince anche dall'introduzione della figura del responsa-

[54] Cfr. Relazione Parlamentare di accompagnamento al testo del Codice in materia di protezione dei dati personali, commento all'art. 3 del Codice della *privacy*.

[55] Cfr. F. Modafferi, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, cit., p. 134.

[56] Cfr. C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, 2018, *passim*.

[57] Com'è noto, il Reg. UE n. 679/2016 pone l'accento sulla responsabilizzazione del titolare del trattamento, ovvero sull'obbligo di adottare misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato in maniera conforme al regolamento medesimo. Cfr. artt. 5, par. 2, e 24, GDPR.

[58] Cfr. S. Warren-L. Brandeis, *The right to privacy*, in *Harvard Law Review*, Boston (MA), 1890, p. 205.

bile della protezione dei dati, a supporto del titolare e del responsabile del trattamento per assicurare il rispetto della medesima.

Come già s'è avuto modo di precisare, il GDPR, pur non effettuando alcun autonomo ed esplicito riferimento al «principio di necessità», incardina su di esso l'intero impianto normativo, a tal punto che tale principio finisce per costituire parte integrante e imprescindibile dell'intero GDPR.

Il principio di necessità rappresenta dunque l'elemento essenziale del principio dell'*accountability*, dato che, nella corretta attuazione del regolamento ai sensi degli artt. 5, par. 2, e 24 GDPR, il titolare del trattamento non può prescindere dall'applicazione del principio di necessità: la valutazione in ordine alla "necessità" del trattamento, in altre parole, accompagna il titolare del trattamento in ogni scelta preventiva che compirà nello svolgimento della propria attività di trattamento dei dati personali.

Nel GDPR, infatti, troviamo numerosi riferimenti – più o meno impliciti – al principio di necessità, nell'ambito di specifiche disposizioni normative, tra le quali possono annoverarsi, ad esempio, quelle relative al principio di minimizzazione dei dati (art. 5, par. 1, lett. *c)*, GDPR), agli obblighi in tema di *privacy by design* e *by default* (art. 25, GDPR), alla valutazione di impatto (art. 35, par. 7, GDPR), alle condizioni di liceità del trattamento alternative al consenso (artt. 6 e 9, GDPR), nonché, in via generale, quelle che impongono un bilanciamento tra diritto alla protezione dei dati e libera circolazione (art. 1, par. 3, GDPR).

2.4. (*segue*): Il principio di necessità nel bilanciamento tra diritto alla protezione dei dati e libera circolazione degli stessi (art. 1, par. 3, GDPR)

Il «principio di necessità» in materia di protezione dei dati personali ha, nel GDPR, una portata applicativa ampia, perché si pone alla base del procedimento che porta al bilanciamento proporzionale tra il diritto alla protezione ai dati personali e la libera circolazione dei dati[59].

Ai sensi dell'art. 1, par. 3, GDPR, il diritto alla protezione del trattamento dei dati personali di persone fisiche non può limitare né vietare la libera circolazione dei dati nell'Unione Europea[60].

---

[59] Per un commento v. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 210 ss.; nonché F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, n. 1, pp. 190-216.

[60] Cfr. artt. 8 e 52 Carta dei diritti fondamentali e *considerando* n. 4 GDPR (ove il legislatore ha precisato che «Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»). Anche nella Dir. 95/46/CE all'art. 1, par. 2, si affermava che «Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1», ovvero il diritto al trattamento dei dati personali. Si tenga anche presente che l'obiettivo di tale norma era quello di armonizzare la tutela dei diritti e delle libertà fondamentali rispetto alla libera circolazione dei dati personali. Quanto appena affermato trova riscontro anche al *considerando* n. 3 GDPR.

Per come è strutturata, tale norma potrebbe dare l'impressione che la libera circolazione costituisca una priorità gerarchica rispetto al diritto alla protezione dei dati personali.

Se venisse intesa in tal modo, si potrebbe affermare che il principio di necessità – nella sua veste di principio posto a tutela del diritto alla protezione dei dati – perderebbe la sua portata cogente, facendo inevitabilmente soccombere il diritto alla protezione dei dati di fronte alla libera circolazione dei dati medesimi.

Invero, si tratterebbe di un palese errore di approccio metodologico[61]. Difatti la norma, se fosse strutturata in tal modo, andrebbe inevitabilmente a scardinare l'intero assetto normativo previsto dalla clausola generale di limitazione di cui all'art. 52, par. 1, della Carta dei diritti fondamentali[62].

L'art. 52 della Carta prevede che eventuali limitazioni all'esercizio dei diritti per essere legittime possano essere disposte – nel rispetto del principio di proporzionalità[63] – e apportate solamente laddove siano "necessarie" e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Ciò significa che la libera circolazione dei dati può limitare il diritto di protezione dei dati personali, purché tale limitazione sia giustificabile (*rectius* proporzionale) e, prima ancora, *necessaria* rispetto alla misura e agli obiettivi utilizzati.

Ne consegue che il titolare del trattamento nell'ambito della sua attività dovrà, prima di iniziare la raccolta dei dati, bilanciare i due diritti già indicati.

Per far questo, dovrà verificare se la limitazione del diritto alla protezione dei dati («sottoposto a limitazione») – nella misura del principio di *necessità* – sia in qualche modo proporzionata rispetto alla libera circolazione («avente portata limitante»).

Per compiere tale valutazione, sarà indispensabile che il titolare del trattamento proceda all'analisi della "necessità"[64] e della "proporzionalità" del trattamento[65].

---

[61] Cfr. F. Bravo, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 210.

[62] Cfr. F. Bravo, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 210-212.

[63] Per principio di proporzionalità nell'ambito dell'Unione Europea si intende un principio di portata generale secondo cui la limitazione del diritto deve essere giustificata. Per una completa analisi del principio di proporzionalità si segnala: EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, on 19 Aprile 2019.

[64] Per una completa analisi del principio di necessità in ambito europeo si segnala: EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit,* 11 April 2017. Degno di nota risulta il passo in cui l'EDPS precisa che «*The necessity test should be considered as the first step with which a proposed measure involving the processing of personal data must comply. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure which is not proven to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity: in other words, necessity is a pre-condition for proportionality*» (*Ibidem*, p. 10).

[65] Cfr. nota 70.

Con riguardo al requisito della "necessità", si dovrà *in primis* verificare quale sia la misura (e/o lo strumento) che permetta al titolare di ridurre al minimo l'utilizzo dei dati personali. Una volta individuata tale misura si dovrà procedere a una descrizione fattuale della stessa[66] per poi verificare se costituisca una limitazione al diritto di protezione dei dati personali[67] e, se così fosse, si dovranno definire gli obiettivi di tale misura[68] per poter scegliere l'opzione più efficace e meno invasiva[69].

---

[66] L'EDPS individua gli otto *step* per il test di necessità e di proporzionalità. Con riguardo al primo, l'EDPS precisa che «*Step 1 is preliminary; it requires a detailed factual description of the measure proposed and its purpose, prior to any assessment*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 8. Ai fini della descrizione fattuale della misura, ci spiega l'EDPS che *in primis* si dovrà verificare se la misura scelta implichi l'utilizzo dei dati personali e se così fosse bisognerà provvedere a descriverne la consistenza fattuale, ovvero «*the objective of general interest pursued by the measure; the exact purpose of the processing of personal data, explained in more detail than the objective; the categories of data; the persons whose data are processed (e.g. passengers, workers, migrants); who is processing and accessing the data (e.g. a private company, a public organisation); which processing operations are envisaged (e.g. collection, storage, access, transfer); any other relevant provisions, such as the duration of processing*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 10.

[67] Al riguardo è stato rimarcato che lo «*Step 2 will help identify whether the proposed measure represents a limitation on the rights to the protection of personal data or respect for private life (also called right to privacy), and possibly also with other rights*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 8. Dopo aver verificato che la misura implichi l'utilizzo dei dati personali, bisognerà verificare se essa costituisca una limitazione al diritto alla protezione dei dati. Per far questo, si dovrà identificare quali sono i diritti e le libertà fondamentali oggetto di limitazione. Una volta individuati si valuterà se e in che modo possa essere identificata una "differenza di trattamento" tra il diritto limitato e il diritto limitante e a quali conseguenze ciò potrebbe portare. A tal proposito, l'EDPB precisa che «*If the essence of the right is adversely affected by the measure, then the limitation is not lawful and the measure should be withdrawn or modified before proceeding to the next steps*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 12.

[68] Così lo Step 3 «*considers the objective of the measure against which the necessity of a measure should be assessed*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 8. Per poter scegliere gli obiettivi della misura bisognerà valutarne la legittimità, ovvero «*Identify and assess the legitimacy of the aim pursued by the measure: o Make sure that the problem is sufficiently and clearly described in the measure; o Integrate sufficient and scientifically verifiable evidence supporting the existence of the problem; o Define precisely the objective of general interest or the right of others which the measure seeks to address; o Make sure that the purpose of the processing of personal data genuinely aims to achieve an objective of general interest recognised by the Union or the need to protect the rights and freedoms of others; o Explain the importance of the objective to be achieved and how it is critical for the functioning of society*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 15.

[69] Così, lo Step 4 «*provides guidance on the specific aspects to address when performing the necessity test, in particular that the measure should be effective and the least intrusive*». Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 8. L'individuazione dell'opzione più efficace e meno invasiva è sottoposta ad una valutazione volta a determinare se la misura considerata sia essenziale (necessaria) a soddisfare il bisogno da affrontare. Ciò può verificarsi sia quanto le misure esistenti risultino insufficienti per il raggiungimento di obiettivi legittimamente perseguiti, sia quando la misura da adottare risulti ne-

Una volta conclusa la fase preliminare volta a verificare la "necessità" della misura limitante, si dovrà valutare la sua "proporzionalità" attraverso un procedimento articolato in diversi *step*, valutando, dapprima, se la misura soddisfi gli obiettivi perseguiti[70] e quale sia la portata, l'estensione e l'intensità delle interferenze prodotte sul diritto fondamentale antagonista, che va a limitare[71]. Successivamente, il test di proporzionalità richiede che si proceda con il bilanciamento dei diritti e delle libertà da contemperare (diritto alla protezione dei dati personali e libera circolazione degli stessi) al fine di individuare la soluzione che imponga il minor sacrificio possibile per il diritto fondamentale sottoposto a limitazione e che pertanto possa dirsi "proporzionata"[72]. Se così non fosse, il titolare dovrà introdurre tutta una serie di misure, accorgimenti e clausole di salvaguardia che limitino il trattamento dei dati da parte del titolare o del responsabile e, allo stesso tempo, tutelino i diritti e le libertà fondamentali dell'interessato[73]. Dovrà cioè raggiungere le finalità di trattamento imponendo il minor sacrificio possibile per i diritti e le libertà dell'interessato.

Tra gli strumenti in grado di assicurare il "proporzionale" bilanciamento degli interessi effettuato a seguito del vaglio preliminare di "necessità", possono essere annoverati anche quelli che, nel settore del trasferimento dei dati all'estero in Paesi extra UE, garantiscono un adeguato livello di protezione dei dati *ex* art. 46, par. 2, lett. *c)*, GDPR, quali le c.d. *standard contractual clauses*[74].

---

cessaria per il loro raggiungimento. Cfr. EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 18.

[70] L'EDPB descrive nel dettaglio anche i quattro test di proporzionalità. Di seguito si riportano i contenuti dello Step 1 della proporzionalità «*(or 5 of the overall combined workflow): assess the importance ('legitimacy') of the objective (identified under step 3 of the Necessity Toolkit) and whether and to what extent the proposed measure would meet this objective and addresses the issue identified in the problem definition ("genuinely meets")* [*this would be 'the advantage/benefit'*]». EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., p. 13.

[71] L'EDPS illustra nel modo seguente i contenuti dello Step 2 « *(or 6 of the overall combined workflow): assess the scope, the extent and the intensity of the interference (identified under step 2 of the Necessity Toolkit) in terms of impact on the fundamental rights to privacy and data protection* [*this would be 'the disadvantage/cost'*]». Cfr. EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., p. 13. Per valutare la portata, l'estensione e l'intensità delle limitazioni apportate al diritto fondamentale sottoposto a sacrificio, si dovrà innanzitutto identificare e valutare l'impatto che hanno su di esso.

[72] Si riportano di seguito i contenuti dello «*Step 3 (or 7 of the overall combined workflow): proceed to the fair balance (advantage/disadvantage; benefit/cost) evaluation of the measure».* Cfr. EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., p. 13.

[73] Così viene illustrato il contenuto dello «*Step 4 (or 8 of the overall combined workflow): take a decision ('go/no go') on the measure. If the result is 'no go', taking into account all factors which determined the 14 evaluation as disproportionate, identify and introduce (if possible) safeguards which could make the measure proportionate».* Cfr. EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., pp. 14 ss.

[74] Per un maggior approfondimento della *standard contractual clauses* si veda: la Decisione 2001/497/EC della Commissione Europea del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della Dir. 95/46/CE. Si tratta di una decisione in cui la Commissione ha approvato due set di clausole tipo per il trasferimento di dati personali da titolari del trattamento siti nell'Unione europea verso titolari al di fuori dell'Unione europea o dello

Con riguardo a tali aspetti l'EDPS ha precisato, infatti, che «*Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal.* "Necessity" *is also a data quality principle and a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU data protection secondary law. There is also a link between Article 8(2) of the Chapter and the secondary law, as Article 8(2) refers to the legitimate basis for processing "laid down by law"* (…)»[75].

Alla luce di ciò, si può affermare che nel regolamento europeo il principio di necessità mantiene la sua forza cogente e raggiunge una portata applicativa di carattere generale.

2.5. (*segue*): Principio di necessità e condizioni di liceità del trattamento diverse dal consenso

Anche alla luce di quanto precisato dall'EDPS, appare evidente che il principio di necessità pervade le condizioni di liceità (diverse dal consenso) previste all'art. 6 e all'art. 9 del GDPR[76]. Tali articoli disciplinano, in base all'art. 8, par. 2, della Carta dei diritti fondamentali dell'UE, i "fondamenti" che rendono legittimo il trattamento qualora abbia ad oggetto, rispettivamente, dati personali comuni o quelli appartenenti a categorie particolari. Oltre al consenso dell'interessato[77], il legislatore europeo ha previsto una serie di ulteriori condizioni di liceità, alternative al consenso medesimo, per la cui applicazione si richiede che il trattamento sia «necessario» rispetto al fondamento legittimo indicato *ex lege*. Tali condizioni di liceità effettuano una «selezione degli interessi»[78] rilevanti, secondo logiche di necessità e proporzionalità. L'assenza di tali condizioni di liceità o del rapporto di necessità che deve

Spazio economico europeo. Si veda, inoltre, la Decisione 2010/87/UE della Commissione Europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della Dir. 95/46/CE del Parlamento europeo e del Consiglio decisione. Quest'ultima riguarda l'approvazione da parte della Commissione di un set di clausole tipo per il trasferimento di dati personali da titolari del trattamento siti nell'Unione europea verso responsabili del trattamento al di fuori dell'Unione europea o dello Spazio economico europeo.

[75] EDPS, *Assessing the necessary of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., p. 5.

[76] Sulle condizioni di liceità del trattamento di dati personali nel GDPR si rinvia a F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, pp. 110-193; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, 12, pp. 2783 ss.

[77] Il consenso dell'interessato *ex* art. 6, par. 1, lett. *a),* non richiede da parte del titolare o del responsabile del trattamento una valutazione in ordine alla necessità del trattamento. Sarà onere dell'interessato porre in essere una valutazione di meritevolezza del trattamento a seconda se quest'ultimo rientri nelle finalità predeterminate *ex lege*.

[78] La dottrina sul punto è unanime, si veda F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 126; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, cit., p. 2783.

sussistere tra queste e il contrattamento, esclude a priori la possibilità di qualificare lecito un trattamento.

Ci stiamo riferendo innanzitutto alle ipotesi previste dall'art. 6, par. 1, lett. *b-f)*, del GDPR, ovvero ai casi in cui il trattamento sia necessario: per l'esecuzione di un contrato di cui l'interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso [lett. *b)*]; per adempiere ad un obbligo legale [lett. *c)*]; per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica [lett. *d)*]; per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri [lett. *e)*] ed infine per il perseguimento del legittimo interesse del titolare del trattamento o di terzi [lett. *f)*].

Si tratta di requisiti equipollenti ed alternativi a quello del consenso[79], ma che, allo stesso tempo, possono dirsi disomogenei e non ordinati sistematicamente.

Quello che risulta evidente è che il legislatore ha intenzionalmente predeterminato *ex lege* le condizioni di liceità (diverse dal consenso) in modo da legittimare il trattamento anche nei casi in cui esso abbia un effetto limitante sul diritto alla protezione dei dati, purché tale trattamento sia posto in rapporto di "necessità" e "proporzionalità" con il diritto fondamentale che va a limitare in vista del raggiungimento di finalità legittime, che l'ordinamento considera meritevoli di essere perseguite.

Quanto esposto, trova conferma nell'*Opinion* n. 6/2014 ove il Gruppo di lavoro *ex* Art. 29 si è concentrato sul concetto di «liceità» e sui fondamenti giuridici "necessari" che legittimano il trattamento[80] e dai quali si può dedurre come «il parametro della necessità del trattamento entra dunque a comporre (al di fuori del consenso) la stessa nozione di liceità»[81].

Senza soffermarsi su ognuno dei criteri di liceità, degni di nota risultano quelli relativi alle lett. *b)* ed *f)* dell'art. 6 cit., che sono utili a comprendere il grado di complessità nella valutazione del *test* di "necessità" e "proporzionalità" in cui si potrebbe trovare il titolare del trattamento.

Con riferimento alla nozione di trattamento «necessario all'esecuzione di un contratto stipulato con l'interessato»[82] il Gruppo di lavoro *ex* Art. 29 ha affermato che tale nozione si riferisce alle ipotesi in cui il contratto viene determinato unilateralmente dal titolare del trattamento e certamente «non contempla le situazioni in cui il trattamento non è effettivamente necessario all'esecuzione di un contratto»[83].

---

[79] F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 110-193.

[80] Cfr. Gruppo di lavoro ex Art. 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., pp. 7 ss.

[81] D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, cit., p. 2784.

[82] L'art. 6, lett. *b)*, Reg. cit. considera anche la possibilità che un trattamento possa dirsi necessario non solo per la fase contrattuale, ma anche per quella precontrattuale. Si pensi ad esempio a tutte quelle volte in cui un professionista si trovi a dover eseguire, su richiesta del cliente, un preventivo. In tale occasione, dovranno essere trattati quei dati che abbiamo superato positivamente il *test* di necessità.

[83] Cfr. Gruppo di lavoro ex Art. 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., p. 20. Precisa, inoltre, l'EDPB che «Ai fini della valutazione dell'applicabilità dell'articolo 6, paragrafo 1, lettera b), possono risultare utili le domande riportate di seguito: qual è la natura del servizio fornito all'interessato? quali sono le sue caratteristiche distintive? qual è la ratio esatta del contratto (ossia la sua sostanza e il suo oggetto fondamentale)? quali sono gli elementi essenziali del contratto? quali sono le prospettive

Spiega, difatti, il Gruppo di lavoro che la circostanza che alcuni trattamenti siano fondati su un contratto non implica automaticamente che questi siano oggettivamente indispensabili (*rectius* necessari) alla sua esecuzione.

Per comprendere se il trattamento sia lecito, il titolare deve, quindi, compiere un *test* di necessità: egli dovrà verificare se i dati che andrà a raccogliere siano utili e indispensabili per l'esecuzione del contratto e, se così non fosse, li dovrà ridurre al minimo. Sostanzialmente il titolare dovrà essere in grado di giustificare la necessità di tale trattamento in base alle finalità determinate nel contratto[84].

Anche l'altra condizione di liceità *ex* art. 6, lett. *f)*, relativa al trattamento necessario per il perseguimento di un interesse legittimo, è particolarmente problematica, in quanto si fonda su un concetto (quello di «interesse legittimo») che risulta difficilmente determinabile a priori e che pertanto, proprio per tale ragione, comporta enormi difficoltà sul piano applicativo. Spesso viene utilizzato erroneamente dal titolare per conferire una base giuridica a trattamenti per i quali non abbia provveduto (o non sia stato possibile provvedere) all'acquisizione del consenso degli interessati e non sussistano altre condizioni di liceità.

A fronte dell'introduzione del principio della responsabilizzazione nel GDPR, è in capo al titolare l'onere di valutare la prevalenza di un interesse legittimo, proprio o di un terzo, su altro interesse, diritto o libertà fondamentale, non spettando più al Garante tale preventiva valutazione, come invece richiesto dalla normativa previgente.

Secondo l'*Opinion* 6/2014, ai fini di un lecito trattamento è indispensabile operare un *test* comparativo, ulteriore rispetto a quello della necessità, che valuti la sussistenza dell'interesse legittimo del titolare o dei terzi rispetto a interessi, diritti e libertà fondamentali dell'interessato[85].

Lo svolgimento di tale ulteriore *test* si articola in quattro fasi, nell'ambito delle quali occorre: *a)* valutare l'interesse legittimo[86]; *b)* individuare quali siano i diritti,

---

e le aspettative reciproche delle parti contraenti? Come viene promosso o pubblicizzato il servizio all'interessato? Un utente medio del servizio potrebbe ragionevolmente aspettarsi che, tenuto conto della natura del servizio stesso, il trattamento previsto abbia luogo per l'esecuzione del contratto di cui è parte?». Cfr. EDPB, *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, dell'8 ottobre 2019, pp. 10-11.

[84] Si segnala che per i contratti relativi a servizi digitali il titolare dovrà prestare particolare attenzione alle finalità per cui chiede l'esecuzione. Molte volte, difatti, si esula dal campo di applicazione delle condizioni di liceità *ex* artt. 6 lett. *b-f)* rientrando piuttosto nella condizione del consenso. Ci stiamo riferendo ai casi di marketing e profilazione dei dati.

[85] GRUPPO DI LAVORO EX ART. 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., p. 1-2.

[86] L'*Opinion* 6/2014 cit. afferma che l'interesse per essere legittimo deve essere ammesso dalla legge, quindi «deve essere lecito (ossia conforme al diritto nazionale e unionale applicabile; essere articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti fondamentali dell'interessato (ossia sufficientemente specifico); rappresentare un interesse concreto ed effettivo (ossia non deve essere teorico)». Cfr. GRUPPO DI LAVORO EX ART. 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., pp. 30-31. Si segnala inoltre, l'art. 6, par. 2 GDPR che sancisce l'inapplicabilità della lett. *f)* alle ipotesi di trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

gli interessi e le libertà fondamentali dell'interessato e verificarne "l'impatto"[87] con l'interesse legittimo; *c)* effettuare un bilanciamento provvisorio; *d)* e ove lo ritenesse opportuno il titolare potrebbe adottare garanzie supplementari per evitare qualsiasi impatto indebito[88].

L'esito positivo del *test* consente al titolare di giustificare il trattamento che sta eseguendo, poiché "necessario" e "proporzionato" rispetto ai diritti, libertà e interessi del soggetto interessato.

A ben vedere, il *test* comparativo effettuato ai sensi dell'art. 6, lett. *f)*, GDPR altro non è che un *test* di necessità[89], che si differenzia da quello relativo alle altre condizioni di liceità (diverse dal consenso) solamente per l'incertezza del concetto di «interesse legittimo», il cui inquadramento rappresenta ancora una "zona grigia", che il legislatore europeo ha inteso risolvere facendo appello al principio di *accountability* e all'operatività del diritto di opposizione dell'interessato, esercitabile ai sensi dell'art. 21 GDPR.

Ad ogni modo, appare opportuno chiedersi, prima di soffermarsi sulle condizioni di liceità di cui all'art. 9, se la "necessità" in qualche modo incida anche sulla condizione del "consenso". Per rispondere a tale quesito si deve leggere l'art. 6, lett. *a)*, in combinato disposto con gli artt. 5 e 25 del GDPR.

L'art. 5 del GDPR enuncia i principi applicabili al trattamento. La circostanza che il trattamento dei dati sia stato "autorizzato" dal consenso dell'interessato, ai sensi dell'art. 6, par. 1, lett. *a)* – così come dell'art. 9, par. 2, lett. *a)* – del GDPR, non dispensa il titolare e/o il responsabile dal rispettare i principi cardine dell'ordinamento europeo, tra i quali quelli di *accountability*, di minimizzazione e di *privacy by design* e *by default*, il cui elemento costitutivo ed insopprimibile è proprio la "necessità" del trattamento.

Così, ad esempio, nei casi di *marketing* diretto, il titolare del trattamento, anche ove si avvalga della base giuridica del consenso, non è esonerato dal compiere un *test* di necessità e proporzionalità sul trattamento, sia per comprendere se la finalità di *marketing* possa essere raggiunta in egual modo con un mezzo alternativo e meno

---

[87] Il Gruppo di lavoro *ex* Art. 29 spiega che il concetto di "impatto" è un termine che comprende «tutte le possibili (potenziali o effettive) conseguenze del trattamento dei dati». Ai fini della sua valutazione il titolare dovrà verificare la sua fonte, ovvero la probabilità che il rischio si concretizzi e la gravità delle sue conseguenze, la cui intensità potrebbe variare a seconda della natura dei dati trattati (personali o categorie particolari di dati). Cfr. Gruppo di lavoro ex Art. 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., pp. 44-45.

[88] La quarta fase è eventuale e si verifica solo nei casi in cui non è chiaro in quale modo deve operare il bilanciamento, ovvero nelle ipotesi di dubbia interferenza. Le garanzie che deve attuare il responsabile (o il titolare) sono generalmente quelle prescritte dalla legge, e queste o «misure tecniche e organizzative. utilizzo estensivo di tecniche di armonizzazione, aggregazione di dati, tecnologie di rafforzamento della tutela della vita privata, tutela della vita privata fin dalla progettazione ("*privacy by design*") nonché valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati, maggiore trasparenza, diritto generale e incondizionato di revoca ("*opt-out*"), portabilità dei dati e misure correlate volte a responsabilizzare gli interessati». Cfr. Gruppo di lavoro ex Art. 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., pp. 49-50.

[89] Si veda, per l'analisi del test di necessità, quanto riferito *amplius* al par. 2.4.

invasivo, sia per verificare se i dati trattati siano effettivamente quelli strettamente necessari per il raggiungimento di tale finalità, che l'interessato ha autorizzato con il proprio consenso.

Il titolare che ha ricevuto il consenso dall'interessato dovrà rispettare anche l'art. 25 del GDPR, ovvero il principio dell'*accountability* e privacy *by default*, quale consolidamento del principio di necessità[90].

Procedendo ora con l'analisi delle condizioni di liceità di cui all'art. 9 del GDPR, rubricato «Trattamento di categorie particolari di dati personali», va rilevato che anche in quest'ambito, il principio di necessità manifesta la sua forza cogente.

L'art. 9 al par. 1. del Reg. cit. sancisce il divieto di trattare alcune c.d. particolari categorie di dati, ovvero quelli che rivelino «l'origine razziale o etica, le opinioni politiche, le condizioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Tuttavia, al paragrafo successivo, il legislatore prontamente precisa che tale divieto non opera in presenza di alcune circostanze particolari e predeterminate *ex lege* [art. 9, par. 2, lett. *a)- j)*, GDPR].

Come si può vedere da una lettura della norma, alcune di tali eccezioni risultano simili alle condizioni di liceità di cui all'art. 6 del Reg. cit., seppur con talune variazioni richieste dall'esigenza di accordare un maggior livello di tutela per l'interessato. Esse operano, segnatamente, quanto: l'interessato ha prestato il proprio consenso esplicito al trattamento [lett. *a)*]; il trattamento risulta necessario per assolvere gli obblighi di legge [lett. *b*)]; occorre tutelare un interesse vitale [lett. *c)*] o porre in essere un trattamento per motivi di interesse pubblico rilevante [lett. *g)*]. Altre condizioni di liceità *ex* art. 9, par. 2, GDPR, sono invece contemplate in maniera specifica per il trattamento di dati personali, senza che vi sia alcuna corrispondenza con quelle di cui all'art. 6 GDPR[91].

Si pensi ai casi di trattamento «necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce pe la salute a carattere transfrontaliero (…)» [lett. *i)*], in cui vengono il Garante ricomprende *le app* di *contract tracing,* che dovranno essere predisposte in modo da garantire la necessità, proporzionalità ed effettività del trattamento dei dati, anche particolari.

2.6. (*segue*): Principio di necessità e principio di minimizzazione dei dati nel GDPR

Il GDPR ha previsto che ogni trattamento dei dati personali debba avvenire nel rispetto dei principi indicati all'art. 5, tra i quali, al par. 1, lett. *c),* si rinviene il principio di minimizzazione dei dati, secondo il quale il titolare del trattamento deve utilizzare e raccogliere i dati personali in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali i dati sono trattati[92]. Rispetto all'o-

[90] Cfr., *amplius*, par. 2.8.

[91] Ci stiamo riferendo alle lett. *d)*, *f)*, *g)*, *h)*, *i)*, *j)* dell'art. 9, par. 2, GDPR.

[92] L'art. 5 GDPR riprende quanto previsto dall'art. 6, par. 1, lett. *c)*, della Direttiva 95/46/CE, nonché dall'art. 5, lett. *c)*, della Convenzione n. 108/81.

perattività in tema di condizioni di liceità del trattamento diverse dal consenso, qui il principio di necessità ha, come termine di riferimento, non il presupposto legittimo individuato dal legislatore, ma la finalità del trattamento determinata dal titolare.

In altre parole, il principio di necessità sembra avere una valenza generale, pervadendo altri principi e istituti, con connotati e direzioni di volta in volta diversi. Negli artt. 6 e 9 del GDPR vale a determinare le condizioni di liceità del trattamento, ma la necessità va rapportata a ciò che il legislatore ha indicato quale fondamento legittimo del trattamento. Nell'art. 5, par. 1, lett. *c)*, GDPR, il principio di necessità pervade il principio di minimizzazione e richiede che la necessità riguardi non solo l'adeguatezza e la pertinenza dei dati, ma anche la loro limitazione qualitativa e quantitativa in relazione a quanto necessario rispetto alle finalità del trattamento. Nell'interazione con principio di minimizzazione dei dati, il principio di necessità opera, dunque, in maniera analoga a quanto già previsto nel Codice della *privacy* all'art. 3, nel testo precedente alla riforma del 2018.

Sicché, il principio di minimizzazione non è certamente un principio innovativo, poiché lo stesso è riconducibile al «principio di necessità» del trattamento dei dati di cui all'abrogato art. 3 del Codice della *privacy* e al principio di pertinenza, completezza e non eccedenza dei dati di cui all'art. 11 del medesimo Codice, anch'esso abrogato con la riforma del 2018[93].

Quanto appena affermato risulta ben evidenziato da una recente ordinanza del 2019 della Corte di Cassazione n. 34113, in cui, riferendosi al principio di minimizzazione, afferma come lo stesso «era ben espresso dal d.lgs. n. 196 del 2003, art. 3, recante il titolo "principio di necessità nel trattamento dei dati", e dall'art. 11, lett. *d)* legge cit., richiedente la pertinenza, la completezza e non eccedenza dei dati rispetto alle finalità per cui sono raccolti e trattati»[94]. E in tal senso sono anche i provvedimenti del Garante per la protezione dei dati personali[95].

Sebbene il principio di necessità costituisca un canone minimo del principio di minimizzazione risulta pacifico, sia in dottrina[96] che in giurisprudenza[97], che si tratta di principi parzialmente sovrapponibili: il principio di necessità costituisce

[93] Cfr. F. Resta, *Comm. all'art. 5. Principi applicabili al trattamento dei dati personali,* cit., p. 57.

[94] L'ordinanza in commento riguarda il trattamento delle informazioni personali effettuato nell'ambito delle attività di recupero crediti, che viene considerata lecita solo se conforme al principio di minimizzazione*,* ovvero sole se vengono utilizzati dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento dello scopo per cui sono trattati. Cfr. Cass., sez. I, ord. n. 34113/ 2019.

[95] Cfr. GPDP, Provv. 20 luglio 2017, doc. *web*. n. 6955363.

[96] Cfr. F. Resta, *Comm. all'art. 5. Principi applicabili al trattamento dei dati personali*, cit., p. 57; G. Cristofari-F. Sartore, *Comm. art. 5 GDPR* (*Principi applicabili al trattamento di dati personali)*, cit., p. 88; C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale,* cit. pp. 23 e 24, il quale rimarca che nel principio di minimizzazione – espresso nella nuova formulazione contenuta nell'art. 5, par. 1, lett. *c)*, GDPR – si ritrova il principio di necessità già previsto all'art. 3 del Codice della *privacy*, con l'avvertenza che il principio di necessità di cui all'art. 3 cit. sembra scindersi nel principio di minimizzazione, di esattezza e di limitazione della conservazione. Di tutti e tre, però, il primo ha una «valenza più generale, idonea a ricomprendere gli altri due».

[97] *Ex multis*: Cass., sez. I, ord. n. 26778/2019, Cass., sez. I, ord. n. 34113/ 2019.

un tassello fondamentale della minimizzazione, ma non si può certo affermare che abbia la medesima portata applicativa, avendo una portata ben più ampia, come del resto risulta dall'analisi condotta nei precedenti paragrafi, con riguardo, tra l'altro, al bilanciamento tra diritti fondamentali *ex* art. 1, par. 3, GDPR e alle condizioni di liceità diverse dal consenso *ex* art. 6 e 9 del GDPR.

2.7. (*segue*): Principio di necessità e valutazione d'impatto *ex* art. 35 GDPR

Che il principio di necessità e quello di minimizzazione abbiano una portata non identica sul piano applicativo trova conferma anche con riguardo agli strumenti che sono stati posti dal legislatore europeo per la mitigazione dei rischi generati da un trattamento di dati personali che faccia uso di strumenti tecnologici, facendo leva sulla responsabilizzazione del titolare.

Ci si sta riferendo alla DPIA (c.d. *data protection impact assessment*), ovvero a quello strumento attraverso il quale il titolare del trattamento è tenuto a valutare i rischi di un trattamento (c.d. *privacy impact assessment*)[98] ed a predisporre le relative misure qualora ravvisi un *rischio elevato* di lesione dei diritti e delle libertà dell'interessato. Come precisato dall'art. 35 del GDPR, la valutazione d'impatto «mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli»[99].

Va effettuata nei casi previsti dalla legge e prima di dare inizio al trattamento.

Il legislatore europeo, al par. 7, ha previsto che la valutazione d'impatto debba necessariamente avere i seguenti contenuti minimi, che devono essere sviluppati in quattro fasi, tra loro consecutive, del processo di valutazione: (i) la descrizione dei trattamenti previsti e delle finalità del trattamento, (ii) la valutazione della *necessità* e proporzionalità dei trattamenti, (iii) la valutazione dei rischi per i diritti e le libertà degli interessati e, infine, (iv) l'individuazione delle misure di sicurezza idonee ad affrontare i rischi che incombono sul trattamento, nonché le misure volte a garantire la protezione dei dati e dimostrare la conformità del trattamento al GDPR.

Per quel che ci interessa, è lapalissiano come l'aderenza al principio di necessità costituisca un aspetto indefettibile ed imprescindibile del processo di valutazione d'impatto, poiché l'art. 35, par. 7, del Reg. cit. prevede espressamente che il titolare debba dapprima valutare la necessità del trattamento e solo successivamente dovrà prendere in considerazione se la misura adottata sia proporzionata rispetto ad altre che sarebbero state meno invasive dei diritti degli interessati[100].

---

[98] Il regolamento europeo ha un approccio basato sulla valutazione del rischio. Per l'analisi del rischio come elemento strutturale della normativa europea si veda A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 473 ss.

[99] Definizione rinvenibile sul sito del Garante per la protezione dei dati personali, all'url https://www.garanteprivacy.it/regolamentoue/dpia e confermata dall'EDPB, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679,* on 4 April 2017.

[100] Cfr. F. CECAMORE, *Comm. art. 35 GDPR* (*Valutazione d'impatto sulla protezione dei dati)*, in G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario al Regolamento (UE) 2016/679*, cit., p. 328.

Nella valutazione d'impatto il principio di necessità opera in due direzioni e dunque il titolare del trattamento dovrà svolgere due test di necessità: con il primo dovrà valutare se il trattamento è di per sé necessario in relazione alle finalità legittime che si intendono perseguire; il secondo riguarda gli aspetti qualitativi e quantitativi del trattamento, dovendosi limitare a quanto strettamente necessario in relazione alle finalità del trattamento, con valutazione che deve coinvolgere anche i tempi di conservazione dei dati, gli strumenti utilizzati nel trattamento, le procedure di gestione del flusso dei dati (*workflow*).

2.8. Il principio di necessità e *privacy by design* e *by default* nel GDPR. Il consolidamento nell'ordinamento europeo dell'originaria accezione del «principio di necessità» già emergente *ex* art. 3 del Codice della *privacy*

Il principio di necessità, come già precisato, è alla base anche delle disposizioni normative di cui all'art. 25 del GDPR, in tema di «Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita»[101]. Si può affermare che la *privacy by design* e *by default* costituisce il consolidamento nell'ordinamento europeo del principio di necessità[102].

L'art. 25 cit. disciplina il principio della *privacy by design* e *by default* quale declinazione del principio di necessità e di *accountability* ed ha una portata indubbiamente innovativa nel *framework* normativo europeo in materia di protezione dei dati personali, anche se è possibile intravedere un antecedente nel nostro ordinamento giuridico proprio con riguardo all'art. 3 del Codice della *privacy*, abrogato per le note esigenze di coordinamento con il GDPR[103].

Il legislatore europeo, ricollegandosi a quanto già previsto nel nostro Codice e in linea con l'impostazione caldeggiata anche in altre esperienze giuridiche[104], ha

[101] Con riguardo alla *privacy by design* e *by default* nel GDPR si veda F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 775-854; F. Bravo, *Data Management Tools and Privacy by Design and by Default*, in R. Senigaglia-C. Irti-A. Bernes (ed. by), *Privacy and Data Protection in Software Services*, Springer, 2022, pp. 85-95.

[102] Cfr. L. Rufo, *Il dossier sanitario elettronico. Un approccio traslazionale alla disciplina del trattamento dei dati sanitari in ambito europeo*, Bologna, 2018, p. 85.

[103] Tra i promotori della *privacy by design* si veda A. Cavoukian, *The 7 Foundational Principles*. Tale principio è stato riconosciuto durante la 32° International Conference of Data Protection and Privacy Commissioners, Resolution on *privacy by design*, Jerusalem-Israel, 27-29 October 2010 e in Europa è stata codificata per la prima volta soltanto con il Reg. UE n. 2016/679. Inoltre, Klitou definisce la *privacy by design* come «*pratical measures, in the form of technological and/or design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimizing the privacy intrusive capabilities of the technologies concerned*». Cfr. D. Klitou, *A solution, but not a panacea for defending privacy: The challenges, criticism and limitations of privacy by design*, in Prenel-Ikonomou, Privacy, Thecnologies and Policy; First Annual Privacy Forum, APF, 2012, Springer Verlag 2014, p. 86.

[104] Cfr. A. Cavoukian, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices,* in privacybydesign.ca, January 2011, consultabile *online* all'url https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (verificato da ultimo in data 25 gennaio 2023). Ivi l'A., che all'epoca di redazione del documento cit. ricopriva la

così posto a carico del titolare del trattamento l'obbligo[105], di carattere generale, di adozione delle misure tecniche e organizzative «adeguate»[106], che siano in grado sia di attuare efficacemente «i principi di protezione dei dati, quali la minimizzazione, e (…) [di] integrare nel trattamento dei dati le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati» (art. 25, par. 1), sia di «garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento» (art. 25, par. 2)[107].

L'evidente connessione con il principio di necessità è stata messa ben in risalto dall'*European Data Protection Board*, laddove, con riferimento alla struttura del principio della *privacy by design* e *by default*, ha rilevato che la «*data minimisation substantiates and operationalises the principle of necessity*»[108], precisando altresì, nel medesimo contesto, che «*Key design and default elements may include* (…) *Necessity*»[109], nel senso che «*Each personal data element shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means*».

---

carica di *Information & Privacy Commissioner* del Canada, ha individuato i sette elementi costitutivi – di seguito riportati – connotanti la *privacy by design* (comprensiva, secondo tale impostazione, della *privacy by default*): «1) *Proactive, not reactive; preventive, not remedial*; 2) *Privacy as the default setting*; 3) *Privacy embedded into design*; 4) *Full functionality – positive-sum, not zero-sum*; 5) *End-to-end security – full life-cycle protection*; 6) *Visibility and transparency – keep it open*; 7) *Respect for user privacy – keep it user-centric*». Si rinvia alla lettura del contributo sopra citato per un ulteriore approfondimento.

[105] Che si tratti di obbligazioni *ex lege* è chiarito da S. FAILLACE, *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di* privacy *by design e* di *privacy by default*, in *Contratto e impresa*, 2022, 4, pp. 1123 ss.

[106] Si tratta di misure tecniche e organizzaive diverse da quelle previste dagli artt. 24 e 32 GDPR, da cui si possono comunque trarre elementi utili. L'art. 32 stabilisce che le misure di sicurezza devono essere approntate «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche».

[107] Il *considerando* n. 78 del GDPR precisa che «La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell›arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati».

[108] Cfr. EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, on 13 November 2019, p. 21.

[109] *Ibidem*.

Alla luce di ciò, il principio della *privacy by design* e *by default* costituisce una particolare declinazione, nell'ordinamento europeo, del principio di necessità[110], che connota l'intero ciclo di vita del trattamento, dalla fase iniziale della progettazione e della successiva raccolta dei dati, fino alla loro cancellazione o anonimizzazione, ovvero fino alla cessazione del trattamento[111].

3. Applicazione del principio nella casistica

Nella prassi del Garante per la protezione dei dati personali maturata nella vigenza del Reg. UE n. 679/2016, l'applicazione del principio di necessità, almeno in via espressa, appare più contenuta rispetto al passato.

Detto principio, d'altra parte, non risulta esplicitato nel regolamento europeo e non è più stabilito dal d.lgs. 30 giugno 2003, n. 196, a fronte dell'abrogazione dell'art. 3 («*Principio di necessità nel trattamento dei dati*») nel contesto dell'adeguamento della normativa nazionale al GDPR realizzato a opera del d.lgs. 10 agosto 2018, n. 101[112].

L'applicazione espressa del principio in esame a opera del Garante emerge essenzialmente in fattispecie nelle quali maggiore è il contatto con la normativa previgente, come per la casistica basata su orientamenti cristallizzati in provvedimenti adottati nel vigore di quest'ultima o comunque nel contesto di decisioni poste a cavallo tra i due regimi normativi.

In tal senso, è opportuno richiamare anzitutto il provvedimento del 16 dicembre 2021[113], adottato in applicazione della normativa previgente, nel quale il Garante da un lato riconduce il principio di necessità agli abrogati artt. 3 e 11, co. 1, lett. *d)*, d.lgs. n. 196/2003[114], in conformità al proprio orientamento pregresso[115], dall'altro

---

[110] *Ibidem*.

[111] A. Cavoukian, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, cit., p. 6, ove ha rimarcato che «*Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end*».

[112] Sull'art. 3 d.lgs. n. 196/2003, si veda, oltre a quanto illustrato *supra* al par. 2, G. Buttarelli, *Comm. art. 3 (Principio di necessità nel trattamento dei dati)*, cit., pp. 32 ss.; G. Finocchiaro, Privacy *e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 113 ss.

[113] GPDP, Provv. 16 dicembre 2021, doc. *web* n. 9742485.

[114] L'art. 11, co. 1, lett. *d)*, d.lgs. n. 196/2003 prevedeva che i dati personali oggetto di trattamento dovessero essere «pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati». Su questa norma e, più ampiamente, sui principi applicabili al trattamento e le condizioni di liceità nel contesto del Codice *privacy* previgente, v. F. Bravo-J. Monducci, *Le condizioni di liceità del trattamento dei dati*, in J. Monducci-G. Sartor (a cura di), *Il Codice in materia di protezione dei dati personali*, Padova, 2004, pp. 35 ss.

[115] Nella prassi del Garante il principio di necessità è normalmente identificato nei citati artt. 3 e 11, co. 1, lett. *d)*, d.lgs. n. 196/2003 ed è spesso richiamato unitamente al principio di proporzionalità (cfr. ad es. GPDP, Provv. 25 maggio 2005, doc. *web* n. 1131826; Provv. 24 novembre 2016, doc. *web* n. 5796783; Provv. 19 gennaio 2017, doc. *web* n. 6068256). Occorre infatti ricordare come l'art.

chiarisce come il medesimo principio, nella nuova cornice normativa, sia da identificarsi nell'odierno principio di minimizzazione di cui all'art. 5, par. 1, lett. *c)*, GDPR.

Nel caso in questione, una stazione appaltante, acquisita e verificata la documentazione per l'iscrizione di una società al proprio albo dei fornitori, comprensiva dell'autocertificazione sull'assenza di condanne penali a carico di persone con determinati ruoli nella società, provvedeva ad estrarre dal sistema informativo del casellario il certificato riferito al sindaco supplente di tale società, inviandolo successivamente alla stessa per richiedere chiarimenti su di una sentenza penale riportata al suo interno. Il Garante ha accertato l'illiceità delle operazioni di estrazione e di successiva comunicazione del certificato in questione per violazione dei principi di necessità, pertinenza e non eccedenza. Al tempo dei fatti esaminati, invero, non era affatto pacifico che i requisiti di onorabilità previsti dal Codice dei contratti pubblici (d.lgs. 18 aprile 2016, n. 50) fossero riferibili anche ai membri dell'organismo di vigilanza e, in particolare, ai sindaci supplenti. In ogni caso, a fronte di quanto stabilito nelle linee guida ANAC n. 6 del 2016, l'appaltante avrebbe dovuto procedere a una «valutazione sulla reale idoneità in concreto della condanna risultata a carico del reclamante, in relazione alla natura del reato commesso, alla gravità del fatto, al tempo trascorso dalla condanna, ad incidere sulla attività oggetto di affidamento da parte dell'operatore economico, prima di procedere alla richiesta e successivamente alla comunicazione di dati, di tipo giudiziario, riferiti al reclamante»[116].

La violazione del principio di necessità emergeva altresì dal contrasto con l'autorizzazione n. 7/2016 in materia di trattamento dei dati giudiziari[117], la quale infatti recava «prescrizioni (…) rese dal Garante anche in applicazione delle regole generali per il trattamento dei dati (v. artt. 3 e 11 del Codice, testo vigente al tempo dei fatti oggetto di reclamo)», in particolare laddove disponeva che «[p]ossono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa» (Capo VII, punto 1) e che «[i] dati possono essere comunicati e, ove previsto dalla legge, diffusi, a soggetti pubblici o privati nei limiti strettamente indispensabili per le finalità perseguite e nel rispetto, in ogni caso, del segreto professionale e delle altre prescrizioni sopraindicate» (Capo VII, punto 4)[118].

La decisione in commento, inoltre, consente di cogliere la collocazione sistematica del principio in esame e la sua centralità. L'Autorità afferma infatti che i principi di necessità, pertinenza ed eccedenza sono «espressione del principio gene-

11, co. 1, lett. *d)* del Codice *privacy* disponesse in ordine al principio di proporzionalità, il quale è distinto da quello di necessità (cfr. ad es. GPDP, Provv. 29 aprile 2004, doc. *web* n. 1003482; Provv. 24 febbraio 2005, doc. *web* n. 1103045). A ogni modo, nella prassi l'applicazione dei due principi tende a sovrapporsi, a fronte dell'evidente affinità degli obiettivi cui ciascuno di essi è funzionale (sul rapporto fra tali principi, v. anche quanto indicato *supra*, par. 2.2).

[116] GPDP, Provv. 16 dicembre 2021, cit.

[117] GPDP, Provv. 15 dicembre 2016, doc. *web* n. 5803630. Detta autorizzazione ha cessato di produrre effetti giuridici alla data di entrata in vigore del d.lgs. n. 101/2018, in conformità a quanto previsto dall'art. 21, co. 3 di tale decreto.

[118] GPDP, Provv. 16 dicembre 2021, cit.

rale di proporzionalità, che costituisce parametro generale di legittimità delle limitazioni del diritto alla protezione dei dati personali *ex* art. 52 della Carta dei diritti fondamentali dell'Unione europea»[119]. Emerge, pertanto, l'operatività del principio di necessità nel contesto del giudizio di proporzionalità, quale elemento essenziale del medesimo, servente alla realizzazione del corretto bilanciamento tra le «due anime» della normativa europea in materia di protezione dei dati personali[120], cioè tra le contrapposte esigenze della protezione e della libera circolazione dei dati personali (art. 1, par. 3, GDPR)[121].

Su queste basi, il Garante accertava in ultimo la «irragionevole compressione del diritto alla riservatezza dell'interessato», posto che la suddetta comunicazione di dati relativi a condanne penali e reati «non era in concreto "strettamente indispensabil[e] per le finalità perseguite", in violazione dei principi di necessità, pertinenza e non eccedenza», come detto ricondotti agli abr. artt. 3 e 11, co. 1, lett. *d)*, d.lgs. n. 196/2003 e all'odierno principio di minimizzazione[122].

Procedendo oltre, un'ampia applicazione del principio di necessità è riscontrabile nell'ambito delle decisioni relative ai trattamenti con finalità di trasparenza dell'azione amministrativa svolti mediante diffusione di dati personali *online*[123].

In merito, si richiama il caso definito con provvedimento dell'8 luglio 2021[124], nel quale un ente pubblico diffondeva sull'albo pretorio *online* del proprio sito *web* un documento recante dati personali sia in chiaro sia in forma "oscurata". Tralasciando altri profili, tra cui i limiti per le operazioni di diffusione dei dati personali imposti ai soggetti pubblici dall'art. 2-*ter* del d.lgs. n. 196/2003, si evidenzia che, alla base delle proprie argomentazioni relative al principio di necessità, ivi il Garante richiama gli odierni principi di minimizzazione, protezione dei dati *by design* e *by default*, nonché di responsabilizzazione, sottolineando peraltro la coerenza del quadro emergente da tali principi con quanto già stabilito nelle Linee guida del 2014 relative al trattamento svolto da soggetti pubblici per fini di trasparenza amministrativa[125], ritenute attuali nella parte sostanziale.

---

[119] *Ibidem*.

[120] Cfr. N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla* privacy, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 35 ss.

[121] Sulle questioni del bilanciamento tra diritti e libertà fondamentali e, in particolare, tra diritto alla protezione dei dati personali e libera circolazione di tali dati, si v. F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 188 ss.; Id., *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, cit., pp. 190-216.; V. Ricciuto, *L'equivoco della* privacy. *Persona* vs *dato personale*, Napoli, 2022, pp. 35 ss. e 49 ss.

[122] GPDP, Provv. 16 dicembre 2021, cit. Sul punto della necessità di valutare "in concreto", cioè in considerazione delle specifiche caratteristiche del singolo caso, la proporzionalità delle limitazioni ai diritti alla riservatezza e alla protezione dei dati personali, vi è coerenza tra prassi del Garante e giurisprudenza unionale, come meglio descritto *infra*.

[123] V. ad es. GPDP, Provv. 17 dicembre 2020, doc. *web* n. 9557753; Provv. 22 luglio 2021, doc. *web* n. 9697724; Provv. 16 settembre 2021, doc. *web* n. 9713735.

[124] GPDP, Provv. 8 luglio 2021, doc. *web* n. 9703134.

[125] GPDP, Provv. 15 maggio 2014, doc. *web* n. 3134436.

Richiamando dette Linee guida, l'Autorità afferma che «anche nell'ipotesi in cui esista un obbligo per l'amministrazione di pubblicare un atto o documento nel proprio sito *web* istituzionale (…) è in ogni caso necessario "selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni", in quanto non necessari rispetto alle finalità per le quali sono trattati (cfr. ora il principio di "minimizzazione" dei dati di cui art. 5, par. 1, lett. *c*, del RGPD, che ha sostituito i principi di pertinenza e non eccedenza, nonché di necessità, di cui agli artt. 3, 11, comma 1, lett. *d*, del Codice previgente e all'art. 6, par. 1, lett. *c*, della Direttiva 95/46/CE abrogata dal RGPD)»[126].

I principi di necessità, pertinenza e non eccedenza sono dunque riportati all'attuale principio di minimizzazione, in applicazione del quale la diffusione dei dati effettuata dall'ente pubblico viene ritenuta illecita in quanto ultronea rispetto alle esigenze di trasparenza rilevanti nel caso concreto.

Parimenti d'interesse è che l'Autorità, in tal caso, ha ritenuto violati anche i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, segnatamente sotto il profilo della minimizzazione. Il titolare del trattamento, infatti, pur avendo oscurato parte dei dati personali contenuti nei documenti pubblicati, aveva adottato «strumenti del tutto inadeguati all'obiettivo, sottovalutando i rischi del trattamento (art. 25, parr. 1 e 2, RGPD)», con la conseguenza che «chiunque in maniera molto agevole (…) poteva visualizzare il testo sottostante alle "etichette oscuranti" di colore bianco utilizzate, tramite una semplice operazione di copia e incolla all'interno di un mero *file* .doc (es. *Word*)». Le misure adottate, pertanto, non garantivano, fin dalla progettazione, l'attuazione in modo efficace del principio di minimizzazione né assicuravano che, per impostazione predefinita, fossero trattati i soli dati personali necessari per ogni specifica finalità del trattamento (art. 25, parr. 1 e 2 GDPR). In tal senso, veniva accertata la violazione delle norme in materia di protezione dei dati *by design* e *by default*, parimenti espressione del principio in esame nella sua portata applicativa più ampia (v. *supra*, par. 2.8) e comunque coerenti con le prescrizioni di configurazione dei sistemi di trattamento stabilite in passato dall'abr. art. 3 d.lgs. n. 196/2003[127].

Dalla prassi relativa ai trattamenti per fini di trasparenza amministrativa emerge anche il richiamo al principio di necessità come elemento essenziale del bilanciamento tra i diritti e le libertà antagonisti nel caso concreto.

Sul punto, è indicativo il provvedimento del 9 giugno 2022, sempre relativo a un caso di diffusione di dati personali su di un albo pretorio *online*[128]. Il Comune di Brindisi, in particolare, pubblicava una delibera di giunta avente a oggetto la costituzione in giudizio del Comune in una causa mossa da un genitore per le lesioni

[126] GPDP, Provv. 8 luglio 2021, cit.

[127] Sul rilievo dell'art. 3 d.lgs. n. 196/2003 come disposizione recante precetti di *privacy by design*, v. ad es. G. FINOCCHIARO, Privacy *e protezione dei dati personali. Disciplina e strumenti operativi*, cit., p. 115. Rispetto alla *privacy by design* e *by default* nel regime del GDPR, si v. F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 775-854; R. D'ORAZIO, *Protezione dei dati* by default *e* by design, cit., pp. 79 ss.

[128] GPDP, Provv. 9 giugno 2022, doc. *web* n. 9789037.

subite dal proprio figlio minore a seguito di una caduta all'interno della scuola e, in questo modo, diffondeva i dati personali di tali interessati. L'Autorità ha stabilito che le norme relative agli obblighi di trasparenza imposti alle pubbliche amministrazioni dal d.lgs. 14 marzo 2013, n. 33 devono essere «in ogni caso interpretate alla luce dei principi [in] materia di protezione dei dati personali, in base ai quali il trattamento dei dati personali deve rispettare i principi di necessità e proporzionalità e i dati personali devono essere non solo adeguati e pertinenti, ma anche "limitati a quanto necessario rispetto alle finalità per le quali sono trattati" secondo il principio di "minimizzazione" (art. 5, par. 1, lett. *c*, del RGPD)»[129].

L'esigenza correlata alla finalità di trasparenza dell'azione amministrativa, infatti, «va contemperata, in ogni caso, con i principi e le regole in materia di protezione dei dati personali, considerando che "non può riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali" (sent. Corte cost. n. 20 del 21/02/2019, punto n. 3.1. del cons. dir.)»[130]. L'Autorità richiama la citata sentenza della Corte Costituzionale anche laddove quest'ultima riporta la consolidata giurisprudenza unionale tale per cui, in conformità al principio di proporzionalità – il quale, nella sua accezione "ampia", include anche quello di necessità[131] –, «"deroghe e limitazioni alla protezione dei dati personali devono (…) operare nei limiti dello stretto necessario, e prima di ricorrervi occorre ipotizzare misure che determinino la minor lesione, per le persone fisiche, del suddetto diritto fondamentale e che, nel contempo, contribuiscano in maniera efficace al raggiungimento dei confliggenti obiettivi di trasparenza, in quanto legittimamente perseguiti" (*ibidem*, cfr. anche giurisprudenza europea ivi citata)»[132].

Su queste basi, il Garante ha ritenuto non proporzionata la diffusione in Rete dei nominativi delle parti in causa, «che non risultano "limitati a quanto necessario rispetto alle finalità per le quali sono trattati" alla luce del principio di "minimizzazione" dei dati e quindi anche di proporzionalità (art. 5, par. 1, lett. *c*, del RGPD)», posto che a tali fini sarebbe stato «sufficiente indicare nell'oggetto della delibera anche solo il numero di ruolo generale della causa»[133].

I provvedimenti adottati nell'ambito in considerazione, sotto altro angolo prospettico, consentono di trarre utili indicazioni rispetto alla dimensione del principio di necessità collegata alle condizioni di liceità diverse dal consenso dell'interessato[134] e, in particolare, alle basi giuridiche previste dall'art. 6, par. 1, lett. *c)* ed *e)*, GDPR, ossia al trattamento "necessario", rispettivamente, all'adempimento di obbli-

[129] *Ibidem*.
[130] *Ibidem*.
[131] Cfr. ad es. EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., pp. 5 ss.
[132] GPDP, Provv. 9 giugno 2022, cit.
[133] *Ibidem*.
[134] Sulle condizioni generali di liceità del trattamento di cui al GDPR si veda, più in generale, F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 110-193; D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, cit., pp. 2783-2789.

ghi di legge oppure all'esecuzione di compiti di interesse pubblico o all'esercizio di pubblici poteri[135].

Come sopra evidenziato, infatti, il principio di necessità opera anche nel contesto di tali attività, nonostante le stesse siano svolte per adempiere obblighi di legge o comunque per soddisfare interessi pubblici. La conseguenza applicativa è che questo tipo di trattamenti risulta legittimo soltanto se il titolare del trattamento, anche nel rispetto dei propri doveri di responsabilizzazione (artt. 5, par. 2, e 24, GDPR), ne assicuri l'effettuazione nella misura strettamente necessaria all'adempimento degli obblighi di legge oppure all'esecuzione dei compiti di interesse pubblico o all'esercizio dei pubblici poteri specificamente rilevanti nel caso concreto[136].

Proseguendo oltre, rispetto alle condizioni di liceità diverse dal consenso stabilite, in particolare, all'art. 6, par. 1, lett. *b)* e *f)*, GDPR, risulta significativo il provvedimento relativo al *social network* Clubhouse[137].

Per quanto concerne la base giuridica della necessità di dare esecuzione a un contratto di cui l'interessato è parte o a misure precontrattuali adottate su richiesta dello stesso [lett. *b)*, norma cit.], il *provider*, nel caso di specie, si avvaleva di tale condizione rispetto a trattamenti svolti mediante profilazione per offrire agli utenti contenuti rispondenti ai loro interessi. Il fornitore sosteneva che il proprio servizio fosse «personalizzato by *design*» in quanto offerto per aiutare gli utenti a connettersi e creare una comunità[138]; ciò, al punto da doversi ritenere sussistente una ragionevole aspettativa degli utenti rispetto a detta personalizzazione, la quale non era svolta per finalità di *marketing* e che doveva considerarsi, invece, quale «elemento intrinseco e atteso del servizio (…) necessario all'esecuzione del contratto con l'utente, vale a dire l'esecuzione dei Termini di Servizio»[139]. Queste attività, nella specie, prevedevano il trattamento di un'amplissima gamma di dati degli utenti, tra cui in sostanza «tutto ciò che l'utente dice, pubblica o rende disponibile», essenzialmente per fini di miglioramento della partecipazione dell'interessato alla comunità[140].

L'Autorità ha accertato che il suddetto trattamento non poteva ritenersi basato sulla condizione di liceità indicata, facendo leva proprio sul requisito della necessità:

---

[135] Rispetto alla base giuridica relativa al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, la Corte di Giustizia UE nel caso *Huber* ha chiarito come la nozione di "necessità" prevista da tale condizione di liceità, a fronte dell'obiettivo di garantire un livello di tutela delle persone fisiche equivalente in tutti gli Stati membri, debba considerarsi quale nozione autonoma del diritto comunitario, da interpretarsi in maniera tale da rispondere pienamente alla finalità della normativa sulla protezione dei dati personali (Corte di Giustizia UE, Grande Sezione, sentenza del 16 dicembre 2008, causa C-524/06).

[136] Per completezza, si evidenzia che i principi di necessità e proporzionalità, previsti dalla clausola generale di limitazione di cui all'art. 52 della Carta dei diritti fondamentali UE, si applicano anche ai trattamenti disciplinati dalla Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati (cfr. ad es. Corte di Giustizia UE, Quinta Sezione, sentenza del 26 gennaio 2023, causa C-205/21, punto 3) del dispositivo).

[137] GPDP, Provv. 6 ottobre 2022, doc. *web* n. 9828901.

[138] *Ibidem.*

[139] *Ibidem*.

[140] *Ibidem.*

«[i]l discrimine va ricercato nella necessità dell'attività di profilazione ai fini della esecuzione del contratto, necessità che nel caso in argomento non si ravvisa posto che ciascun utente può unirsi alla comunità di Clubhouse anche senza esporre informazioni aggiuntive rispetto a quelle necessarie per la creazione dell'*account* e senza consentire ad Alpha Exploration di effettuare autonome elaborazioni in ordine alle modalità delle sue interazioni con la piattaforma»[141].

Il Garante perviene a tali conclusioni richiamando quanto sostenuto dal Comitato Europeo per la Protezione dei Dati nelle Linee guida sull'art. 6, par. 1, lett. *b)*, GDPR nel contesto della fornitura di servizi *online*[142]. L'Autorità, nella specie, ricorda come il Comitato abbia ritenuto che «[n]ella maggior parte dei casi, la raccolta di dati relativi a parametri organizzativi concernenti un servizio o di dettagli relativi al coinvolgimento degli utenti non può essere considerata necessaria per la prestazione del servizio, in quanto il servizio può essere fornito in assenza del trattamento di tali dati personali» e che, «[s]ebbene la possibilità di apportare miglioramenti e modifiche a un servizio sia spesso sistematicamente inclusa nei termini contrattuali, tale trattamento non può essere considerato oggettivamente necessario, in via generale, all'esecuzione del contratto stipulato con l'utente»[143].

Risultano altresì richiamate le indicazioni del Gruppo di lavoro *ex* Art. 29 fornite nelle Linee guida in materia di profilazione e processi decisionali automatizzati[144], laddove è stato ribadito che la base giuridica contrattuale «deve essere interpretata rigorosamente e non contempla le situazioni in cui il trattamento non è effettivamente necessario all'esecuzione di un contratto, bensì imposto unilateralmente all'interessato dal (…) [titolare] del trattamento. Inoltre, il fatto che alcuni trattamenti di dati siano coperti da un contratto non significa automaticamente che tali trattamenti siano necessari alla sua esecuzione»[145].

Per quanto concerne il legittimo interesse, il fornitore si avvaleva di questa base giuridica per registrare in modo sistematico le conversazioni effettuate dagli utenti in ogni "stanza" virtuale, provvedendo al monitoraggio automatizzato delle stesse per finalità di indagine su eventuali violazioni delle linee guida della comunità. Per maggiore chiarezza, si consideri che Clubhouse è un *social network* basato esclusivamente su interazioni vocali che si svolgono in apposite "stanze" di conversazione ("*room*").

Pur riconoscendo che, in astratto, un trattamento per fini di prevenzione delle frodi possa fondarsi sul legittimo interesse, come previsto dal *considerando* n. 47 GDPR, l'Autorità nel caso di specie ha ritenuto non soddisfatte le condizioni per avvalersi di tale base giuridica, anche a fronte delle indicazioni emergenti dalla giuri-

[141] *Ibidem*.

[142] EDPB, *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, cit.

[143] GPDP, Provv. 6 ottobre 2022, cit.

[144] Gruppo di lavoro ex art. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018.

[145] GPDP, Provv. 6 ottobre 2022, cit. Ulteriori indicazioni sul requisito della "necessità" relativamente alla base giuridica contrattuale si rinvengono in GPDP, Provv. 28 ottobre 2021, doc. *web* n. 9722661.

sprudenza unionale. Sul punto è stato infatti sottolineato che, in conformità a quanto statuito dalla Corte di giustizia UE nella causa C-13/16, tra i parametri necessari per valutare la sussistenza del legittimo interesse non vi è solo «la circostanza che gli interessi, i diritti e le libertà fondamentali dell'interessato non siano prevalenti rispetto a tale interesse», ma anche, «elemento non secondario, che i dati trattati siano "strettamente necessari" per la finalità perseguita, in particolare se la stessa è riconducibile alla prevenzione di condotte illecite»[146].

Ed è proprio valorizzando il requisito delle necessità che viene accertata l'inidoneità del legittimo interesse a fondare la liceità del suddetto trattamento. Il Garante rileva infatti che il trattamento funzionale a prevenire e contrastare possibili condotte illecite «non si attiverebbe solo su segnalazione da parte degli utenti di comportamenti concreti e lesivi delle regole della comunità, realizzati da altri soggetti, ma anche (e soprattutto) in via preventiva su ogni stanza e su ciascuna conversazione che verrebbe registrata e monitorata mediante sistemi automatizzati (…)»[147].

Di conseguenza, viene affermata la «sproporzione fra un monitoraggio così diffuso e pervasivo, nel quale, peraltro, la segnalazione di eventuali comportamenti illeciti è rimessa, in prima battuta, a processi decisionali automatizzati (monitoraggio che incide peraltro sui diritti di libertà di riunione, di associazione e di espressione del pensiero dei quali la Costituzione italiana riconosce l'inviolabilità in base a quanto stabilito dagli artt. 17, 18 e 21), e la finalità di prevenire e contrastare eventuali comportamenti non conformi alle linee guida della comunità, quasi che il solo far parte di un'associazione (di una comunità, come nel caso di specie) consenta alla medesima di "ascoltare" tutte le conversazioni di ogni associato, per confermarne in ogni istante l'aderenza con le norme statutarie»[148].

In tema di "necessità" delle misure limitative del diritto alla protezione dei dati personali rispetto a trattamenti che prevedono il monitoraggio delle comunicazioni, occorre richiamare altresì le argomentazioni fornite dalla Corte di Giustizia UE nel caso *Digital Rights Ireland*, con il quale è stata dichiarata l'invalidità della Direttiva 2006/24/CE (c.d. direttiva Frattini)[149].

Questa normativa, com'è noto, imponeva ai fornitori di servizi di comunicazione elettronica di conservare per un certo periodo di tempo (c.d. *data retention*) i dati da essi trattati, come quelli relativi al traffico e all'ubicazione degli utenti, allo scopo di garantirne la disponibilità alle autorità competenti per le attività di prevenzione, indagine, accertamento e perseguimento di reati gravi.

---

[146] *Ibidem.*

[147] *Ibidem*.

[148] *Ibidem*. Sul rilievo del requisito della necessità nel contesto della valutazione del legittimo interesse, si v. inoltre EDPB, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, 29 gennaio 2020, spec. par. 3.1, nonché, in precedenza, GRUPPO DI LAVORO EX ART. 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, cit., *passim*.

[149] Corte di Giustizia UE, Grande Camera, sentenza del 4 aprile 2014, cause riunite C-293/12 e C-594/12. Al riguardo, v. anche F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., p. 158.

In questo caso, la Corte ha accertato che l'ingerenza nei diritti alla riservatezza e alla protezione dei dati personali derivanti da tale direttiva non risultava limitata allo stretto necessario e, pertanto, non poteva ritenersi proporzionata ai sensi degli artt. 7, 8 e 52 della Carta dei diritti fondamentali UE. Tra le ragioni alla base di tale conclusione, preme evidenziare come vi era la considerazione che le misure previste riguardassero, in modo generale, qualsiasi persona, incluso cioè quelle per cui non esisteva alcun indizio tale da far ritenere che il loro comportamento potesse avere un nesso, anche soltanto indiretto, con reati gravi; l'applicazione delle misure limitative, inoltre, non richiedeva la sussistenza di una relazione tra i dati da conservare e una determinata minaccia alla sicurezza pubblica, mancando, ad esempio, di circoscrivere l'obbligo di conservazione ai soli dati riferiti a un certo periodo di tempo, a una determinata area geografica o a una particolare cerchia di persone che poteva ritenersi coinvolta nei gravi reati perseguiti[150].

Ulteriore ambito nel quale il Garante ha mostrato particolare sensibilità ai profili legati alla necessità del trattamento, nel contesto della valutazione del bilanciamento proporzionale tra diritti fondamentali, è quello dei trattamenti per finalità statistiche, rispetto al quale, tuttavia, la necessità non risulta espressamente richiamata in termini di principio.

Di particolare interesse è, sotto quest'ultimo profilo, il provvedimento del 17 dicembre 2020[151], in particolare nei passaggi riguardanti i lavori statistici volti alla creazione di registri o archivi basati sulla raccolta di un elevato numero di basi di dati amministrative e sulla loro interconnessione. Nell'esame di tali lavori, l'Autorità ha infatti provveduto a un'attenta verifica della «necessità in concreto di tale invasiva modalità di realizzazione della statistica ufficiale»[152].

Ritenendo l'utilizzo di fonti amministrative tale da comportare rischi elevati per i diritti e le libertà degli interessati, il Garante ha specificato che «occorre, prima ancora di individuare specifiche misure tecniche e organizzative per mitigarne l'impatto sui diritti e sulle libertà fondamentali degli interessati, verificare, di volta in volta, l'effettiva necessità rispetto al caso concreto, in ragione delle specifiche finalità perseguite, e che tali finalità non possano essere utilmente soddisfatte, anche tenuto conto del contesto di riferimento, attraverso misure meno invasive»[153].

Ciò precisato, il Garante ha accertato la necessità e proporzionalità del trattamento previsto nel caso esaminato, rilevando che «l'utilizzo di fonti amministrative costituisce la via più efficace per l'acquisizione, in tempi rapidi, di informazioni qualitativamente precise e aggiornate e quantitativamente sufficienti per l'elaborazione di indicatori effettivamente coerenti rispetto al fenomeno osservato e al debito informativo nei confronti delle istituzioni europee e nazionali»[154].

[150] Corte di Giustizia UE, sentenza del 4 aprile 2014, cit., punti 52 e ss.

[151] GPDP, Provv. 17 dicembre 2020, doc. *web* n. 9523274. In questo ambito, si v. anche GPDP, Provv. 9 giugno 2022, doc. *web* n. 9802796, relativo all'uso di fonti di "*Big Data*" per la produzione di statistiche ufficiali da parte dell'ISTAT.

[152] GPDP, Provv. 17 dicembre 2020, cit.

[153] *Ibidem*.

[154] *Ibidem*.

Anche questo arresto mostra come la prassi del Garante sia allineata alla giurisprudenza UE in materia di limitazioni ai diritti fondamentali alla tutela della vita privata e alla protezione dei dati personali. Ci si riferisce, in particolare ai seguenti aspetti: *i)* la valutazione della necessità e della proporzionalità deve essere svolta in considerazione delle circostanze del caso concreto e della specifica finalità perseguita; *ii)* il giudizio di necessità, in particolare, richiede di accertare sia l'efficacia della misura rispetto all'obiettivo perseguito sia l'assenza di una misura alternativa, meno invasiva, idonea a consentire il soddisfacimento del medesimo scopo; *iii)* occorre effettuare prima il test di necessità e poi quello di proporzionalità[155].

Rispetto ai trattamenti con finalità statistiche, più ampiamente, deve rilevarsi come il principio di necessità occupi una posizione centrale anche a livello normativo. L'art. 89 GDPR, ad esempio, prevede che se le finalità statistiche, così come quelle di archiviazione nel pubblico interesse e di ricerca scientifica o storica possano essere soddisfatte attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, dette finalità devono essere conseguite in questo modo. In aggiunta, la medesima disposizione, com'è noto, condiziona la possibilità per gli Stati membri di stabilire una disciplina maggiormente flessibile per i trattamenti con tali finalità alla previsione di «garanzie adeguate per i diritti e le libertà dell'interessato» (art. 89, par. 1, GDPR), le quali possono includere «misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e necessità» (*considerando* n. 156 GDPR). In Italia, d'altra parte, l'attenzione a questo principio emerge anche dalla disciplina sul trattamento dei dati personali prevista dalla normativa sul Sistema statistico nazionale, stabilita all'art. 6-*bis* del d.lgs. 6 settembre 1989, n. 322, introdotto con d.lgs. 30 luglio 1999, n. 281, ad esempio laddove si prevede che «[i] soggetti che fanno parte o partecipano al Sistema statistico nazionale possono raccogliere ed ulteriormente trattare i dati personali necessari per perseguire gli scopi statistici previsti dal presente decreto, dalla legge o dalla normativa comunitaria, qualora il trattamento di dati anonimi non permetta di raggiungere i medesimi scopi» (art. 6-*bis*, co. 1, d.lgs. n. 322/1989).

Plurime applicazioni del principio di necessità sono riscontrabili inoltre nei provvedimenti relativi all'utilizzo di dispositivi di geolocalizzazione in ambito lavorativo[156]. In questa casistica, il Garante ha mantenuto costante il proprio orien-

[155] Cfr. ad es. quanto indicato dall'EDPS, in considerazione della rilevante giurisprudenza unionale in materia, relativamente alla valutazione della "necessità" nel contesto del giudizio di proporzionalità "in senso ampio" (EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit., pp. 5 ss.). Per completezza, è bene chiarire che, con il concetto di "efficacia", si intende il carattere essenziale della misura limitativa rispetto all'obiettivo perseguito: «*The measure should be genuinely effective, i.e. essential to achieve the objective of general interest pursued*» (*Ibidem*, p. 17). Sul punto, si noti anche come il citato *Toolkit* dell'EDPS sia espressamente considerato dal Garante nel citato provvedimento del 17 dicembre 2020.

[156] V. ad es. GPDP, Provv. 16 marzo 2017, doc. *web* n. 6275314; Provv. 28 giugno 2018, doc. *web* n. 9023246; Provv. 28 febbraio 2019, doc. *web* n. 9094427. In tema di necessità e proporzionalità dei trattamenti effettuati nel contesto lavorativo tramite sistemi di geolocalizzazione, v. D. SBORLINI, *Proporzionalità dei trattamenti di dati personali svolti mediante dispositivi di geolocalizzazione in ambito lavorativo*, in *Diritto di Internet*, 2023, 1, pp. 151 ss.

tamento enucleato nel provvedimento generale del 2011[157], nel quale è stabilito, in applicazione del principio di necessità [artt. 3 e 11, co. 1, lett. *d)*, d.lgs. n. 196/2003], che la posizione del veicolo di regola non dovrebbe essere monitorata continuativamente, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite[158].

Particolarmente indicativo è il provvedimento del 19 luglio 2018, adottato in applicazione della normativa previgente, riguardante l'uso di un sistema di geolocalizzazione satellitare su di una flotta aziendale[159].

Il sistema in questione, fornito da una società terza agente quale responsabile del trattamento, era utilizzato nel contesto di attività di raccolta e trasporto di rifiuti (anche speciali e pericolosi), acqua e altre merci, essenzialmente per finalità di sicurezza e gestione efficiente del parco veicoli. Le modalità di funzionamento del sistema consentivano al titolare di visualizzare in tempo reale la posizione degli automezzi, acquisita ogni 120 secondi, il loro stato (fermo o in moto), nonché informazioni di altro tipo (velocità, ore di guida, pause, ecc.). L'intero set dei dati raccolti risultava associabile ai singoli autisti alla guida ed era conservato per un anno, assieme alla mappa dei percorsi effettuati ogni giorno,

L'Autorità ha ritenuto questo sistema «in concreto idoneo a realizzare il monitoraggio continuo dell'attività del dipendente, in violazione dei principi di necessità, pertinenza e non eccedenza (in relazione agli artt. 3 e 11, comma 1, lett. *d)* e *e)* del Codice e 5, par. 1, lett. *c)* e *e)* del Regolamento (UE) 2016/679), considerato anche che il sistema medesimo è stato utilizzato nella versione "standard", in assenza di alcuna istruzione impartita al fornitore del servizio circa le caratteristiche essenziali dei trattamenti da effettuare (…)»[160]. Nella specie, la «raccolta di informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti cui i veicoli sono affidati (…), con una periodicità della rilevazione estremamente ravvicinata (…), non sono state ritenute proporzionate con gli scopi rappresentati dalla società (v. artt. 11, comma 1, lett. *d)* del Codice e 5, par. 1, lett. *c)* del Regolamento (UE) 2016/679) che avrebbero potuto essere utilmente e legittimamente perseguiti con la raccolta di informazioni assai più limitate»[161].

Il Garante ha altresì sottolineato che «il titolare non ha provveduto a configurare il sistema tecnologico mediante misure adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento»[162], richiamando sia l'art. 25 GDPR in materia di *privacy by*

[157] GPDP, Provv. 4 ottobre 2011, doc. *web* n. 1850581.

[158] Il rilievo dei principi di necessità e proporzionalità rispetto all'uso di sistemi di geolocalizzazione in ambito lavorativo è stato ribadito anche a livello sovranazionale: v. ad es. Consiglio d'Europa, *Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale*, adottata dal Comitato dei Ministri il 1° aprile 2015, nel corso della 1224a seduta dei rappresentanti dei Ministri, spec. par. 16; Gruppo di lavoro ex art. 29, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro*, 8 giugno 2017, pp. 22 ss.

[159] GPDP, Provv. 19 luglio 2018, doc. *web* n. 9039945.

[160] *Ibidem.*

[161] *Ibidem.*

[162] *Ibidem.*

design e *by default* sia quanto stabilito in attuazione del principio di necessità dal provvedimento generale del 2011 già citato, relativamente al divieto di monitoraggio continuativo della posizione del veicolo. Sotto tale profilo, pertanto, anche in questa decisione il Garante ha evidenziato la sostanziale continuità tra il principio di necessità di cui agli artt. 3 e 11, co. 1, lett. *d)*, d.lgs. n. 196/2003 e i nuovi principi di protezione dei dati fin dalla progettazione e per impostazione predefinita stabiliti dall'art. 25 GDPR.

Rispetto ai trattamenti svolti nel contesto lavorativo, si richiama altresì il provvedimento del 16 dicembre 2021, relativo agli adempimenti di gestione della posta elettronica aziendale da porre in essere alla cessazione del rapporto di lavoro[163].

Ivi, un datore di lavoro manteneva attivo l'*account* di posta elettronica individuale assegnato a un dipendente anche dopo la cessazione del rapporto d'impiego con quest'ultimo, provvedendo alla sua cancellazione solo dopo che l'interessato presentava reclamo al Garante. Richiamando quanto già stabilito nelle Linee guida per posta elettronica e Internet[164], l'Autorità ha ricordato che i principi di necessità, pertinenza e non eccedenza impongono al titolare, alla cessazione del rapporto di lavoro, di rimuovere gli *account* assegnati al dipendente, previa loro disattivazione e contestuale adozione di sistemi automatici volti ad informarne i terzi e a fornire a questi ultimi indirizzi alternativi riferiti alla sua attività professionale.

Su tali basi, l'Autorità ha accertato la violazione tanto degli artt. 3 e 11, co. 1, lett. *d)* ed *e)*, d.lgs. n. 196/2003, quanto dei "corrispondenti" principi di minimizzazione e limitazione della conservazione [art. 5, par. 1, lett. *c)* ed *e)*, GDPR], posto che i fatti in esame si erano svolti nel vigore sia della normativa previgente sia del GDPR[165].

In ultimo, è opportuno soffermarsi brevemente sulla casistica relativa all'adempimento della valutazione d'impatto, la quale, come si è detto (v. *supra*, par. 2.7), deve recare anche una «valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità» [art. 35, par. 7, lett. *b)*, GDPR][166]. Queste decisioni, infatti, pur non citando espressamente il principio di necessità, consentono di apprezzarne la portata applicativa di carattere generale (v. *supra*, par. 2).

In merito, appare utile richiamare quanto rilevato dal Garante rispetto all'impiego di un sistema di supervisione ("*proctoring*") che era stato previsto dall'Università Bocconi nell'ambito dello svolgimento delle prove d'esame degli studenti, al fine di identificare questi ultimi e verificarne il corretto comportamento durante le prove[167].

---

[163] GPDP, Provv. 16 dicembre 2021, doc. *web* n. 9739653.

[164] GPDP, Provv. 1° marzo 2007, doc. *web* n. 1387522.

[165] In senso conforme, v. GPDP, Provv. 2 luglio 2020, doc. *web* n. 9445180; Provv. 4 dicembre 2019, doc. *web* n. 9215890.

[166] Per un'analisi della disciplina relativa alla valutazione d'impatto sulla protezione dei dati, v. ad es. A. MANTELERO, *La gestione del rischio*, cit., pp. 493 ss.; F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., pp. 285 ss.

[167] GPDP, Provv. 16 settembre 2021, doc. *web* n. 9703988.

Nel caso in questione, l'Autorità ha accertato l'inidoneità della valutazione d'impatto pur svolta dal titolare del trattamento, rilevando come quest'ultima non fosse «stata condotta in maniera del tutto adeguata, limitandosi a illustrare le caratteristiche del sistema di supervisione utilizzato, rappresentandolo come conforme al quadro normativo in materia di protezione dei dati, senza però una puntuale valutazione "della necessità e proporzionalità dei trattamenti in relazione alla finalità" e "dei rischi per i diritti e le libertà degli interessati" (art. 35, par. 7, lett. *b)* e *c)*), anche in termini di possibile condizionamento o pressioni indirette nei confronti degli studenti, riportando giudizi di adeguatezza estremamente sintetici, privi di idonea motivazione»[168].

In particolare, è stato accertato che, rispetto alla "necessità e proporzionalità del trattamento", la DPIA svolta non illustrava «le valutazioni effettuate dal titolare in merito alle ragioni per le quali si è reso necessario adottare uno strumento di supervisione degli esami a distanza dotato di funzioni di riconoscimento facciale e in grado di profilare il comportamento degli studenti durante la prova, nonché i motivi per i quali non fosse possibile fare ricorso a strumenti di supervisione alternativi, ma meno invasivi per i diritti e le libertà degli stessi»[169].

Ne emerge un'attenta valutazione del requisito della necessità, il quale, anche in tal caso, è incluso nella – o comunque rapportato alla – più ampia valutazione della proporzionalità delle limitazioni al diritto alla protezione dei dati personali ed è inteso in senso conforme all'interpretazione di tale concetto fatta propria dalla giurisprudenza europea. Come già indicato, infatti, la Corte di Giustizia UE impone di valutare sia l'efficacia della misura limitativa dei diritti rispetto all'obiettivo perseguito sia l'assenza di altre misure, meno invasive, che consentano il soddisfacimento del medesimo scopo[170].

In conclusione, va comunque rilevato che il Garante, nella verifica dei requisiti di "necessità e proporzionalità" previsti nel contesto della DPIA, ha dimostrato di valorizzare anche altre dimensioni del principio di necessità. Il riferimento, segnatamente, è ai casi in cui detti requisiti sono stati riportati al principio di minimizzazione, nonché all'esigenza di escludere il trattamento di dati personali laddove la finalità del trattamento sia conseguibile con dati anonimi, in linea con l'interpretazione del principio in esame maturata prima dell'applicabilità del GDPR [come si è visto, il citato principio era riportato agli abr. artt. 3 e 11, co. 1, lett. *d)*, d.lgs. n. 196/2003]. Si pensi, ad esempio, al provvedimento del 13 maggio 2021[171], riguardante l'uso, da parte di un ospedale, di una applicazione volta a consentire agli accompagnatori del paziente che accede al pronto soccorso di monitorarne l'iter diagnostico. Ivi, l'Autorità ha accertato che la valutazione d'impatto svolta dalla ASL competente «risultava comunque priva di alcuni degli elementi indispensabili richiesti dall'art. 35, par. 7 del Regolamento e, in particolare, di una valutazione circa (…) la necessità

[168] *Ibidem*.

[169] *Ibidem*.

[170] Sulla necessità di operare un bilanciamento tra le esigenze in "collisione" della protezione e libera circolazione dei dati personali in relazione ai requisiti di necessità e proporzionalità previsti dall'art. 35, par. 7, lett. *b)*, GDPR, nonché ai test di necessità e proporzionalità da effettuare in tale contesto, v. F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 213 ss.

[171] GPDP, Provv. 13 maggio 2021, doc. *web* n. 9687977.

e la proporzionalità dei trattamenti, in relazione alle finalità perseguite, tenuto conto che i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi (cfr. art. 5, par. 1, lett. *c)* e *Considerando* 39 del Regolamento)»[172].

[172] *Ibidem*. Nel medesimo senso, v. GPDP, Provv. 22 agosto 2022, doc. *web* n. 9802752.

Capitolo XI
Il principio di proporzionalità

Carlo Basunti

SOMMARIO: 1. Inquadramento normativo. – 1.1. La proporzionalità nell'alveo dei principi inerenti al trattamento dei dati personali: nota introduttiva per un inquadramento sistematico. – 1.2. La limitazione secondo proporzionalità dei diritti fondamentali: tra la funzione sociale insita nel *considerando* n. 4 del GDPR e l'apertura dell'art. 1, par. 3, del GDPR. – 2. Portata del principio. – 2.1. Il principio di proporzionalità: radici antiche e nuove prospettive di applicazione. – 2.2. Il test di proporzionalità: il (più) corretto bilanciamento tra interessi concorrenti. – 2.3. Il trattamento dei dati personali alla luce del principio di proporzionalità. – 3. Applicazione del principio nella casistica. – 3.1. Il principio di proporzionalità nei provvedimenti del Garante e orientamenti applicativi. – 3.1.1. Applicazione del principio di proporzionalità con riferimento al tempo di conservazione dei dati. – 3.1.2. Applicazione del principio di proporzionalità con riferimento alle modalità di trattamento. – 3.1.3. Applicazione del principio di proporzionalità con riferimento alla condizione di liceità del «legittimo interesse» e, segnatamente, con riferimento alla valutazione del bilanciamento proporzionale degli interessi. – 3.1.4. Applicazione del principio di proporzionalità per la valutazione delle deroghe all'esercizio dei diritti dell'interessato e, in particolare, dei casi di esonero dall'obbligo, per il titolare del trattamento, di rendere l'informativa all'interessato. – 3.2. Il principio di proporzionalità in materia di trattamento di dati personali in ambiti specifici. – 3.2.1. Il principio di proporzionalità quale limite al (e garanzia per il) controllo dei lavoratori. – 3.2.2. L'applicazione del principio di proporzionalità nel settore pubblico in seguito alla sentenza n. 20/2019 della Corte costituzionale: dal bilanciamento tra riservatezza e trasparenza, al diritto all'oblio quale "questione di proporzionalità".

1. Inquadramento normativo

1.1. La proporzionalità nell'alveo dei principi inerenti al trattamento dei dati personali: nota introduttiva per un inquadramento sistematico

La tutela dei dati personali, quale diritto della personalità, sancito a livello europeo a partire dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 16 del TFUE, è circondata e assicurata da diversi principi che vengono previsti all'interno del Regolamento generale sulla protezione dei dati (GDPR)[1]. In

[1] Reg. UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la dir. 95/46/CE. In commento a tale Regolamento, senza pretese di esaustività, si vedano, R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della* privacy *e* data protection, Milano, 2021; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019; G. Finocchiaro (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; V. Cuffaro-R.

questo ambito, spicca sicuramente il principio di proporzionalità che viene esplicitato all'interno di varie disposizioni del GDPR, permeandolo nella sua interezza.

È infatti quanto mai vero che il trattamento dei dati personali richiede un attento bilanciamento, spesso tutt'altro che facile ed immediato, tra interessi confliggenti, tutti meritevoli di tutela, dal quale può emergere la prevalenza e la priorità attribuita ad uno dei suddetti interessi senza tuttavia creare un eccessivo detrimento per quello soccombente. Nel perseguire lo sviluppo dell'economia digitale nell'ambito del mercato interno, è di fondamentale importanza la creazione di un clima di fiducia, anche attraverso una sempre più ampia libertà nella circolazione dei dati personali[2]. Sono tuttavia necessari principi e garanzie stringenti, volti ad evitare lesioni dei diritti fondamentali della persona. In questo senso, il canone di proporzionalità ha una portata trasversale e una centrale importanza in tutti i settori del diritto e non solo: se ne parla infatti in termini di modello globale[3].

L'art. 5 del Regolamento apre il Capo II del testo normativo enumerando i principi applicabili al trattamento dei dati personali e richiamando precisamente i principi di liceità, correttezza, trasparenza [lett. *a)*]; limitazione delle finalità [lett. *b)*]; minimizzazione [lett. *c)*]; esattezza [lett. *d)*]; limitazione della conservazione [lett. *e)*]; integrità e riservatezza [lett. *f)*]; responsabilizzazione o, secondo il più comune e più corretto termine inglese, *accountability*, che, posta al paragrafo 2 della norma, rappresenta una delle novità più rilevanti del Regolamento.

Come si può notare, il principio di proporzionalità non compare nell'elenco di cui all'art. 5 GDPR, ma ciò non perché il Regolamento abbia previsto, seguendo la linea tracciata dalla direttiva c.d. madre (dir. 95/64/CE) di non esplicitare detto principio, ma in quanto dello stesso se ne riscontra il riferimento in molte disposizioni del GDPR. Mentre nella direttiva, infatti, il principio di proporzionalità non trovava spazio, almeno a livello esplicito, nel Regolamento – accanto alla pertinenza e non eccedenza nel trattamento dei dati personali – diventa la chiave di lettura dell'intera normativa, il criterio (esplicito) posto a tutela dei soggetti del trattamento, tracciando i confini entro i quali essi sono tenuti ad operare. Il principio di proporzionalità può essere quindi considerato un cardine della tutela dei dati personali, ove deroghe e limitazioni alla loro protezione devono operare esclusivamente nei limiti dello stretto

D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; L. CALIFANO-C. COLAPIETRO (a cura di), *Innovazione, tecnologia e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Napoli, 2017; G. BUSIA-L. LIGUORI-O. POLLICINO (a cura di), *Le nuove frontiere della* privacy *nelle tecnologie digitali Bilanci e prospettive*, Roma, 2016; L. BOLOGNINI-E. PELINO-C. BISTOLFI (a cura di), *Il regolamento* privacy *europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, I (Dalla direttiva 95/46 al nuovo regolamento europeo) e II (Il regolamento europeo 2016/679)*, Torino, 2016.

[2] Cfr. il *considerando* n. 7 GDPR.

[3] Così K. MÖLLER, *The global model of constitutional rights*, Oxford, 2012; v. anche ID., *From constitutional to human rights: on the moral structure of internation human rights*, in *Global constitutionalism*, 2014, 3, p. 377 in cui l'A. afferma: «*the proportionality principle which dominates that stage has become the by far most important doctrinal principle of constitutional rights law around the world*»; ed anche G. HUSCROFT-B.W. MILLER-G. WEBBER, *Introduction*, in EAD. (a cura di), *Proportionality and the rule of law: rights, justification, reasoning*, Cambridge, 2014, pp. 1 ss.

necessario, con riguardo ai diritti in gioco. In altri termini, il principio di proporzionalità può fungere da guida per ogni operazione di bilanciamento tra diritti antagonisti e tra questi, quello alla protezione dei dati personali. In tal modo, non si può avere una compressione ingiustificata della tutela dei dati: ciò sarebbe infatti in contrasto con il suddetto principio.

La proporzionalità, all'interno del GDPR, viene richiamata innanzitutto nel *considerando* n. 4 nel quale diventa criterio per bilanciare il diritto alla protezione dei propri dati personali (che, come ricorda la norma, non è una prerogativa assoluta) con gli altri diritti fondamentali che possono venire in considerazione[4]. Nel Regolamento sono inoltre presenti altri richiami che si incentrano sullo sforzo richiesto ad un soggetto del trattamento e sulla difficoltà di attuazione di una determinata misura. La proporzionalità diventa quindi il metro attraverso il quale valutare l'azione da compiersi: e così, ad esempio, l'art. 24 valuta secondo proporzionalità i compiti del titolare del trattamento; l'art. 14, par. 5, lett. *b)* prevede, quale deroga all'obbligo del titolare di fornire all'interessato l'informativa riguardante il trattamento effettuato, qualora i dati non siano stati raccolti presso quest'ultimo, il caso in cui la comunicazione delle informazioni risultasse impossibile o implicasse uno sforzo sproporzionato; e, similmente, l'art. 34 sancisce che, laddove lo sforzo sia sproporzionato, il titolare non è tenuto a comunicare il *data breach* all'interessato[5]. La proporzionalità viene poi valutata in sede di DPIA ai sensi dell'art. 35, par. 7, lett. *b)*[6], e richiesta come criterio per la valutazione delle sanzioni *ex* art. 83, par. 9. Si aggiunga che l'applicazione del legittimo interesse *ex* art. 6, par. 1, lett *f)*, GDPR sottende un bilanciamento da effettuarsi secondo proporzionalità: tale bilanciamento, nel d.lgs. 196/2003 veniva effettuato dall'autorità Garante ai sensi dell'art 24, par. 1, lett. *g)*, mentre ora viene rimesso al titolare del trattamento in applicazione del citato principio di *accountability*.

Di particolare rilievo pare essere il *considerando* n. 170 che, nel richiamare le finalità del Regolamento, afferma che il principio di proporzionalità è utile per vagliare la necessità delle azioni intraprese per il raggiungimento di dette finalità. È proprio quest'ultima disposizione che, a parere di chi scrive, racchiude la più ampia espressione del principio in esame applicato alla tematica della tutela dei dati personali: il *considerando* n. 170 potrebbe, infatti, essere astrattamente applicabile a tutte le altre disposizioni contenute all'interno del Regolamento. Se la proporzionalità è il criterio principe per la valutazione del perseguimento della finalità generale del GDPR di garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione europea, allora ogni singola norma del *corpus* normativo nella sua interezza (che sarà sicuramente indirizzata di per sé, a mo' di tassello del mosaico, al raggiungimento di tali finalità) potrà, *rectius*, dovrà, essere valutata alla luce del fondamentale principio di proporzionalità. Il *conside-*

[4] Sul punto vedi *infra* par. 1.2.

[5] A ben vedere, la norma prosegue richiedendo però al titolare di procedere ad una comunicazione pubblica o ad una misura simile per informare comunque gli interessati.

[6] Tra gli elementi che devono essere contenuti nella valutazione di impatto *ex* art. 35, par. 7 GDPR si riscontra, alla lett. *b)* una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità.

rando n. 170, richiamando nella sua formulazione "quanto è necessario", pare poter creare una sovrapposizione tra il principio di proporzionalità e quello di necessità. In realtà, tali principi, seppur strettamente connessi, devono essere tra loro distinti, non formando una semplice endiadi di sinonimi. Riservando riflessioni più dettagliate sul punto alle pagine che seguiranno, ci si limita, in via di prima approssimazione, a sottolineare come detti principi richiedano in realtà due valutazioni distinte delle quali l'una è prodromica all'altra: la valutazione circa la necessità di una misura è antecedente rispetto a quella relativa alla proporzionalità, dal momento che la prima richiama la ricerca della misura, tra le varie idonee, che rechi il minor detrimento per l'interesse concorrente e la seconda, invece, riguarda la valutazione del fatto che il sacrificio imposto ai diritti fondamentali della persona, a causa di una misura volta ad un obiettivo di pubblico interesse, sia ragionevolmente equilibrato[7].

È stato quindi il GDPR, come si è accennato, ad esplicitare il principio di proporzionalità che non era sancito dalla direttiva 95/64/CE (ad eccezione di un paio di semplici richiami ad uno "sforzo sproporzionato")[8]. Giova ricordare che nel nostro Paese, la Commissione per i diritti e doveri relativi a Internet ha approvato, nel 2015, la Dichiarazione dei diritti in Internet, *ivi* l'art. 5, co. 4, prevede: «i dati devono essere trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità (…)», anche se poi si aggiunge che «(…) in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa»; ancora, secondo l'art. 6, co. 2, «la raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata»[9].

In epoca ancor antecedente, la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108 del 1981 – primo atto legislativo disciplinante il trattamento dei dati personali che ha dato impulso alla legislazione della materia a livello comunitario – richiamava, al capitolo II, diversi principi fondamentali per la protezione dei dati personali come quelli di liceità, esattezza, limitazione della conservazione, ma non quello di proporzionalità che viene invece oggi previsto, alla luce delle variazioni, apportate alla Convenzione

---

[7] Nella vastissima letteratura sui test di necessità e di proporzionalità (preceduti in realtà da quello di idoneità), ci si limita qui a richiamare M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, relazione tenuta presso il Palazzo della Consulta nell'ambito della conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola, in Roma il 24-26 ottobre 2013, in particolare p. 5 in cui l'A., richiamando le quattro fasi del giudizio di proporzionalità, analizza la verifica della necessità e della proporzionalità in senso stretto.

[8] Cfr. art. 11, par. 2 e art. 12, lett. *c)* della direttiva 95/46/CE; come è noto l'attuazione della direttiva nell'ordinamento italiano è avvenuta con la l. 31 dicembre 1996, n. 675 che è stata successivamente sostituita dalla l. 30 giugno 2003, n. 196, c.d. Codice *privacy*: in nessuno di questi due corpi normativi il legislatore interno ha inteso discostarsi dal dettato europeo introducendo richiami al principio in esame che veniva però ricavato dal Garante dall'art. 11, par 1, lett. *d)* del Codice *privacy*, in questo senso vedi GPDP, Provv. 29 aprile 2004, doc. *web* n. 1003482 in merito all'istallazione di un impianto di videosorveglianza; sullo stesso tema e con le medesime soluzioni, vedi GPDP, Provv. 8 aprile 2010, doc. *web* n. 1712680.

[9] Cfr. A. MASERA-G. SCORZA (a cura di), *Internet, i nostri diritti*, *Prefazione* di S. RODOTÀ, Roma, 2016.

attraverso il Protocollo di modifica del 18 maggio 2018 (anche noto come Convezione 108+)[10], indirizzate ad avvicinare il regime della Convezione con quello del Regolamento. Precisamente, l'art. 7 del Protocollo che modifica l'art. 5 della Convezione, prevede che il trattamento dei dati personali sia proporzionato ai fini perseguiti oltre a richiedere un giusto bilanciamento tra gli interessi considerati e i diritti fondamentali che sono in gioco.

È quindi proprio grazie al Regolamento se gli studiosi sono stati indotti a ripensare alla tutela dei dati personali alla luce delle più moderne logiche di mercato, fondate (soprattutto) sulla globalizzazione degli scambi e sull'evoluzione tecnologica. Si nota come il legislatore europeo abbia inteso porre la proporzionalità come strumento necessario che l'interprete è tenuto ad utilizzare per il difficile bilanciamento che viene sempre richiesto e dal quale non si può mai prescindere quando ci si occupa del trattamento dei dati personali, data l'impostazione duale[11] del Regolamento, costituita da «due anime»[12]: da un lato, la piena tutela dell'interessato e del suo diritto alla *privacy* e, dall'altro, la libera circolazione dei dati sul mercato ed il contestuale soddisfacimento degli interessi di stampo economico, relativi all'attività di trattamento.

1.2. La limitazione secondo proporzionalità dei diritti fondamentali: tra la funzione sociale insita nel *considerando* n. 4 del GDPR e l'apertura dell'art. 1, par. 3, del GDPR

Il *considerando* n. 4 del Regolamento, dopo aver premesso che il diritto alla protezione dei dati personali non può essere considerato come prerogativa assoluta del singolo, afferma che esso vada contemperato, come si è detto, secondo il principio di proporzionalità, con gli altri diritti fondamentali, aggiungendo che ciò va «considerato alla luce della sua funzione sociale»[13].

È dato ormai acquisito l'inserimento del diritto alla tutela dei dati personali nel catalogo (aperto) dei diritti della personalità[14] il cui elenco presente nel codice

[10] Ratificata dall'Italia il 5 marzo 2019.

[11] In questo senso F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 11 e *passim*.

[12] L'espressione è di N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla* privacy, in Ead. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, p. 36.

[13] La versione italiana della norma parla appunto di "funzione sociale", quella inglese invece afferma che il diritto alla protezione dei dati personali deve essere considerato in relazione alla sua "*function in society*". Anche nella prima frase del *considerando* n. 4 si rinviene una traduzione non precisa rispetto alla versione inglese: se in quella italiana si legge che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo», quella inglese recita «*the processing of personal data should be designed to serve mankind*». Sul punto, pare che la versione inglese in cui si parla di "umanità" e non, più semplicemente di "uomo", sia più efficace nel delineare il fatto che il trattamento dei dati personali si deve esplicare in un'ottica sia economica, sia sociale.

[14] Sul tema v. D. Messinetti, *Personalità (diritti della)*, in *Enc. dir*., XXXIII, 1982, pp. 355 ss. P. Rescigno, *Personalità (diritti della)*, in *Enc. giur. Treccani*, XXIII, Roma, 1990, pp. 1 ss.; V. Zeno Zencovich, *Personalità (diritti della)*, in *Dig. disc. priv*., *Sez. civ*., XIII, Torino, 1995, pp. 430 ss.; G. Giacobbe, *Natura, contenuto e struttura dei diritti della personalità*, in Id., A. Giuffrida, *I diritti della personalità*, Torino, 2000, pp. 23 ss.; sulla preesistenza dei diritti della personalità rispetto

civile risulta attualmente limitato rispetto alle esigenze che emergono nella realtà sociale. Pare allora peculiare la negazione dell'assolutezza della tutela dei propri dati personali che pare essere prospettata dal *considerando* n. 4 del GDPR e che è tuttavia caratteristica fondamentale dei diritti della personalità, canone pratico per sottolineare l'intangibilità della sfera individuale. Tale assolutezza merita però alcune precisazioni ulteriori per evitare di incorrere in veloci e fallaci interpretazioni. A ben vedere, infatti, ai sensi della disposizione, la pretesa di tutela dei propri dati è sì esercitabile *erga omnes*, ma può comunque essere soggetta ad alcune limitazioni. Trattasi, quindi, di un diritto assoluto: l'interessato lo può far evidentemente valere nei confronti di chiunque; ma considerando il suo contenuto che pare potersi qualificare elastico, lo stesso può essere oggetto di previsioni che ne limitano il suo esercizio[15]. Ovviamente, simili restrizioni, pur non rendendo relativo il diritto, devono essere oculatamente bilanciate con gli altri diritti fondamentali da un lato e con gli interessi della società dall'altro, seguendo la strada tracciata dal principio di proporzionalità.

Il riferimento a esigenze di carattere superindividuale si rinviene sia nella citata Convenzione 108/1981, e precisamente all'art. 9, par. 2, che ammette restrizioni alla tutela dei dati personali «per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati» nonché per la protezione della persona interessata e i diritti e libertà di altri[16], sia al par. 2 dell'art. 8 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali dove si prevede la possibile ingerenza della autorità pubblica sul diritto al rispetto della vita privata e familiare qualora essa sia «prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». Circa il significato e la portata dei diritti presenti nella Convenzione EDU, si richiama la Carta di Nizza (art. 52, par. 3) che ammette limitazioni all'esercizio dei diritti e delle libertà *ivi* riconosciuti (e quindi anche con

al loro riconoscimento da parte dell'ordinamento giuridico si rinvia a F. GALGANO, *Trattato di diritto civile*, vol. I, Padova, 2014, p. 171, che afferma come essi siano «trovati» dal diritto oggettivo.

[15] Sono di sicuro interesse le considerazioni svolte sul tema da A. RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali,* in *Contratto e impr.*, 2017, 2, p. 600, in cui l'A. sostiene: «il diritto alla protezione dei dati personali è assoluto, nella misura in cui è riconosciuto a chiunque, garantito solo nell'interesse della persona cui si riferisce e vantabile nei confronti di tutti; è relativo, nella misura in cui possono presentarsi vincoli esterni, tali da restringere o limitare l'esercizio delle pretese» e precisa che «la relatività va riferita al contenuto del diritto alla protezione dei dati personali, all'insieme delle facoltà e delle pretese esercitabili dal titolare, non al diritto in quanto tale. Il contenuto del diritto è relativo in quanto i poteri del titolare possono subire delle limitazioni, conseguenti alla necessaria operazione di bilanciamento tra interessi individuali e valori collettivi».

[16] Si aggiunga che, ai sensi dell'art. 11, par. 1 della Convenzione 108+, si ammettono eccezioni alla previsioni del Protocollo stesso qualora siano previste per legge, rispettose dei diritti e delle libertà fondamentali e costituiscano una misura necessaria e proporzionata in una società democratica per: «*a) the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; b) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression*».

riferimento al diritto alla *privacy ex* art. 7 e alla protezione dei dati personali *ex* art. 8) qualora siano previste per legge e rispettose del contenuto essenziale di tali diritti e libertà che si vanno a limitare. È ancora il principio di proporzionalità ad essere l'architrave per valutare la necessità e la rispondenza delle limitazioni alle finalità di interesse generale che, riconosciute dall'Unione, vadano a tutelare diritti o libertà altrui (art. 52, par. 1)[17].

La funzione sociale, riferita al diritto alla protezione dei dati personali, rende opportuno il richiamo al diritto di proprietà cui la nostra Carta costituzionale riconosce la medesima funzione oltre a «renderla accessibile a tutti» (art. 42)[18]. La funzione sociale riferita alla proprietà – i cui precedenti più noti risalgono alla Costituzione di Weimar e che appare capace di operare soprattutto quando sui beni economici di proprietà di un soggetto si instauri un rapporto che implica la collaborazione altrui – richiede l'adempimento del dovere di solidarietà. La solidarietà è infatti un dovere inderogabile – come previsto dall'art. 2 Cost.[19]: norma d'impronta personalistica, generale e aperta ai valori emergenti nella società – posto alla base della costruzione dello stato sociale che ben si adatta alle esigenze in continuo mutamento. La solidarietà è un principio fondante l'ordinamento giuridico che funge altresì da collante, indirizzando l'azione di ogni soggetto sia pubblico sia privato anche in un'ottica di equilibrio tra interessi contrapposti[20].

---

[17] In commento all'art. 52 della Carta di Nizza vedi T. Groppi, *Commento all'art. 52 Portata dei diritti garantiti*, in R. Bifulco-M. Cartabia-A. Celotto (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001, pp. 351 ss., in particolare pp. 352-353, in cui l'A. sottolinea come «l'art. 52, par. 1, pone una clausola limitativa generale, applicabile a tutti i diritti e le libertà garantiti nella Carta, non ci sono, quindi, diritti il cui esercizio non possa essere sottoposto a limiti, ma le limitazioni debbono avvenire entro il quadro di principi delineato da tale disposizione (…). Riguardo alle tecniche di limitazione dei diritti, la Carta non ha seguito la Convenzione europea dei diritti dell'uomo e molte costituzioni nazionali (tra le quali anche quella italiana), che prevedono limiti specifici per i singoli diritti, ma ha optato per una clausola limitativa generale».

[18] In commento all'art. 42 Cost., vedi S. Rodotà, *Art. 42*, in G. Branca (a cura di), *Commentario della Costituzione*, Bologna-Roma, 1982, pp. 69 ss.; F. Macario, *Art. 42*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Commentario alla Costituzione*, Torino, 2006, I, pp. 864 ss.; sulla funzione sociale del diritto di proprietà la letteratura civilistica è sconfinata, v. per tutti F. Galgano, *Trattato di diritto civile*, vol. I, cit., pp. 377 ss.

[19] Sull'art. 2 Cost. vedi per tutti A. Barbera, *Art. 2*, in G. Branca (a cura di), *Commentario della costituzione*, Bologna-Roma, 1975, pp. 50 ss.

[20] Nella vastissima letteratura che si è occupata del principio di solidarietà, si fa rinvio a G. Alpa, *Solidarietà. Un principio normativo*, Bologna, 2022; P. Rescigno, *Solidarietà e diritto*, Napoli, 2006; F.D. Busnelli, *Il principio di solidarietà e "l'attesa della povera gente", oggi,* in *Riv. trim. dir. proc. civ*., 2013, 2, pp. 413 ss.; S. Rodotà, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014; M. Tampieri, *La riscoperta del principio di solidarietà,* in *Jus civile*, 2020, 3, pp. 612 ss.; B. Bertarini, *Il principio di solidarietà tra diritto ed economia. Un nuovo ruolo dell'impresa per uno sviluppo economico inclusivo e sostenibile*, Torino, 2020. Sul principio di solidarietà in materia di protezione dei dati personali si veda inoltre, segnatamente, F. Bravo, *Il principio di solidarietà*, nel presente volume al Cap. XIV, nonché Id., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, pp. 405; Id., *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf.*, 2023, 3, p. 481 ss.

La funzionalizzazione sociale della proprietà è servita per superare quella che era l'identificazione totale tra ottimo economico e interesse dei singoli – concetto caratterizzante l'intero titolo relativo ai rapporti economici –, operando così una netta cesura tra il vecchio e il nuovo modo di intendere la proprietà. A ben vedere, laddove un diritto (quale, ad esempio, la protezione dei dati personali) sia qualificato come inviolabile, gli interventi restrittivi del diritto stesso devono essere considerati assolutamente eccezionali e non applicabili per analogia; differente è invece la conclusione se riferiamo al diritto (anche)[21] una funzione sociale; infatti, la tutela offerta all'interessato (o al proprietario) è, in quest'ultima ipotesi, fortemente depotenziata e aumentano i casi in cui può essere considerato legittimo un intervento restrittivo del diritto, non essendo più presenti nemmeno le strettoie che la disciplina generale dell'interpretazione della legge richiede per le norme di natura eccezionale. Le maglie entro cui sono circoscritte le limitazioni ai diritti fondamentali, per quanto non del tutto inestricabili, sono comunque ben salde, e proprio sul punto interviene il principio di proporzionalità come faro da seguire per bilanciare nella maniera più corretta le opposte esigenze del caso concreto.

I diritti fondamentali, visti nel loro insieme, si inseriscono in un tessuto normativo e sociale complesso all'interno del quale altri diritti o altri interessi possono (legittimamente) limitarne la portata[22]. La funzione sociale si ravvisa dunque nella possibilità per il contenuto del diritto di subire una compressione al fine di tutelare interessi di cui si afferma la priorità (assoluta o nel caso di specie), senza che ciò comporti però una sua ablazione *tout court*[23]. Più precisamente, le limitazioni non paiono essere apportate al diritto in sé, quanto alla sua operatività in determinate circostanze qualificate: la sostanza, e quindi anche la possibile estensibilità del diritto (e non l'estensione nel caso concreto), rimane invariata.

Il privato, pertanto, non rileva unicamente come *singulus*, ma come membro di una *societas* per l'interesse della quale accetta (o comunque subisce) determinate limitazioni ai suoi diritti. La funzionalizzazione del diritto privato avviene principalmente al fine di tutelare determinate categorie di soggetti il cui bisogno di protezione

[21] In seno all'assemblea costituente fu proposto dall'On. Corbino un emendamento (poi respinto) indirizzato ad aggiungere la parola "anche" legata alla funzione sociale della proprietà, con l'intento di rendere tale funzione un elemento solo eventuale e non caratterizzando in maniera profonda e innovativa l'intera disciplina.

[22] Cfr. M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, cit., p. 9, in cui l'A. afferma che «nella Costituzione italiana, ogni diritto è sempre predicato assieme al suo limite e, in questo ambito, il bilanciamento è una tecnica interpretativa e argomentativa che consente il necessario ragionevole contemperamento di una pluralità di interessi costituzionali concorrenti».

[23] Si rinvia a E. NAVARRETTA, *Diritto civile e diritto costituzionale*, in *Riv. dir. civ*., 2012, 5, pp. 673-674, in cui l'A. richiama anche il pensiero di Radbruch che parla di "*konventionelle Luge*", ossia di menzogna convenzionale rispetto a modelli di ispirazione socialista; sono poi interessanti le considerazioni che l'A. svolge a p. 680 avendo riguardo al pluralismo che caratterizza l'istituto della proprietà: «non solo vi sono alcune proprietà inviolabili, come quella all'abitazione, ma vi sono anche proprietà – come quelle dei beni collettivi e dei beni comuni – che, pur richiedendo ancora un'adeguata ricostruzione sul terreno privatistico, lasciano intravedere un volto radicalmente nuovo della funzione sociale».

assurge ad interesse diffuso di cui si fa carico lo Stato, intervenendo sulla situazione del singolo titolare del diritto[24]. Quindi, anche con riguardo al trattamento dei dati personali, qualora esso incida su diritti fondamentali altrui o sia strumentale a bisogni generali, le pretese del singolo possono essere proporzionalmente compresse.

Le osservazioni incentrate sul *considerando* n. 4 del Regolamento trovano vieppiù conferma nel terzo comma dell'art. 1 del Regolamento stesso: norma alla quale detto *considerando* è strettamente legato al fine di non limitare né, tantomeno, vietare la libera circolazione di tali dati.

Richiamando l'indirizzo, che da sempre ha contraddistinto la politica europea, diretto alla realizzazione di un mercato unico efficiente con riguardo alla libera circolazione di merci (parte terza, titolo II, TFUE), persone, servizi e capitali (parte terza, titolo IV, TFUE) ed ora anche di dati, si precisa come i lavori di Lisbona superino il *focus* di attenzione esclusiva sui diritti fondamentali, non annichilendo in tal guisa gli obiettivi iniziali. L'art. 1 par. 3 del GDPR non vuole fissare un rapporto gerarchico tra i due diritti *ivi* contemplati: ciò vorrebbe dire sottrarsi al vaglio di proporzionalità previsto dall'art. 52, par. 1 della Carta di Nizza, fonte di rango sovraordinato rispetto al Regolamento. La norma del Regolamento da ultimo richiamata intende solo sottolineare quale tra i due diritti abbia portata limitante nei confronti dell'altro[25]. Tale disposizione è occasione per il legislatore europeo per confermare l'importanza che i dati personali, e più precisamente la loro libera circolazione, hanno ai fini dell'efficienza del mercato dell'Unione. Si è voluta ribadire la forte dinamicità che caratterizza i dati personali in rapporto al mercato e agli scambi che comunque devono essere circondati da garanzie stringenti al fine di offrire una piena

[24] Cfr. S. Mazzamuto, *Libertà contrattuale e utilità sociale*, in *Europa e dir. priv*., 2011, 2, p. 370; v. pure M. Nuzzo, *Utilità sociale e autonomia privata*, Milano, 1974.

[25] Sul tema vedi F. Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?,* in *Contratto e impr*., 2018, 1, pp. 205-206, p. 209, e p. 315, in cui l'A. riscontra nell'art. 1, par. 3, GDPR una norma avente il fine di «orientare l'operazione di bilanciamento, nel senso di trarre indicazioni da essa per una valutazione su quale debba essere considerato il diritto o la libertà fondamentale "recessivo" o "limitante" e quale quello "prevalente", in difetto di ulteriori indicazioni emergenti da altre disposizioni di dettaglio. La costruzione della norma *de qua* (art. 1, par. 3, del reg. cit.), là dove impedisce al diritto alla protezione dei dati personali di avere un effetto limitante nei confronti della libertà di circolazione dei dati, conduce ad attribuire a quest'ultima – e non al primo – il ruolo di diritto "limitante" o "recessivo". Ne consegue che l'interprete, nell'operare il bilanciamento, sarà tenuto ad individuare quali siano le condizioni limitanti il diritto alla protezione dei dati personali (assunto come diritto "prevalente") e quale sia l'estensione di tali limiti, sotto il profilo quantitativo (al fine di rendere "proporzionale" la predetta limitazione, che deve operare entro i confini di idoneità, necessità e stretta proporzionalità, rispetto al diritto o alla libertà "limitante")»; vedi pure Id., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., p. 210 ss., in cui l'A. rileva anche come la norma in questione sia piuttosto generica e non circoscriva la fattispecie, non permettendo quindi "*ex se*" di operare il bilanciamento con la libera circolazione dei dati, secondo i criteri di idoneità, necessità e stretta proporzionalità, per via della mancanza delle c.d. "leggi di collisione", ovvero delle «regole che consentono di valutare quando siano soddisfatti i criteri specifici contenuti all'interno dell'art. 52, par. 1, per condurre il contemperamento proporzionale di fronte alla fattispecie concreta, che invece ci si aspetta siano contenute nel più complesso articolato normativo racchiuso nell'intero regolamento».

tutela dei diritti dell'interessato: pare dunque che il principio di proporzionalità sia uno strumento euristico fondamentale per operare questo genere di valutazioni.

Posto quindi che l'interesse del singolo a far valere il diritto alla protezione dei dati personali può essere limitato, si deve aver riguardo al modo in cui ciò può avvenire e quindi alle metodiche che devono essere assunte a tal fine. È proprio la proporzionalità la chiave di volta che aiuta l'interprete nell'incessante sforzo diretto alla ricerca del giusto punto di equilibrio fra l'interesse individuale e quello superindividuale; il mezzo per un corretto bilanciamento tra le pretese dell'interessato, degli altri soggetti del trattamento e della comunità tutta; il principio utile per evitare che sotto il velo del bene comune si possa celare una qualche forma di abuso.

2. PORTATA DEL PRINCIPIO

2.1. Il principio di proporzionalità: radici antiche e nuove prospettive di applicazione

Il principio di proporzionalità viene storicamente collegato alle due immagini metaforiche fornite, la prima dalla dottrina tedesca e la seconda dalla giurisprudenza anglosassone, e rispettivamente: «la polizia non deve sparare ai passeri con i cannoni»[26]; non si deve «utilizzare un martello pneumatico per rompere una noce quando basterebbe uno schiaccianoci»[27]. Mentre Aristotele, nell'Etica Nicomachea[28], aveva già riscontrato un collegamento tra l'idea di proporzione e quella di giustizia, tale principio, è stato probabilmente coniato da Cicerone per tradurre il termine greco, all'epoca oscuro, *ἀναλογία*[29].

[26] F. FLEINER, *Institutionen des Deutschen Verwaltungsrechts*, Tübingen, 1912, p. 354, secondo cui «*die Polizei soll nicht mit Kanonen auf Spatzen schießen*»; metafora utilizzata anche da W. JELLINEK, *Gesetz. Gesetzanwendung und Zweckmässigkeitserwägung*, 1913, rist. Aalen, 1964, pp. 289 ss.

[27] *House of Lords*, 20 gennaio 1983, *R. v Goldstein,* in *Weekly Law reports*, p. 155, in cui Lord W.J.K. Diplock afferma: *«the principle of proportionality prohibits the use of a steam hammer to crack a nut, if a nutcracker would do»*. Lord Diplock nel definire metaforicamente il principio di proporzionalità sottolinea come esso derivi dal diritto tedesco.

[28] In particolare, ci si riferisce al libro V dell'Etica Nicomachea di Aristotele.

[29] Nella traduzione del Timeo di Platone si comprende che il termine non era ancora utilizzato nella lingua latina dal momento che Cicerone, rivendicandone con orgoglio il conio, afferma: «*id optime adsequitur, quod Graece ἀναλογία, Latine (audiendum est enim, quondam haec primum a nobis novantur) comparatio proportiove dici potest*» (CIC., *Tim.*, 13).

Il principio in esame, consolidatosi in area germanica[30], è stato caratterizzato da una «irresistibile ascesa»[31] nel diritto europeo, importante collettore delle esperienze degli ordinamenti interni, ed in quello dei vari Stati membri, soprattutto grazie alla giurisprudenza della Corte di giustizia dell'Unione europea.

Le metafore richiamate pongono l'attenzione sul rapporto tra mezzi e fini, base del principio che, in via di prima approssimazione, potremmo definire come il criterio per stabilire il (più) corretto rapporto tra lo scopo che si intende perseguire ed il mezzo da impiegare per raggiugere detto scopo. In realtà, ciò non è sufficiente poiché i mezzi utilizzati non possono essere vagliati unicamente in rapporto al fine perseguito, ma anche (e soprattutto) avendo riguardo agli altri diritti fondamentali la cui tutela può senza dubbio limitare e finanche escludere l'utilizzo di determinati mezzi. Solo laddove il beneficio raggiunto realizzando lo scopo prefigurato sia meritevole di maggior tutela rispetto alla limitazione di un diritto, si potrà affermare che la scelta adottata sia proporzionata[32]. Il mezzo prescelto deve certamente essere idoneo per il fine, ma deve inoltre consistere nel giusto *mètron* di potere utilizzato, avuto riguardo al sacrificio che si impone al soggetto e agli altri diritti fondamentali concorrenti.

Il principio di proporzionalità che permea i vari settori del diritto, è atto a presiedere l'esercizio della discrezionalità laddove taluni poteri possano incidere negativamente nella sfera giuridica di un soggetto: il rapporto che ne emerge è infatti quello tra il potere pubblico e l'interesse del singolo individuo. Gli interventi dei pubblici poteri devono dunque essere limitati a quanto strettamente necessario per

---

[30] Precedentemente alla metafora di Fleiner, il principio di proporzionalità viene utilizzato in qualità di termine tecnico-giuridico in G.H. Von Berg, *Handbuch des Teutschen Policeyrechts*, Hannover, 1802, p. 67; se ne ebbe poi un recepimento nella giurisprudenza nel 1882 per mezzo della sentenza *Kreuzberg* del tribunale amministrativo superiore prussiano, sentenza 14 giugno 1882, in *Entscheidungen des preußisches Oberverwaltungsgerichts*, 9, pp. 353 ss. In tale pronuncia, il principio di proporzionalità diviene un freno all'illimitata discrezionalità dell'autorità di polizia. Per una ricostruzione delle radici del principio di proporzionalità v. D.U. Galetta, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Milano, 1998; Id., *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'unione europea)*, in *Riv. it. dir. pubbl. com.*, 2019, 6, pp. 908 ss., e in particolare, p. 909, in cui l'A. afferma che nella sentenza *Kreuzberg* si «è chiaramente sottolineato come non appaia accettabile l'idea di una discrezionalità priva di limitazioni da parte dell'autorità di Polizia (…): poiché per il perseguimento del bene comune (…) non può operarsi un sacrificio totale dell'individuo e della sua posizione giuridica (…). Ad essa fanno seguito, di lì a poco, due pronunzie successive del Tribunale amministrativo superiore prussiano: a partire dalle quali il ragionamento sulla proporzionalità diviene giurisprudenza costante»; nel caso *Kreuzberg*, la Corte aveva ritenuto invalida l'ordinanza di chiusura di un negozio alimentare in quanto privo di licenza per la vendita e distribuzione di alcol, senza che fosse stata ponderata, in concreto, la possibilità di adottare un provvedimento sanzionatorio di minor incisività, vedi sul punto A. Barak, *Proportionality. Constitutional Rights and Their Limitation*, Cambridge, 2012, pp. 178 ss.; in argomento cfr. anche M. Heintzen, *Il principio di proporzionalità: un cosmopolita tedesco del diritto costituzionale*, Modena, 2015.

[31] Così P. Martens, *L'irresistible ascension du principe de proportionnalité*, in Aa.Vv. (a cura di), *Présence du droit public et des droits de l'homme. Mélanges offerts à Jacques Velu*, I, Bruxelles, 1992, pp. 49 ss.

[32] A. Barak, *Proportionality. Constitutional rights and their limitation*, Cambridge, 2012, p. 132.

raggiungere l'obbiettivo perseguito e devono recare il minor detrimento possibile ai diritti individuali.

È proprio dall'esperienza tedesca del *Bundesverfassungsgericht* che la Corte di giustizia UE ha mutuato il principio di proporzionalità in ambito europeo per poi diffonderlo negli altri ordinamenti interni degli Stati comunitari. A livello normativo, è stato inserito a partire dal Trattato di Maastricht del 1992, collegato al canone di necessità (art. 3 B, Titolo II), per essere poi disciplinato nel TUE (art. 5) e nella Carta di Nizza (art. 52, par. 1)[33]. Per la giurisprudenza della Corte di giustizia, il principio di proporzionalità gioca da sempre un ruolo fondamentale per la realizzazione delle politiche socio-economiche, assumendo una funzione trasversale: strumento di controllo dell'azione delle istituzioni dell'Unione nonché della validità degli atti comunitari da un lato e, dall'altro, mezzo per valutare la liceità della condotta degli Stati membri in ottemperanza a misure europee e nell'ambito delle deroghe previste in loro favore sulla base dei Trattati[34].

Il principio di proporzionalità, dai confini senz'altro labili, il cui rispetto, in una logica preventiva, richiama anche il principio di precauzione[35], è, a maggior ragione nel contesto attuale, un fondamentale criterio di riferimento, un presupposto strutturale dell'ordinamento e dei più recenti approdi dell'evoluzione giuridica. In questa ottica, possiamo notare come tale principio interessi molteplici settori della scienza giuridica e tra questi, sicuramente, l'ambito del trattamento dei dati personali nel quale assurge a principio fondamentale.

Nell'articolata cornice dei principi del trattamento dei dati personali, quello di proporzionalità, quale canone ermeneutico per valutare l'operato del titolare, diviene uno strumento di *private enforcement*, capace di presidiare i plurimi diritti che si fronteggiano nelle operazioni di trattamento, componendo i contrasti che inevitabilmente sorgono in tali fattispecie, con l'obiettivo di garantire un modello di sviluppo sostenibile del mercato dei dati.

---

[33] Vedi *supra*, par. 1.2.

[34] Già in Corte di giustizia UE, 24 settembre 1984, n. 181, *Man Sugar*, in *Racc*., 1985, pp. 2889 ss.; sul tema v. *ex multis* M.C. CICIRIELLO, *Il principio di proporzionalità nel diritto comunitario*, Napoli, 1999, pp. 157 ss., e pp. 168-169.

[35] In questa sede ci si limita, nella vasta letteratura sul tema, a richiamare E. AL MUREDEN, *Principio di precauzione, tutela della salute e responsabilità civile*, Bologna, 2008; ID., *Danno da cellulare e doveri di informazione: tra precauzione e autoresponsabilità*, in *Corr. giur*., 2020, 3, pp. 73 ss.; C. IPPOLITI MARTINI, *Principio di precauzione e nuove prospettive della responsabilità civile della pubblica amministrazione*, Milano, 2022; ID., *Gestione del servizio idrico e responsabilità civile della P.A. tra precauzione, prevenzione e risarcimento*, in *Contratto e impr*., 2016, 3, pp. 663 ss.; M.E. ARBOUR, *A proposito della nebulosa. Principio di precauzione-responsabilità civile*, in Liber amicorum *per F.D. Busnelli. Il diritto civile tra principi e regole*, vol. I, pp. 513 ss.; G. COMANDÈ (a cura di), *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, Milano, 2006.

2.2. Il test di proporzionalità: il (più) corretto bilanciamento tra interessi concorrenti

Il principio di proporzionalità trova applicazione nel diritto vivente attraverso un test, nato nell'esperienza tedesca[36], strutturato in tre fasi a concatenazione progressiva che guidano i giudici nella verifica del rispetto del suddetto principio. Soprattutto quando sono in ballo i diritti fondamentali della persona, alle Corti è richiesto di assicurare un corretto bilanciamento, *rectius*, il più corretto bilanciamento tra l'impatto sui diritti che vengono compressi e lo scopo che i pubblici poteri intendono perseguire. Tale controllo trifasico, utilizzato appunto in Germania per valutare l'idoneità, la necessità e la proporzionalità in senso stretto di una misura, non ha tuttavia trovato diffusione in tutti i Paesi: in Italia, ad esempio, non se ne è fatto ampio utilizzo ad opera della Corte costituzionale dove il principio di proporzionalità è perlopiù richiamato insieme a quello di ragionevolezza[37].

I tre gradini di giudizio tendono solitamente ad essere tratteggiati con taglio netto e schematico più che altro per ragioni espositive, ma nella realtà tali passaggi sono sfumati e fluidi, pur rappresentando, sul piano concettuale, tappe logiche l'una susseguente all'altra, concatenate in un sistema di interdipendenze ed interferenze[38]. La mancanza, infatti, del requisito richiesto dal primo *step* (ossia, l'idoneità) renderà inutile l'analisi dei successivi due gradini in merito alla scelta intrapresa.

Il test di idoneità è volto a verificare che la misura che si intende adottare (che va a limitare uno o più diritti fondamentali) sia effettivamente posta in essere per i fini superindividuali perseguiti per la tutela di altri diritti fondamentali (destinati a prevalere nel caso concreto). La valutazione ha quindi ad oggetto la coerenza del mezzo impiegato, la sua idoneità, appunto, a produrre effetti apprezzabili rispetto al risultato che si è prefigurato. È quindi un'analisi atta a comprendere quale strumento sia effettivamente quello più utile, operando così una prima selezione[39]. Raramente tale prima fase esaurisce il giudizio complessivo di proporzionalità, rappresentando, il più delle volte, un mero presupposto per le fasi successive: affinché un atto sia considerato inidoneo, occorrerebbe infatti che il mezzo utilizzato fosse del tutto inappropriato fin dal piano della sua causalità materiale o perfino dannoso[40]. Si sottolinea come, solitamente, la verifica di idoneità della misura debba aver riguardo al fine che viene espressamente dichiarato dall'autorità pubblica, senza dover approfondire

---

[36] Ne dà contezza, offrendone un'ampia analisi basata sulle pronunce del *Bundesverfassungsgericht,* N. Emiliou, *The Principle of proportionality in European Law. A Comparative Study*, Londra, 1996, pp. 26 ss. Le tre fasi nelle quali, in area tedesca, il principio di proporzionalità si declina sono: "*Geeignetheit*", "*Erforderlichkeit*" e "*Verhältnismässigkeit im engeren Sinne*".

[37] V. per tutti Corte cost., 1° giugno 1995, n. 220, in *Giur. cost*., 1195, pp. 1642 ss., secondo cui il principio di proporzionalità «rappresenta una diretta espressione del generale canone di ragionevolezza (*ex* art. 3 Cost.)».

[38] Cfr. S. Cognetti, *Principio di proporzionalità. Profili di teoria generale e di analisi sistematica*, Torino, 2011, pp. 226 ss.

[39] Cfr. A. Sandulli, *La proporzionalità dell'azione amministrativa*, Padova, 1998, in particolare p. 368.

[40] G. Scaccia, *Il principio di proporzionalità*, in S. Mangiameli (a cura di), *L'ordinamento europeo. L'esercizio delle competenze*, Milano, 2006, p. 250.

quelli che potrebbero essere altri fini, non manifesti, ma realmente ispiratori della misura. Ora, posta la grande improbabilità con la quale la pubblica autorità dichiarerebbe un fine palesemente illegittimo, se il giudizio di idoneità si limitasse realmente a ciò, finirebbe per perdere di concretezza[41]. Qualora, comunque, un mezzo idoneo fosse indebitamente oppressivo, si dovrà passare al successivo livello di analisi.

Il test di necessità, che presuppone la precedente valutazione di idoneità, è invece il richiamo alla regola del c.d. mezzo più mite o, secondo la terminologia inglese, il *least restrictive means*. Si tratta di un limite quantitativo all'azione che si intende porre in essere: si ha in questa sede riguardo alla ricerca del mezzo, tra i vari utilizzabili e capaci di raggiungere lo scopo, che arreca un minor detrimento per gli altri diritti o interessi che, seppur soccombenti nel caso concreto, necessitano di una tutela. La ricerca del mezzo più mite può risultare piuttosto complessa in quanto richiede un'indagine di natura prettamente tecnica con apprezzamenti di natura economico relazionale e riflessioni che possono porre in secondo piano l'argomentazione giuridica[42]. Di più, la "necessità" si combina con lo *step* precedente dell'idoneità: esso rileva sia nella scelta sull'*an* dell'esercizio di un potere sia, in caso di risposta positiva, sullo strumento da utilizzare. Si mirerà quindi a seguire la strada che, compatibile con il fine del pubblico interesse, comporterà i minori sacrifici possibili per gli interessi confliggenti[43]. Laddove però vi sia, nel caso di specie, un solo mezzo adottabile, tale mezzo sarà sicuramente anche necessario, dal momento che non può essere sostituito con un mezzo più mite: si ha così, in una simile circostanza, una sovrapposizione di fatto tra idoneità e necessità[44]. Riprendendo le due metafore utilizzate da Fleiner e Lord Diplock[45], si nota come in detti casi, le scelte di sparare ai passeri con un cannone o di rompere una noce con un martello pneumatico, siano senz'altro idonee allo scopo, ma non rispettino sicuramente il canone della necessità. Del resto, se da un lato un mezzo necessario è sicuramente idoneo, non per forza è vero anche il contrario: un mezzo idoneo non è infatti sempre anche necessario.

Quando i vari mezzi, tutti aventi il medesimo livello di idoneità, abbiano anche la stessa portata lesiva, si potrà agilmente e indifferentemente scegliere tra loro, data la parità di *pros* e *cons*. Quando invece tali mezzi, tutti aventi lo stesso livello di incidenza negativa, abbiano un differente livello di idoneità, la scelta ricadrà su

---

[41] Una simile considerazione è offerta da G. PINO, *Diritti fondamentali e ragionamento giuridico*, Torino, 2008, p. 135, nt. 101, dove afferma «particolare curioso: talvolta si dice, come riportato nel testo, che la verifica deve riguardare il fine *dichiarato* della misura impugnata, senza indulgere in speculazioni su eventuali fini reconditi; ebbene, poiché difficilmente l'autorità politica *dichiarerà* di perseguire un fine illegittimo, allora il controllo su quest'ultimo requisito non potrà che essere pleonastico, al limite della farsa».

[42] Questi rilievi vengono esposti da G. SCACCIA, *Il principio di proporzionalità*, cit., p. 259.

[43] A. SANDULLI, *La proporzionalità dell'azione amministrativa*, cit., pp. 372-373.

[44] J. BARNES, *Introduccion al principio de proporcionalidad en el derecho comparado y comunitario*, in *Rev. Administración Públ*., 1994, 135, p. 506 in cui l'A. afferma: «*el principio de necesidad se edifica sobre el de idoneidad, que es su presupuesto lógico, es decir, presume la existencia de varios medios útiles entre los que es posible optar. Si, por el contrario, no hay más que un instrumento idóneo para la satisfacción de la finalidad perseguida, será por definición necesario puesto que no habrá elección ni contraste posible*».

[45] Vedi *supra*, par. 2.1.

quello con il più alto coefficiente di idoneità, data la pari efficacia negativa. Casi di problematicità più elevata sono quelli in cui i mezzi selezionati hanno differenti livelli di idoneità e, al contempo, variabili potenzialità di danno: se è infatti vero che si dovrebbe scegliere quel mezzo che risulti più consono per la realizzazione dello scopo perseguito e meno gravoso, non sempre una simile scelta è possibile o agevole. Qualora il mezzo più idoneo non sia infatti anche quello che arrechi il minor detrimento per gli interessi contrapposti, l'indagine della necessità dovrà cedere il passo al successivo *step* della proporzionalità in senso stretto[46].

Pare potersi affermare che la mitezza del mezzo impiegato non debba solamente aver riguardo agli effetti negativi che subisce il soggetto, ma anche ai costi che vengono impiegati per porre in essere detto mezzo. È quindi necessario, per rispettare il criterio in esame, ricercare il mezzo meno dispendioso, in un'ottica di costi e benefici, nel rispetto del principio di economicità.

L'ultima fase, quella più difficile e di più rara applicazione, è quella della proporzionalità in senso stretto, o come talvolta si preferisce, della adeguatezza, volta all'indagine degli effetti dell'azione: i benefici verranno in questa sede soppesati con i costi richiesti per ottenerli[47]. In questa sede, si opera quindi una valutazione comparativa tra l'incisività dell'intervento pubblico e il detrimento patito dal singolo. Precisamente, si avrà riguardo al rapporto tra frustrazione del diritto e ragioni per le quali tale frustrazione viene operata, ricordando però che non si può incidere sul contenuto essenziale del diritto[48]. Tale terzo gradino del giudizio di proporzionalità richiede che i vantaggi ottenuti ponendo in essere la misura, siano superiori rispetto agli effetti negativi sofferti dal singolo, pretendendo che l'importanza relativa dei mezzi e dei fini, sia equamente bilanciata. Quanto più si riterrà di dover intervenire nella sfera giuridica del singolo, tanto più rilevante dovrà essere l'interesse superindividuale che si persegue con l'azione sottoposta al vaglio di proporzionalità[49]. Verrà quindi analizzato il peso che gli obiettivi cui si mira hanno nel caso concreto; se, in altre parole, valga la pena perseguire detti obiettivi o se, piuttosto, il sacrificio che si impone al concorrente interesse non sia eccessivo[50], intollerabile[51], smisurato, e,

[46] G. Scaccia, *Il principio di proporzionalità*, cit., p. 266.

[47] Vedi M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, cit., p. 5, in cui si afferma: «è in questa dimensione esperienziale che il giudice – rispondendo all'immagine che lo rappresenta nell'iconografia di ogni tempo, con la bilancia in mano – può bilanciare i diritti e gli interessi in gioco, ricerca la soluzione che più di ogni altra persegue in modo equilibrato la massima espansione di tutti i diritti e i valori».

[48] Cfr. G. Morbidelli, *Corte costituzionale e Corti europee: la tutela dei diritti (dal punto di vista della corte di Lussemburgo),* in *Dir. proc. amm.*, 2006, 2, p. 298.

[49] D.U. Galetta, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, cit., p. 39.

[50] G. Pino, *Diritti fondamentali e ragionamento giuridico*, cit., p. 137.

[51] Il Cons. Stato, 17 aprile 2007, n. 1736 parla, in riferimento alla valutazione di adeguatezza, di «tollerabilità della restrizione che (la misura) comporta per il privato», in *Foro it*., 2007, 11, cc. 550 ss.; v. anche G. Martinico-M. Simoncini, *An italian perspective on the Principle of Proportionality*, in S. Vogenauer-S. Weatherill (a cura di), *General Principles of Law*, Portland, 2017, p. 223, in cui, nell'analisi del principio di proporzionalità in senso stretto, si richiede che «*the measure may not impose an intolerable burden on the individuals that it affects*».

come tale, sproporzionato. Sarà perciò recessivo quell'interesse pubblico il cui raggiungimento determina compressioni intollerabili per i diritti dei destinatari.

Si nota come i tre gradini di analisi hanno il comune obiettivo di arrivare alla scelta ottimale per il caso concreto, ma mentre i primi due hanno riguardo alle effettive possibilità, ad alternative nella realtà di fatto, la proporzionalità in senso stretto è un giudizio effettuato tra alternative giuridiche[52].

La proporzionalità, che fonda il bilanciamento tra fine perseguito e detrimento provocato per raggiungerlo, garantisce che non si vada ad annullare il contenuto essenziale del diritto del singolo che nel caso concreto cede il passo ad interessi e diritti considerati come prevalenti. Anche laddove si richiedesse la compressione di situazioni giuridiche soggettive per fini che travalicano l'interesse individuale, è sempre necessaria un'attenta valutazione, diretta ad un intervento proporzionato che non vada ad incidere negativamente sul contenuto essenziale dei diritti.

2.3. Il trattamento dei dati personali alla luce del principio di proporzionalità

Il principio di proporzionalità, si è detto, è un principio generale, immanente il diritto europeo e, con particolare riguardo all'ambito dei diritti fondamentali della persona, e tra questi al diritto alla tutela dei dati personali, è la chiave per ottenerne la giusta limitazione laddove questa appaia necessaria. La sua applicazione in questo settore è di indubbia utilità, data la conflittualità che si origina a causa della natura stessa del "bene" che circola: *asset* negoziale strategico da un lato, ma, dall'altro, espressione della personalità dell'individuo e quindi non sfruttabile come una qualsiasi merce[53].

Il principio di proporzionalità viene sovente richiamato in coppia dialettica con l'affine, ma differente, principio di necessità. Quest'ultimo, che riveste particolare importanza nell'alveo delle condizioni di liceità del trattamento dei dati personali[54], precede il giudizio in merito alla proporzionalità e sembra rappresentare la

---

[52] In questo senso R. ALEXY, *Theorie der grundrechte*, Baden Baden, 1994, p. 101, secondo cui «*der verhältnismässigkeit im engeren Sinne folgt daraus, dass Prinzipien Optimierungsgebote relativ auf die rechtlichen möglichkeiten sind. Die grundsatze der Erfordlichkeit und der Geeignetheitfolgen demgegenuber aus dem Character der Prinzipien als Optimierungsgebote relativ auf die tatsächlichen Möglichkeiten*».

[53] Sul principio di proporzionalità in materia di protezione dei dati personali si veda F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 160 ss. e, spec., pp. 188 ss.; nonché ID., *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, cit., pp. 190 ss.; A. CARAVITA DI TORITTO, *La proporzionalità multilivello nel mercato "presidiato" dei dati personali*, in *Media Laws*, 2021, 3, pp. 157 ss.

[54] Sulle condizioni di liceità del trattamento dei dati personali v. per tutti l'ampia analisi di F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 110 ss.; con particolare riferimento al consenso, cfr. P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ*., 2022, 6, pp. 1054 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021; P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; sia poi consentito il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello*

prima cesura a possibili restrizioni del diritto, richiedendo appunto che esse siano limitate a quanto strettamente necessario. Pare quindi potersi affermare che, qualora la misura che si intende porre in essere non superi con esito positivo il sindacato di necessità, ad esso non dovrà far seguito quello di proporzionalità.

L'*European Data Protection Supervisor* (EDPS) ha redatto una breve ed agile guida operativa su come affrontare il test di proporzionalità e quello di necessità nel loro reciproco rapporto[55]. Tale guida consta di otto *steps* consecutivi: i primi quattro dedicati all'*assessment* della necessità, gli altri quattro a quello inerente alla proporzionalità. Seguendo tale percorso, si dovrebbe operare una descrizione fattuale della misura da adottare; identificare quei diritti che, eventualmente, potrebbero subire limitazioni ad opera del trattamento dei dati che si intende porre in essere (in particolare il diritto alla *privacy* e alla protezione dei dati personali), ricordando però che il nucleo essenziale di tali diritti non potrà, comunque, essere compresso né, tantomeno, annullato; in seguito, definire i fini che si intendono perseguire con la misura e, tra tali fini, sia la tutela di altri diritti fondamentali in gioco sia altri fini di interesse generale, avendo riguardo alla funzione sociale che, ai sensi del *considerando* n. 4 GDPR, viene riconosciuta alla tutela dei dati personali[56]; la scelta ricadrà quindi su quell'opzione che sia al contempo dotata di una maggior efficacia (rispetto al fine) e di una minor intrusività (rispetto ai diritti che vengono limitati).

Avendo poi propriamente riguardo al *proportionality assessment*, si attuerà una valutazione dell'importanza del fine perseguito e dell'idoneità della misura da adottare per perseguirlo: una adeguata analisi degli scopi è infatti fondamentale anche per la *compliance* con l'art. 52, par. 1 della Carta di Nizza; si dovrà in seguito valutare la portata e l'intensità dell'interferenza, operata dalla misura che si intende adottare, sui diritti dei soggetti coinvolti; si porrà in essere una valutazione circa la *fair balance* della misura e, infine, laddove la misura non risulti proporzionata nel caso di specie, si dovranno introdurre dei *safeguards*, riportando la valutazione entro i canoni della proporzionalità.

Risultano di particolare interesse le linee guida, redatte dall'EDPS sia in riferimento alla necessità sia alla proporzionalità: il primo documento, risalente all'11 aprile 2017[57] e il secondo, che interessa maggiormente in questa sede, emanato il 19 dicembre 2019[58]. L'EDPS sottolinea come i principi di necessità e proporzionalità siano due requisiti essenziali – strettamente collegati, ma comunque distinti[59] – da

specchio delle condizioni di liceità del trattamento dei dati personali, in *Contratto e impr*., 2020, 2, pp. 860 ss.

[55] EDPS, *Quick guide to necessity and proportionality*, del 28 gennaio 2020.

[56] Sul punto v. *supra*, par. 1.2., nonché F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 188 ss.

[57] EDPS*, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit,* dell'11 aprile 2017.

[58] EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* del 19 dicembre 2019. Tale documento fornisce (pp. 12 ss.) anche una ampia spiegazione della guida in 8 *steps* di cui si è innanzi parlato richiamando anche importanti decisioni della Corte di giustizia dell'Unione europea.

[59] EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* cit., p. 5 dove si legge «*it is essential to highlight*

valutare qualora una misura incida su diritti fondamentali, comprimendoli. Le condizioni alle quali tali diritti possono essere limitati vanno pertanto indagate a fondo, proprio perché sono in grado di determinare l'estensione con la quale essi possono essere goduti.

L'emersione del requisito della proporzionalità, uno degli sviluppi più sorprendenti degli ultimi dieci anni in tema di *data privacy law*[60], richiede un attento esercizio di bilanciamento, soppesando la portata (negativa) dell'interferenza sui singoli soggetti con l'importanza (presuntivamente positiva) del fine ultimo. Per comprendere però l'effettivo impatto che detta interferenza può avere, e quindi per poterne proficuamente analizzare il peso, si dovranno tenere in considerazione vari fattori, e tra questi, sicuramente: il numero di soggetti che subiscono la compressione dei loro diritti; l'estensione temporale della limitazione; la natura dell'attività sottoposta alla limitazione (se ad esempio si tratta di attività che impongono un obbligo di riservatezza o se il processo prevede l'uso di decisioni automatizzate con un significativo margine di errore); se gli interessati sono persone vulnerabili; ancora, se i diritti fondamentali che vengono limitati nel caso concreto, oltre a quello alla *privacy* e alla protezione dei dati personali, sono anche altri, inestricabilmente collegati ai primi[61].

Lo scrutinio di proporzionalità risulta quindi essere tutt'altro che semplice, anche e soprattutto quando il caso concreto ha a che vedere con il diritto alla protezione dei dati personali. Il bilanciamento che viene richiesto va al di là di quella che è la ricerca dell'ottimo paretiano, non è neppure sufficiente un semplicistico discorso sul rapporto costi-benefici. I "costi" che un intervento può comportare per un diritto fondamentale vanno infatti analizzati utilizzando anche il metodo *Law and Economics*[62], tenendo ben presente che non potrà essere considerata ammissibile una misura che incida sul nucleo essenziale del diritto in questione. Il bilanciamento circa l'azione in favore dell'interesse superindividuale, trova quindi un limite nel *quantum* sopportabile, imposto al singolo, a prescindere dall'importanza dell'azione stessa per la società. Il *favor* per l'azione rivolta all'interesse collettivo trova pertanto un limite, non prefissato e da individuare caso per caso, nel "costo" che ogni soggetto può essere ragionevolmente tenuto a sopportare.

Ma c'è di più.

Il trattamento dei dati personali deve necessariamente essere governato da un'idea di giustizia che si esplichi non solo, e non tanto, in astratto, ma anche, e

---

that necessity and proportionality, even though strictly linked to each other (both conditions must be fulfilled by the legislation), entail two different tests».

[60] In questo senso si esprime L.A. BYGRAVE, *Data Privacy Law. An International Perspective*, Oxford, 2014, p. 147, riportato in EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* cit., p. 11.

[61] EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., pp. 22-27.

[62] Sul tema si rinvia alle autorevoli considerazioni di G. CALABRESI, *Il futuro del law and economics. Saggi per una rimeditazione ed un ricordo*, F. FIMMANÒ-V. OCCORSIO (a cura di), trad. ad opera di D. MALTESE, Presentazione di E. AL MUREDEN, Milano, 2018; si rinvia altresì a E. AL MUREDEN, *Il futuro del Law and Economics nel pensiero di Guido Calabresi*, in *Riv. dir. civ*., 2018, pp. 779 ss., e a G. ALPA, *Il futuro di "Law & Economics": le proposte di Guido Calabresi*, in *Contratto e impr*., 2016, 3, pp. 597 ss.

soprattutto nel concreto del suo procedimento applicativo. L'esigenza di giustizia, nella costante tensione dialettica tra *Nomos* e *Dike*, è, infatti, connaturata anche alle operazioni di trattamento[63].

Il principio di proporzionalità, nella sua evoluzione, da schema giuridico per la valutazione degli atti amministrativi con valenza sanzionatoria a criterio generale di risoluzione dei conflitti tra diritti, pare poter svolgere un ruolo pregnante nel dare risposta alle nuove questioni che il rapido mutamento sociale pone (e porrà) al diritto. Tale principio è, pertanto, funzionale alla ricerca del giusto punto di equilibrio tra diritti e principi concorrenti – tra i quali non esiste un ordine gerarchico aprioristicamente stabilito –, la cui composizione può ben mutare nel corso del tempo, proprio come è accaduto nell'ambito della protezione e circolazione dei dati personali. Come si è precedentemente accennato, infatti, se nella vigenza della direttiva 95/46/CE ed in seguito all'emanazione del Codice *privacy*, le istanze personalistiche assumevano una rilevanza preminente, con l'avvento del GDPR, le suddette istanze vengono poste, già all'art. 1 della normativa, sullo stesso piano della libera circolazione dei dati e, dunque, della possibilità di un loro sfruttamento sul mercato.

Un ruolo essenziale in tale cambio di paradigma – nell'ottica di un nuovo bilanciamento, indirizzato al rafforzamento del "diritto" al trattamento[64] –, è giocato dalla perdita di centralità del consenso[65] tra le basi giuridiche del trattamento che viene oggi equiparato alle altre condizioni di liceità ad esso equipollenti, privando così l'interessato, in talune circostanze, della valutazione discrezionale in merito alla legittimità del trattamento[66].

La mutata prospettiva, che caratterizza il fenomeno circolatorio dei dati personali, è espressione della profonda incidenza che l'evoluzione tecnologica ha avuto in questo settore, inducendo il legislatore ad un ripensamento degli equilibri fondanti la disciplina in esame. Del resto, «immaginare che il bilanciamento sia operato una volta per tutte dal legislatore, così definitivamente risolvendo ogni indice valutativo, significherebbe negare l'essenza stessa del diritto come esperienza sociale»[67].

In questo scenario, il giusto bilanciamento non può che essere ricercato caso per caso ed il mezzo teleologicamente indirizzato a tale fine è senza dubbio il principio di proporzionalità, capace, da un lato, di mostrare di volta in volta quale diritto debba prevalere e, dall'altro, di arginare derive che conducano ad un annichilimento del diritto soccombente: è, dunque, funzionale a calare la giustizia nel caso di specie.

Anche nell'ambito dei dati personali, il principio di proporzionalità si mostra, quindi, vero protagonista: presupposto indefettibile (prima), strumento fondamentale (durante) e metro di giudizio (dopo) per gli operatori del diritto.

---

[63] Le lucide argomentazioni di N. Lipari, *Elogio della giustizia*, Bologna, 2021, spec. pp. 59 ss. sembra possano essere proficuamente calate anche nel contesto del trattamento dei dati personali.

[64] In questo senso, cfr. F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit.

[65] Sul punto sia consentito rinviare a C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit.

[66] Lo osserva, in modo condivisibile, N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla* privacy, cit., pp. 36-37 e nt. 4.

[67] Così N. Lipari, *Elogio della giustizia*, cit., p. 60.

3. Applicazione del principio nella casistica

3.1. Il principio di proporzionalità nei provvedimenti del Garante e orientamenti applicativi

3.1.1. *Applicazione del principio di proporzionalità con riferimento al tempo di conservazione dei dati*

Il Garante per la protezione dei dati personali ha mostrato di fare ampio ricorso al principio di proporzionalità, nei propri provvedimenti, applicandolo in diverse direzioni.

Una di esse riguarda la valutazione relativa alla congruità del tempo di conservazione dei dati e, in generale, del tempo relativo al trattamento dei dati in riferimento alle finalità perseguite: il Garante mostra di applicare il principio di proporzionalità per adattare i criteri ordinari al caso di specie, apportando deroghe in ragione delle modalità specifiche con cui la fattispecie concreta si presenta, estendendo i tempi di conservazione dei dati trattati per raggiungere le finalità legittime di trattamento.

Con riguardo al tema della fidelizzazione dei clienti, l'autorità Garante aveva preso in esame, con un provvedimento generale[68], i tempi di conservazione dei dati acquisiti, in applicazione del principio di proporzionalità. In tale occasione, partendo dal presupposto secondo il quale i dati personali dei quali non appare necessaria la conservazione devono essere cancellati o comunque trasformati in forma anonima, il Garante aveva previsto la possibilità di conservare i dati relativi al dettaglio degli acquisti effettuati dal cliente (individuabile), per finalità di profilazione o *marketing*, per un periodo che non eccedesse, rispettivamente dodici e ventiquattro mesi a partire dalla loro registrazione. Si lasciava poi la possibilità di adire l'Autorità per ottenere un *prior check* ai sensi dell'ora abrogato art. 17 Codice *privacy*[69], in merito alla sussistenza di motivazioni tali da permettere una conservazione dei dati più estesa nel tempo. Numerosi sono stati i provvedimenti[70] del Garante emessi in seguito alla presentazione di tale istanza di verifica preliminare da parte del titolare del trattamento: il vaglio ha avuto ad oggetto la proporzionalità dell'arco temporale previsto per la conservazione dei dati dei clienti per le sopra citate finalità di profilazione o *marketing* diretto.

Al fine di valutare se il limite temporale di dodici o ventiquattro mesi potesse ridurre in modo significativo l'utilità dell'attività posta in essere dal titolare del

[68] GPDP, Provv. 24 febbraio 2005, doc. *web* n. 1109624.

[69] L'art. 17 Codice *privacy* è stato abrogato dal citato d.lgs. 101/2018 che ha quindi limitato sensibilmente la possibilità di consultazione preventiva dell'autorità Garante, ora prevista unicamente *ex* art. 36 GDPR con riguardo alla valutazione di impatto.

[70] *Ex multis* v. GPDP, Provv. 22 maggio 2018, doc. *web* nn. 9019902; 9018611; 9019890; 9022048; 9022056; 9019882; 9018628; 9020270; 9020258; 9020250; 9020242; 9018611; vedi, inoltre, GPDP, Provv. 5 luglio 2017, doc. *web* n. 6844421; GPDP, Provv. 18 maggio 2016, doc. *web* n. 5260385; GPDP, Provv. 2 dicembre 2015, doc. *web* n. 4642844.

trattamento, si è presa in considerazione la collocazione del prodotto venduto dal titolare, e precisamente se tale merce si potesse collocare in una fascia medio-alta o meno. Solamente laddove il prodotto sia considerato di livello medio-alto, il Garante ha previsto la possibilità di estendere i tempi di conservazione dei dati personali della clientela proprio perché simili categorie merceologiche presentano una frequenza media di acquisto piuttosto bassa, tale da vanificare le finalità perseguite dal titolare qualora le operazioni di trattamento non si potessero protrarre per un tempo più lungo. Il rispetto dei tempi di conservazione dei dati dei clienti, di dodici o ventiquattro mesi avrebbe reso, invero, di fatto impossibile o, comunque, priva di efficacia qualsiasi attività di profilazione della clientela con riguardo agli acquisti compiuti. Si è pertanto deciso di estendere a sette anni, decorrenti dalla loro registrazione, il tempo massimo di conservazione dei dati personali dei clienti di quelle società-titolari del trattamento che vendono prodotti di fascia medio-alta e obbligare al rispetto dei termini di dodici o ventiquattro mesi gli istanti non in possesso di detto requisito. Va da sé che, allo scadere del tempo previsto, i dati raccolti debbano essere cancellati o trasformati in forma anonima in modo permanente e non reversibile.

Similmente, il Garante per la protezione dei dati personali si è espresso con riferimento al tempo di conservazione dei dati raccolti per mezzo della videosorveglianza. La conservazione delle immagini acquisite deve essere commisurata al tempo necessario in rapporto alle finalità perseguite, nel rispetto del principio di proporzionalità e comunque senza che si eccedano i sette giorni[71]. Scopi specifici e determinati sui quali si basa la videosorveglianza, proprio come nel caso della profilazione dei clienti, possono però rappresentare la ragione per (la richiesta al Garante di) una dilazione del periodo di conservazione dei dati di una settimana, stabilito, come si è detto, quale limite massimo. Un'estensione temporale della facoltà di conservare i dati può essere infatti sottoposta ad una verifica preliminare del Garante, ma deve essere ipotizzata dal titolare del trattamento come eccezionale, pur sempre in conformità al principio di proporzionalità. Il titolare dovrà fornire adeguata motivazione in merito alle esigenze di sicurezza perseguite, in aderenza ad eventi concreti e realmente incombenti. che rendono pertanto necessario un più ampio lasso temporale di conservazione dei dati[72]. Tale sistema, del quale si sottolinea l'eccezionalità

[71] GPDP, Provv. 8 aprile 2010, doc. *web* n. 1712680 che, nel riportare i tempi di conservazione, afferma: «la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana».

[72] GPDP, Provv. 8 aprile 2010, doc. *web* n. 1712680, cit. che aggiunge: «il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto (…), con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi

rispetto alla regola, trova pertanto il suo fondamento nel principio di proporzionalità e, precisamente, nel nesso che deve sussistere tra mezzi impiegati e fini perseguiti.

Il richiamato rapporto mezzo-fine viene preso in considerazione dal Garante anche in materia di geolocalizzazione di veicoli aziendali, laddove non ha ritenuto conforme al principio di proporzionalità il trattamento effettuato da una società, da un lato con riguardo al tempo (eccessivo) di conservazione dei dai dati (365 giorni), dall'altro, come si dirà, con riferimento alle modalità, certo non necessarie, di acquisizione dei dati stessi[73].

automatici di *expiring* dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare»; v. anche, GPDP, Provv. 18 ottobre 2012, doc. *web* n. 2138277 che ha ammesso la conservazione dei dati per un periodo (massimo) di trenta giorni data la «specifica esigenza di sicurezza, in relazione ad una concreta situazione di rischio riguardante un evento realmente incombente» che, nel caso di specie, riguardava la prevenzione e la repressione di azioni atte a sottrarre opere d'arte conservate nel museo archeologico di Ascoli Piceno; in senso conforme GPDP, Provv. 17 novembre 2011, doc. *web* n. 1877929 che ha esteso ad un periodo di venti giorni la possibilità di conservare i dati acquisiti, data la necessità da un lato di garantire la certezza del denaro riscosso, versato presso la cassaforte e giunto alla società incaricata delle operazioni di rendicontazione, dall'altro di tutelare l'interesse dei lavoratori che solo in tal modo possono avere garanzia della corrispondenza tra il versamento effettuato e l'importo rendicontato; e GPDP, Provv. 18 gennaio 2018, doc. *web* n. 7968051 che ha autorizzato la conservazione delle immagini registrate dal sistema di videosorveglianza presente a bordo delle navi da crociera per quattordici giorni, tempo ritenuto necessario per la ricostruzione di eventuali condotte illecite; come pure GPDP, Provv. 7 luglio 2011, doc. *web* n. 1836347 in merito alla videosorveglianza all'interno di un'azienda metalmeccanica al fine di prevenire atti di sabotaggio per cui si è prevista un'estensione temporale di ventiquattro mesi; e GPDP, Provv. 14 dicembre 2017, doc. *web* n. 7450667 relativa all'istanza presentata da una società fornitrice di soluzioni di installazione, manutenzione e assistenza tecnica, con riguardo ad impianti e tecnologie di produzione di energia: si è in tal caso allungato il periodo di conservazione dei dati raccolti a sei mesi dal momento che le tempistiche standard non permetterebbero alla società di accertare eventuali illeciti o ammanchi di materiale; cfr. inoltre GPDP, Provv. 18 aprile 2018, doc. *web* n. 8995078; GPDP, Provv. 8 marzo 2018, doc. *web* n. 8763222 in cui il Garante afferma che in casi in cui non sia solo presente l'esigenza di tutelare il patrimonio dell'azienda, ma anche il personale ed i dati dei clienti, e in cui vi sia un'estrema delicatezza dei servizi gestiti: «una loro eventuale manomissione potrebbe non solo arrecare grave danno al patrimonio aziendale, ma sarebbe anche in grado di mettere in pericolo la gestione e messa in sicurezza di dati, di informazioni e di contenuti fondamentali per la continuità dello svolgimento delle attività degli stessi clienti. Infatti, in alcuni casi, eventuali condotte illecite, compromettendo l'operatività dei clienti, determinerebbero un impatto dannoso anche su alcune rilevanti attività economiche italiane. Tali obiettive circostanze già permettono di ritenere che i siti in questione siano caratterizzati da specificità che giustificano l'adozione di standard di sicurezza di livello superiore alla media»; GPDP, Provv. 9 gennaio 2020, doc. *web* n. 9263597 dove si sottolinea come spetti al titolare del trattamento «individuare i tempi di conservazione delle diverse tipologie di dati personali in relazione a ciascuno degli scopi in concreto perseguiti, facendo riferimento alla finalità principale per la quale il sistema è stato adottato».

[73] GPDP, Provv. 28 giugno 2018, doc. *web* n. 9023246; in senso conforme v. anche GPDP, Provv. 19 luglio 2018, doc. *web* n. 9039945; si è invece considerato legittimo e rispettoso del principio di proporzionalità il trattamento sottoposto al vaglio, ad esempio, in GPDP, Provv. 16 marzo 2017, doc. *web* n. 6275314 nel quale, precisamente, si è ritenuto che la previsione di conservare i dati per un periodo di novanta giorni sia conforme ai principi di necessità e proporzionalità; in argomento, cfr. anche GPDP, Provv. 9 gennaio 2020, doc. *web* n. 9263597 in cui viene evidenziato che «l'eventuale implementazione della raccolta e conservazione dei dati di localizzazione deve essere valutato alla

3.1.2. *Applicazione del principio di proporzionalità con riferimento alle modalità di trattamento*

In altra direzione, il principio di proporzionalità è stato utilizzato dal Garante per valutare, sempre con riferimento al caso concreto, le modalità del trattamento dei dati personali impiegate per raggiungere le finalità legittimamente perseguite dal titolare del trattamento.

La geolocalizzazione – che, come si è visto, è stata materia utile per mostrare come il principio di proporzionalità venga utilizzato quale strumento per adattare al meglio le regole generali al caso di specie, con riferimento al tempo di conservazione dei dati – risulta essere un valido punto di riferimento per segnalare come il principio di proporzionalità venga impiegato anche con riferimento alle modalità utilizzate per effettuare il trattamento.

Il Garante ha infatti affermato[74] che determinate modalità di trattamento utilizzate dal titolare al fine di controllare i veicoli aziendali non siano proporzionate a detto scopo: segnatamente si trattava della raccolta di informazioni eccessivamente particolareggiate sull'attività dei singoli veicoli e quindi, indirettamente, sul lavoro degli autisti di tali veicoli, come ad esempio la precisa ricostruzione su mappa del tragitto percorso sia in tempo reale sia giornalmente, con l'ulteriore ricostruzione puntuale, per ciascuna tratta, non solo del percorso effettuato, ma anche delle modalità (includendo quindi anche le pause), utilizzando un intervallo di rilevazione molto ravvicinato (120 secondi). Lo scopo perseguito dall'impresa potrebbe infatti essere raggiunto con l'impiego del *least restrictive means* e quindi di modalità meno invasive, ma comunque pienamente idonee ai fini prefigurati. L'autorità Garante ha evidenziato come, nel caso di specie, ben si sarebbe potuto adottare il dispositivo di disattivazione della geolocalizzazione durante le pause previste nello svolgimento dell'attività lavorativa: l'adozione di un simile dispositivo sarebbe stata in linea con il principio di proporzionalità[75].

Sul punto, assume particolare importanza l'identificabilità degli autisti geolocalizzati, a partire dalla (ampia) definizione di «dato personale» contenuta nell'art. 4 GDPR. Affinché l'interessato del trattamento possa essere identificabile, infatti, si ha riguardo alla sua identificabilità sia in via diretta quanto in via indiretta. Proprio in base a questo assunto, il Garante non ha considerato dirimente la dichiarazione di una società che aveva sottolineato come i dispositivi GPS, deputati alla geolocalizzazione dei propri autisti, fossero collegati alla targa dell'automezzo e non al singolo conducente. L'associazione del dispositivo al numero di targa, invero, anche qualora la guida dell'automezzo sia affidata a persone diverse che si avvicendano tra loro, consente sicuramente al titolare del trattamento di identificare il guidatore attraverso l'associazione con altre informazioni a disposizione come, ad esempio, i documenti relativi ai turni di servizio[76].

luce dei principi di proporzionalità e minimizzazione dei dati»; e GPDP, Provv. 17 gennaio 2022, doc *web* n. 9737210.

[74] GPDP, Provv. 28 giugno 2018, doc. *web* 9023246, cit.

[75] GPDP, Provv. 28 giugno 2018, doc. *web* 9023246, cit.

[76] In questo senso, GPDP, Provv.15 dicembre 2022, doc. *web* n. 9861249.

In un altro provvedimento[77], relativo al trattamento dei dati personali dei dipendenti di una società attraverso la localizzazione di dispositivi *smartphone* e *tablet*, al fine di ammettere il trattamento, risulta cruciale l'argomentazione del Garante concernente il rispetto dei principi di necessità e proporzionalità nella scelta delle modalità per effettuare il trattamento.

Di particolare rilievo ai fini del discorso che si sta svolgendo, sono altresì le considerazioni espresse dal Garante in relazione al trattamento dati effettuato dall'ormai nota *app* Immuni[78]. L'autorità Garante si è soffermata sulla possibilità di considerare come proporzionato il sistema di allerta operato attraverso tale *app*, proprio in ragione delle modalità utilizzate, «volte a garantire in misura sufficiente il rispetto dei diritti e le libertà degli interessati attenuandone i rischi derivanti dal trattamento»[79]. Posta infatti l'esigenza di avviare un sistema di *contact tracing,* ba-

[77] GPDP, Provv. 30 novembre 2017, doc. *web* 7522639 secondo cui «le modalità di trattamento dei dati personali da parte del sistema tecnologico prospettato, così come rappresentate dalla società, in particolare la pseudonimizzazione dei dati dei *controller* e la circostanza che il trattamento dei dati relativi alla sua posizione geografica non sia effettuato ad intervalli predeterminati né continuativamente, bensì esclusivamente al momento dell'attivazione da parte del *controller* (di fronte ad un numero civico o in un punto determinato della verifica a campione) risultano conformi ai principi di necessità, pertinenza e non eccedenza in relazione alle finalità perseguite dalla società»; sul tema, conformemente, v. pure GPDP, Provv. 24 maggio 2017, doc. *web* 6495708 per il caso di un trattamento derivante dalla rilevazione di coordinate satellitari relative alla geolocalizzazione di apparati elettronici; e GPDP, Provv. 11 settembre 2014, doc. *web* 3474069 nonché GPDP, Provv. 9 ottobre 2014, doc. *web* 3505371, entrambi relativi al trattamento dei dati personali dei dipendenti attraverso la localizzazione di dispositivi *smartphone*; si richiama inoltre, in tema di videosorveglianza GPDP, Provv. 8 aprile 2010, doc. *web* 1712680, cit. secondo cui risulta necessario che «l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite»; v. pure GPDP, Provv. 22 luglio 2021, doc. *web* n. 9685994 e GPDP, Provv. 10 giugno 2021, doc. *web* n. 9675440.

[78] Il riferimento è al *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19*- App *Immuni*: GPDP, Provv. 1° giugno 2020, doc. *web* 9356568; tale provvedimento è stato poi seguito da GPDP, Provv. 25 febbraio 2021, doc. *web* n. 9555987 per l'aggiornamento della valutazione d'impatto effettuata dal Ministero della salute; e da GPDP, Provv. 24 novembre 2022, doc. *web* n. 9837022 per l'autorizzazione a continuare il trattamento relativo al sistema di allerta Covid-19. Sulle problematiche sollevate dal tracciamento effettuato dall'*App* Immuni con particolare riferimento al diritto alla protezione dei dati personali v. C. CAMARDI-C. TABARRINI, Contact Tracing *ed emergenza sanitaria. "Ordinario" e "straordinario" nella disciplina del diritto al controllo dei dati personali*, in *Nuova giur. civ. comm*., *Speciale digitale*, 2020, 3, pp. 32 ss.; D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, in *Persona e Mercato*, 2020, 2, pp. 65 ss.; A. CELOTTO, *"Immuni" e la Costituzione*, in *Giust. civ. com.*, 29 aprile 2020; P. TEREZA, *Immuni e tracciamento digitale: fra protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, in *Nuove leggi civ. comm*., 2020, 5, pp. 1134 ss.; M. PLUTINO, *"Immuni". Un*'"exposure notification app" *alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, in *dirittifondamentali.it*, 2020, 2, p. 553 ss.; sul bilanciamento degli interessi e sulle misure adottate per la protezione dei dati personali al tempo della pandemia vedi le considerazioni di G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, in *Giust. civ.com*, 5 maggio 2020; V. CUFFARO-R. D'ORAZIO, *La protezione dei dati personali ai tempi dell'epidemia*, in *Corr. giur*., 2020, 6, pp. 729 ss.

[79] Così GPDP, Provv. 1° giugno 2020, doc. *web* 9356568, cit.

sato sulle moderne tecnologie digitali, finalizzato al contrasto della diffusione del virus Sars-Cov-2 (responsabile della pandemia da Covid-19), si è assicurato che detto sistema, pur dotato di adeguate misure di prevenzione e diagnosi per facilitare la presa in carico ad opera del Sistema Sanitario Nazionale, delle persone contagiate, nonché la rapida individuazione di focolai di infezione, rispettasse i diritti e le libertà degli interessati.

L'esclusione di ogni obbligatorietà nell'utilizzo dell'*app*[80], la confinazione del trattamento ai soli dati di prossimità, resi tra l'altro anonimi o almeno pseudonimizzati, la circoscrizione della raccolta dei dati unicamente a quelli utili per avvisare gli altri utenti dell'avvenuto contatto con un soggetto risultato positivo, l'automatica cancellazione delle TEK (*temporary exposure key*) e degli RPI (*rolling proximity identifier*) dopo quattordici giorni, l'esclusione del ricorso alla geolocalizzazione dei dispositivi degli utenti, sono tutti elementi che denotano il rispetto del principio di proporzionalità, rispetto ai fini perseguiti, nelle modalità di impostazione e funzionamento dell'*app* Immuni e quindi del trattamento dei dati da questa effettuato.

La *data protection law* è stata chiamata ad affrontare una nuova sfida che deve necessariamente essere fronteggiata bilanciando attentamente il diritto alla salute, inteso anche come interesse della collettività *ex* art. 32 Cost. e quindi anche in una prospettiva solidaristica, con gli altri diritti fondamentali della persona come il diritto alla protezione dei propri dati personali. Un siffatto bilanciamento non può certo prescindere dal puntuale rispetto dei principi fondamentali del trattamento, e tra questi, sicuramente, quello di proporzionalità.

3.1.3. *Applicazione del principio di proporzionalità con riferimento alla condizione di liceità del «legittimo interesse» e, segnatamente, con riferimento alla valutazione del bilanciamento proporzionale degli interessi*

Altra direzione in cui il Garante mostra di adottare il principio di proporzionalità del trattamento ha riguardato le valutazioni in ordine alla sussistenza del bilanciamento proporzionale tra gli interessi riconducibili all'interessato e al titolare del trattamento (o a soggetti terzi), da porre a base dell'accertamento del legittimo interesse, quale condizione di liceità del trattamento dei dati personali, alternativa rispetto al consenso[81].

[80] Affrontano efficacemente il tema di questa soluzione C. Camardi-C. Tabarrini, Contact Tracing *ed emergenza sanitaria. "Ordinario" e "straordinario" nella disciplina del diritto al controllo dei dati personali,* cit., pp. 37-38; G. Resta, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, cit., pp. 10 ss.; D. Poletti, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, cit., p. 70; L. D'Arcangelo, Contact tracing *e protezione dei dati nella fase 2 dell'epidemia da Covid-19 (anche nel rapporto di lavoro)*, in *Giust. civ. com.*, 8 maggio 2020.

[81] Sull'inadeguatezza del consenso a costituire sempre idonea base giuridica del trattamento dei dati personali, sia consentito il rinvio a C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., spec. p. 873, in cui si afferma che: «non si deve infatti ritenere che il consenso costituisca sempre il fondamento più adeguato perché svariati possono essere i casi nei quali questo risulti solo apparente, non capace pertanto di legittima-

Sul punto giova ricordare, seppur in via di massima sintesi, che il GDPR chiude il novero delle condizioni di liceità del trattamento con la previsione di un concetto piuttosto indeterminato: quello di legittimo interesse (art. 6, par. 1, lett. *f)*)[82]. Si tratta di una base giuridica la cui valutazione, sulla scorta del principio di *accountability*, viene sottratta ad una verifica dell'interessato nonché ad una valutazione preventiva del Garante, mentre spetta all'autonoma valutazione del titolare del trattamento, restando quindi possibile per l'interessato e per il Garante unicamente un vaglio successivo[83]. La responsabilità del bilanciamento che viene in questa sede richiesto ricade, pertanto, sul titolare che sarà tenuto a valutare con prudenza gli interessi del *data subject*, in rapporto con i suoi, in modo da poter dimostrare come gli interessi facenti capo a lui (o a un terzo) siano tali da superare quelli dell'interessato, senza, tuttavia, porre in pericolo i diritti e le libertà dell'interessato con riguardo alla protezione dei dati personali, prestando poi particolare attenzione all'interessato minore di età. In questo quadro, il Regolamento viene in aiuto del titolare con le indicazioni previste nei *considerando* nn. 47-50.

Nei provvedimenti del Garante relativi alla valutazione del menzionato bilanciamento tra interessi, la proporzionalità del trattamento si ritiene assicurata dalla previsione di indicazioni limitative del trattamento, poste a garanzia dell'interessato, per rendere effettiva la protezione dei dati personali nella fattispecie concreta, salvaguardando al contempo il raggiungimento delle finalità legittime perseguite dal titolare del trattamento.

Un esempio in tal senso si può rinvenire in un provvedimento[84] del Garante relativo alla verifica preliminare del trattamento dei dati connesso all'adozione di un sistema di dispositivi indossabili (c.d. *body cam*) per la raccolta e trasmissione di

re il trattamento; casi in cui avrebbe un effetto distorsivo in quanto prestato senza contezza di tutte quelle informazioni che al soggetto sarebbero necessarie».

[82] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 185, che afferma: «i confini della norma sono piuttosto labili»; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it*., 2019, 12, pp. 2787 ss., che descrive tale condizione di liceità come la «più problematica».

[83] *Amplius* sul tema F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, *supra cit*., pp. 185 ss., che sottolinea la differenza dell'attuale assetto normativo con quello del Codice *privacy* prima dell'intervento di riforma avutosi con il d.lgs. 101/2018 e ricorda che l'abrogata disposizione codicistica (art. 24, co. 1, lett. *g)*) richiedeva che l'operatività di tale condizione di liceità fosse ammessa nei soli casi previsti dall'autorità Garante, «sicché il vaglio di meritevolezza degli interessi sottesi al trattamento dei dati, ai fini dell'accertamento della liceità, e la loro ponderazione rispetto ad altri interessi concorrenti o confliggenti veniva rimessa all'autorità di controllo e non al titolare del trattamento, che ben avrebbe potuto approfittare altrimenti della propria posizione e delle proprie prerogative per travalicare irrimediabilmente le esigenze di tutela volute dall'ordinamento a salvaguardia dei diritti dell'interessato».

[84] GPDP, Provv. 22 maggio 2018, doc. *web* 8995107; simile ragionamento viene offerto anche, ad esempio, nel provvedimento GPDP, Provv. 18 aprile 2018, doc. *web* 9358266, relativo a un sistema di localizzazione geografica di dispositivi aziendali; come pure GPDP, Provv. 18 aprile 2018, doc. *web* 8987133, relativo ad un sistema di registrazione, trascrizione ed analisi di chiamate *inbound*; e GPDP, Provv. 16 febbraio 2017, doc. *web* 6164054, relativo all'installazione di apparecchiature di rilevazione audio-video su navi da crociera; in argomento v. anche GPDP, Provv. 11 novembre 2021, doc. *web* n. 9725891; e GPDP, Provv. 11 gennaio 2023, doc. *web* n. 9861827.

immagini nell'ambito del trasporto ferroviario. La società di trasporti manifestava l'esigenza di ricorrere ad un sistema di videosorveglianza per ragioni di sicurezza e tutela del patrimonio aziendale e presentava la necessità di servirsi di tale sistema di *body cam* dal momento che non era possibile installare videocamere nelle numerose vetture ferroviarie più datate.

L'autorità Garante, nel caso di specie, ha ritenuto il trattamento proporzionato, in quanto la società, per raggiungere i fini perseguiti, si prefigurava, in un tempo congruo, concretamente, la tipologia di eventi in presenza dei quali si sarebbe dovuto attivare il sistema di *body cam* il cui numero sarebbe stato comunque limitato e le cui immagini raccolte sarebbero state visionate unicamente dal personale autorizzato. Il ragionamento del Garante si spinge però oltre nell'applicazione del principio di proporzionalità, analizzando il bilanciamento di interessi tra titolare e interessati, con particolare riguardo alle misure previste a tutela di questi ultimi[85]. Poste infatti le finalità rappresentate, sono proprio gli accorgimenti volti a garantire una piena tutela degli interessati, e quindi per altro verso a limitare l'invasività del trattamento effettuato, a vestire, in un certo qual modo, di legittimità l'interesse del titolare.

Il principio di proporzionalità esprime pertanto la sua importanza quale principio fondamentale del trattamento dei dati personali, anche nel bilanciamento di interessi che postula l'ultima (in ordine meramente espositivo) condizione di liceità. Si mostra quale guida indirizzata sì a permettere che il titolare raggiunga gli scopi (legittimi) che si è prefigurato, ma anche, ad un tempo, ad arginare le superflue, *rectius*, sproporzionate intrusioni nella sfera dell'interessato.

[85] Tali misure previste dal Garante sono, nel caso di specie: l'individuazione «all'interno di un disciplinare relativo all'uso consentito delle '*body cam*', le specifiche condizioni che legittimano l'attivazione dei dispositivi (…) nonché le modalità di utilizzo dei dispositivi stessi, con particolare riferimento alle cautele da adottare nel caso in cui le riprese video coinvolgano soggetti "deboli" (…) specifiche istruzioni devono altresì essere fornite ai soggetti autorizzati in servizio presso la centrale operativa»; «l'effettuazione da parte dei soggetti autorizzati (…) di attività di verifica sulle immagini al fine di accertarne l'effettiva rilevanza rispetto alle finalità perseguite», anche qualora se ne effettuasse una conservazione superiore a sette giorni; il tracciamento degli accessi e delle estrazioni di dati effettuati dai soggetti autorizzati; la predisposizione di «misure idonee affinché la funzionalità audio non sia attiva»; l'oscuramento di immagini relative a soggetti terzi qualora tali immagini vengano inviate alla compagnia di assicurazione; la predisposizione di «idonee misure affinché gli operatori che hanno in dotazione i dispositivi non possano effettuare operazioni di modifica, cancellazione e duplicazione delle immagini raccolte»; la conservazione delle «registrazioni video in forma cifrata»; la cancellazione irreversibile delle registrazioni alla scadenza del tempo di conservazione; la predisposizione di «adeguati strumenti di comunicazione per avvisare gli utenti anche a bordo delle vetture, con linguaggio semplice e sintetico, della presenza del sistema di videosorveglianza mobile e le sue caratteristiche, specificando anche che una spia accesa sul dispositivo indossabile indica che la funzionalità di videoripresa è attiva».

3.1.4. *Applicazione del principio di proporzionalità per la valutazione delle deroghe all'esercizio dei diritti dell'interessato e, in particolare, dei casi di esonero dall'obbligo, per il titolare del trattamento, di rendere l'informativa all'interessato*

Un ulteriore ambito in cui il Garante ha applicato il principio di proporzionalità riguarda i diritti dell'interessato, ed in particolare il diritto a ricevere un'informativa da parte del titolare sia qualora i dati vengano raccolti presso quest'ultimo sia qualora non siano stati raccolti presso di lui (artt. 13 e 14 GDPR).

Precisamente, l'art. 14 del Regolamento, al par. 5, nel sancire deroghe ulteriori rispetto a quella contenuta nel precedente art. 13, par. 4 (ossia il caso in cui le informazioni siano già note all'interessato), prevede, giusta la lett. *b)*, la fattispecie in cui la comunicazione di tali informazioni risulti impossibile o implichi uno sforzo sproporzionato per il titolare. È pertanto il principio di proporzionalità a fungere da metro per la valutazione dell'obbligo di fornire all'interessato le informazioni previste dall'art. 14, parr. 1 e 2 GDPR e con le tempistiche di cui all'art. 14, par. 3 GDPR, e quindi ad essere la chiave per dispensare il titolare da tale obbligo.

In questo senso, il Garante si è espresso in un provvedimento in materia di propaganda elettorale e comunicazione politica[86], ribadendo l'esonero dall'obbligo in capo al titolare, sottolineando però, sempre ai sensi del Regolamento, come il titolare stesso sia comunque tenuto ad adottare le misure idonee alla tutela dei diritti, libertà e legittimi interessi dell'interessato anche, laddove risultasse utile in tal senso, rendendo pubbliche le informazioni. Si tratta di una espressione del principio di *accountability* che rimette al titolare, nell'ottica di una sua responsabilizzazione, l'adozione di adeguate misure tecniche ed organizzative al fine di risultare sempre *compliant* con la normativa vigente.

Nel caso di specie, l'autorità Garante ha previsto che laddove rendere l'informativa risulti impossibile o rappresenti uno sforzo sproporzionato per il titolare, spetta ai partiti, movimenti politici e comitati di promotori e sostenitori oltre che ai candidati, scegliere di non adempiere a detto obbligo purché si individuino con rigore le misure appropriate[87].

Sempre nell'ambito del provvedimento in questione, il Garante ha richiamato alcuni suoi precedenti[88], anch'essi riferiti all'esonero dall'obbligo di informativa e

---

[86] GPDP, Provv. 18 aprile 2019, doc. *web* n. 9105201.

[87] Secondo GPDP, Provv. 18 aprile 2019, doc. *web* n. 9105201, *supra cit*., si potrebbe prescindere «dall'obbligo di rendere l'informativa individuale, a partire dal sessantesimo giorno precedente la data delle consultazioni fino al sessantesimo giorno successivo al termine delle stesse (o dell'eventuale ballottaggio), a condizione che: – nel materiale inviato sia indicato un recapito (…) al quale l'interessato possa agevolmente rivolgersi per esercitare i diritti di cui agli artt. 15 e ss. del Regolamento; e – l'informativa recante tutti gli elementi di cui all'art. 14, paragrafi 1 e 2 del Regolamento sia resa mediante pubblicazione della stessa sui propri siti web di riferimento o tramite annunci pubblicati su quotidiani a diffusione nazionale o locale (a seconda della consultazione)».

[88] Il riferimento è a GPDP, Provv. 6 marzo 2014, doc. *web* n. 3013267; GPDP, Provv. 12 febbraio 2004, doc. *web* n. 634369; GPDP, Provv. 7 settembre 2005, doc. *web* n. 1165613; GPDP, Provv. 24 aprile 2013, doc. *web* n. 2404305; si vedano inoltre GPDP, Provv. 26 novembre 1998, doc. *web* n. 39624; GPDP, Provv. 4 aprile 2001, doc. *web* n. 40763; GPDP, Provv. 18 gennaio 2007, doc. *web* n.

relativi al tema della propaganda elettorale, ma adottati in vigenza della precedente normativa (quindi sulla base dell'art. 13, co. 5, lett. *c)* del Codice *privacy*), al fine di guidare il titolare del trattamento nella ricerca dei presupposti di applicabilità dell'art. 14, par. 5, lett. *b)* del Regolamento e, nel caso, aiutarlo nell'adozione delle misure più opportune. In seguito all'entrata in vigore del GDPR, è infatti sul titolare, giova ribadirlo, che grava la valutazione sull'eventuale sproporzione dello sforzo a lui richiesto per adempiere all'obbligo di informativa e può pertanto risultare di particolare utilità per lui stesso fondare le proprie decisioni, sulla base del percorso tracciato negli anni dal Garante. Nei menzionati provvedimenti, il Garante, premettendo la possibilità di inviare un'informativa sintetica benché efficace, aveva già puntualmente bilanciato il diritto degli interessati con l'obbligo (sproporzionatamente gravoso) del titolare e, in questo senso, aveva ritenuto di esonerare dall'obbligo di informativa i soggetti politici che utilizzano, per esclusivi fini di propaganda elettorale e comunicazione politica, dati personali estratti dalle liste elettorali, elenchi o atti conoscibili da chiunque senza il bisogno di contattare tutti gli interessati e quindi da intendersi quali "fonti pubbliche", per il circoscritto periodo di tempo connesso a consultazioni politiche, amministrative o referendarie, nonché a iniziative volte alla selezione di candidati (c.d. primarie). Il titolare veniva altresì dispensato da detto obbligo nel caso di invio di materiale propagandistico di dimensioni ridotte che, a differenza di una lettera o di una *email*, non renda possibile fornire con efficacia un'idonea informativa, anche di carattere sintetico.

Come affermato nei menzionati provvedimenti più risalenti, i casi di esonero dall'obbligo di informativa risultano anche utili ad evitare che in un breve arco temporale un elevato numero di interessati riceva una messe di informative tra loro analoghe inviate da diversi soggetti che, impegnati nella stessa campagna elettorale, utilizzano le stesse fonti conoscitive[89].

Quindi, nel caso di propaganda elettorale, l'adempimento agli obblighi di informativa deve essere considerato, a parere del Garante, come sproporzionato rispetto al diritto dell'interessato qualora ricorrano le circostanze che si sono esposte.

Ancora, un altro caso di esonero dall'obbligo di fornire un'informativa individualmente a tutti gli interessati, si rinviene, a parere del Garante, laddove il titolare provveda a pubblicarla sul proprio sito *web*[90].

Da tali provvedimenti emerge la rilevanza del principio di proporzionalità anche con riferimento all'informativa da fornire all'interessato, dal momento che al titolare, non si può richiedere ovviamente il raggiungimento di un fine impossibile, ma, qualora detto fine fosse astrattamente realizzabile, non può parimenti essere ri-

1392461; GPDP, Provv. 19 febbraio 2015, doc. *web* n. 3864423; GPDP, Provv. 19 aprile 2019, doc *web* n. 9105208; simili considerazioni si rinvengono anche, con riguardo a finalità di ricerca scientifica, *ex multis*, in GPDP, Provv. 24 novembre 2022, doc. *web* n. 9842737.

89 Cfr., in particolare, GPDP, Provv. 12 febbraio 2004, doc. *web* n. 634369, *supra cit*.

90 Cfr. GPDP, Provv. 5 luglio 2017, doc. *web* n. 6845231; GPDP, Provv. 9 novembre 2017, doc. *web* n. 7489156; GPDP, Provv. 11 giugno 2015, doc. *web* n. 4169456; GPDP, Provv. 14 maggio 2009, doc *web* n. 1616828, tutti conformi nel ritenere la possibilità di a) pubblicare l'informativa sul sito *web* della società titolare del trattamento; b) affiggerla presso i locali della società; c) comunicarla agli interessati in occasione della prima circostanza utile di contatto.

chiesto un impiego di mezzi manifestamente sproporzionati. È quindi necessario bilanciare correttamente, secondo proporzionalità, lo sforzo richiesto al titolare con il rispetto del diritto tutelato, stante la forte eco del considerando 4 GDPR che non pone il diritto alla protezione dei dati personali come prerogativa assoluta.

3.2. Il principio di proporzionalità in materia di trattamento di dati personali in ambiti specifici

3.2.1. *Il principio di proporzionalità quale limite al (e garanzia per il) controllo dei lavoratori*

Un profilo di primaria rilevanza del principio di proporzionalità nell'ambito della protezione dei dati personali è sicuramente quello dei controlli che, attraverso Internet o altri strumenti tecnologici *ad hoc*, il datore di lavoro può effettuare sui lavoratori dipendenti. L'ontologica inscindibilità tra il lavoro e la persona che lo svolge, determina un inevitabile conflitto tra il datore di lavoro – le cui ingerenze, legate alla vigilanza sull'attività di lavoro, rappresentano un fondamentale strumento per coordinare e valutare il lavoro prestato nonché per esercitare il potere disciplinare – e la persona del lavoratore i cui diritti fondamentali prestano il fianco a profonde lesioni[91].

Emerge, in simili situazioni, l'esigenza di un attento bilanciamento tra due istanze sì contrapposte, ma entrambe meritevoli di tutela: quella del datore di lavoro alla sicurezza e alla salvaguardia dei propri interessi connessi all'esercizio dell'impresa da un lato, e quella del lavoratore al rispetto della propria riservatezza nonché ad un legittimo trattamento dei propri dati personali dall'altro.

Pertanto, al fine di salvaguardare la persona umana da (quella che sarebbe) una smodata deriva dei poteri datoriali, l'incisività dei controlli cui possono essere sottoposti i lavoratori devono trovare una precisa giustificazione che necessariamen-

[91] V., *ex pluribus*, A. PIZZOFERRATO, *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore*, in *Argomenti dir. lav*., 2018, 4-5, pp. 1034 ss.; P. TULLINI, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in ID. (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, Torino, 2017, pp. 9 ss.; C. ZOLI, *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Riv. it. dir. lav*., 2009, 4, pp. 485 ss.; A. LEVI, *Il controllo informatico sull'attività del lavoratore*, Torino, 2013; A. TROJSI, *Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013; J. MILAJ, *Privacy, surveillance, and the proportionality principle*, in *Int. Rev. of Law, comp. & Tech*., 2016, 3, pp. 115 ss.; V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, Napoli, 2018; A. INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina* privacy*: una lettura integrata*, Bari, 2018; S. SANDULLI, *Controlli a distanza e* privacy *dei lavoratori*, in *Corr. giur*., 2019, 11, p. 1337 ss.; M. TUFO, *Potere di controllo datoriale "*vs. privacy*" del lavoratore: alla ricerca delle coordinate di ammissibilità dei controlli occulti*, in *Studium iuris*, 2020, 7-8, pp. 846 ss.; A. SARTORI, *Il controllo tecnologico sui lavoratori*, Torino, 2020; M. DE LUCA, *Potere di controllo del datore di lavoro fra tradizione e innovazione: dal codice civile al codice della "*privacy*", passando per lo statuto dei lavoratori ed il* Jobs Act, in *Variazioni sul tema di dir. lav*., 2022, 4, pp. 781 ss.; C. PISANI-G. PROIA-A. TOPO (a cura di), Privacy *e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, 2022; C. CARDARELLO-G. LIPARI, *La* privacy *ed il rapporto di lavoro subordinato*, Torino, 2022.

te troverà la sua base nel principio di proporzionalità e nel bilanciamento valoriale sotteso a tale principio.

L'impiego, sempre più ampio, delle nuove tecnologie ha incrementato il potere di controllo datoriale, già immanente al rapporto di lavoro e propaggine del potere direttivo. Questo anche attraverso l'utilizzo di strumenti nuovi, più penetranti, funzionali alla prestazione lavorativa e che, ad un tempo, consentono il controllo di colui che li utilizza. Un ruolo tutt'altro che marginale è, in questo senso, rivestito dagli strumenti dotati di intelligenza artificiale che, operando attraverso l'utilizzo di ingenti quantità di dati (*Big Data*), elaborati con grande rapidità da complessi algoritmi[92], e grazie alla loro capacità di raccogliere, catalogare, custodire e trasmettere informazioni, intensificano i rischi per la dignità e la *privacy* del prestatore di lavoro[93].

Nell'attuale società informatizzata, il datore di lavoro ha gli strumenti per controllare la posta elettronica dei dipendenti[94], l'utilizzo dei *social networks*[95], i loro accessi al luogo di lavoro[96], finanche la loro posizione geografica[97] e, le attività che,

[92] Ne evidenzia l'impatto A. Pizzoferrato, *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore*, *supra cit*., spec. pp. 1034-1035 e p. 1059.

[93] Cfr. S. Mainardi, *Intelligenze artificiali e diritto del lavoro*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 378 ss.; e A. Sitzia-B. Lopez, *Le più avanzate modalità di controllo sul lavoratore: machine learning e social media*, in C. Pisani-G. Proia-A. Topo (a cura di), Privacy *e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, cit., pp. 358 ss.

[94] Trib. Roma, 26 marzo 2019, in *Red. Giuffrè*, 2019 distingue in particolare tra *account* personale e *account* aziendale di posta elettronica: con riguardo al primo, il datore di lavoro ha il divieto categorico di accesso, il controllo del secondo invece, a determinate condizioni, è legittimo; Trib. Milano, 13 maggio 2019, n. 17778, in *Riv. it. dir. lav*., 2019, 4, pp. 639 ss., nel sottolineare l'importanza dell'informativa da fornire circa i controlli della posta elettronica, afferma che «il controllo della posta elettronica aziendale può anche avvenire senza un espresso consenso del dipendente, al quale comunque deve essere data adeguata informativa» cosicché le informazioni eventualmente acquisite siano utilizzabili anche per fini disciplinari.

[95] V. Cass., 27 maggio 2015, n. 10955, in *Giust. civ. mass*., 2015 in merito a controlli effettuati sui *social network*s per verificare sospetti comportamenti illeciti del dipendente; v. anche Cass., 31 gennaio 2017, n. 2499, in *Giust. civ. mass*., 2017; e Cass., 12 novembre 2018, n. 28878, in *De Jure* sul licenziamento di un dipendente che aveva pubblicato tramite *social network*, un contenuto che il datore di lavoro aveva ritenuto offensivo; si richiama inoltre A. Ingrao, *Il controllo a distanza realizzato mediante* Social network, in *Labour & Law Issues*, 2016, 1, p. 115 secondo cui: «il *Social network*, data la sua eclettica polivalenza, rappresenta un paradigma perfetto di come la funzione di lavoro e la funzione di controllo possano condensarsi e aggrovigliarsi in un medesimo programma informatico»; sulle nuove funzionalità che i *social networks* hanno nel contesto lavorativo vedi anche Gruppo di lavoro ex art. 29, Parere 2/2017 sul trattamento dei dati sul posto di lavoro, dell'8 giugno 2017.

[96] Cass., 14 luglio 2017, n. 17531, in *De Jure* sull'utilizzo del *badge* quale strumento per effettuare controlli a distanza sul lavoratore; v. inoltre Cass. 13 maggio 2016, n. 9904, in *Giust. civ. mass*., 2016, sulla possibilità di realizzare tramite il *badge*, in concreto, un controllo costante a distanza dell'attività lavorativa.

[97] Cass., 12 ottobre 2015, n. 20440, in *Riv. it. dir. lav*., 2016, 2, pp. 249 ss.; Cass., 5 ottobre 2016, n. 19922, in *Riv. it. dir. lav*., 2017, 1, pp. 26 ss., che non ritiene possa essere considerato alla stregua di controllo difensivo quello effettuato tramite un gps installato «*ex ante* ed in via generale ben prima che si potessero avere sospetti su una eventuale violazione da parte del lavoratore».

in generale, possono svolgere per mezzo degli strumenti digitali forniti dall'azienda. Di più, i controlli possono anche avvenire occultamente permettendo così al datore di carpire, anche accidentalmente, informazioni, magari di carattere strettamente privato, sul lavoratore, senza che questi ne sia a conoscenza[98]. Oppure, possono avvenire in modo indiretto, come nel caso di impiego di algoritmi in grado di risalire, indirettamente, al singolo lavoratore, utilizzando dati biometrici[99]. L'uso di *devices* aziendali capaci di controllare a distanza (in senso spaziale, ma anche temporale) i lavoratori ha quindi posto sotto una nuova luce i controlli datoriali creando nuovi confini per il libero esercizio di una simile pratica che non può certo essere indistintamente configurata come condotta illegittima del datore di lavoro.

Tali intrusioni nella sfera del lavoratore richiamano un tema già noto, ma che attualmente assume nuovi contorni: la necessità di regole e di principi in grado di garantire una opportuna tutela al soggetto controllato e che limitino l'attività del controllore.

Non si deve tralasciare sul punto il ruolo che riveste l'art. 4 Stat. Lav., così come novellato dall'art. art. 23, co. 1, del d.lgs. 14 settembre 2015, n. 151, norma che, nel nostro ordinamento, si occupa degli impianti audiovisivi e degli altri strumenti di controllo sui lavoratori e che va letta insieme alle disposizioni del Codice *privacy* data l'inevitabile intersecazione delle discipline. La *privacy* entra infatti «di diritto»[100] nella normativa giuslavoristica, rappresentando un importante corollario per la libertà del singolo lavoratore.

Non di secondaria importanza è, in questo contesto, il principio di proporzionalità che appare, ancora, come cardine fondante le decisioni dei giudici. Tra l'altro, lo scenario tecnologico è caratterizzato da rapidi mutamenti il cui precipitato sui diritti fondamentali della persona, visti in rapporto con altri diritti e interessi concorrenti, è innegabile. Pertanto, in un quadro che, anche sotto il profilo del formante giurisprudenziale, risulta un percorso in continua evoluzione, la Corte Europea dei Diritti dell'Uomo (Corte EDU), ha efficacemente sottolineato che «*the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more sophisticated technologies*»[101], evidenziando quindi il carattere tutt'altro che definitivo delle conclusioni raggiunte in seguito agli arresti giurisprudenziali sul tema.

---

[98] Cfr. C. COLAPIETRO, *Digitalizzazione del lavoro e tutela della riservatezza della persona*, in P. TULLINI (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, cit., pp. 24-25; v. anche Cass., 11 giugno 2018, in *Giust. civ. mass*., 2018 in merito ai controlli occulti effettuati dal datore di lavoro per mezzo di una agenzia investigativa: tali controlli, per la Corte, non possono riguardare l'adempimento o l'inadempimento della prestazione del lavoratore, ma solo illeciti compiuti (o che si sospettano in esecuzione) da parte del prestatore non riconducibili all'inadempimento dell'obbligazione contrattuale del prestatore; in senso conforme Cass., 14 febbraio 2011, n. 3590, in *Guida al dir*., 2011, 12, pp. 48 ss.

[99] In tema vedi Cass., 15 ottobre 2018, n. 25686, in *Resp. civ. e prev*., 2019, 4, pp. 1225 ss.

[100] L. CALIFANO-V. FIORILLO, *Videosorveglianza*, in *Dig. disc. pubbl*., 2015, p. 528.

[101] Corte EDU, *Fifth Section*, 5 ottobre 2010, *Case Köpke v. Germany*, in *Cass. pen*., 2011, 5, pp. 1972 ss.; sottolineano l'importanza di tale monito della Corte, P. PINTO DE ALBUQUERQUE-A SITZIA, *Lavoro e monitoraggio: il "test di proporzionalità" nella giurisprudenza della CEDU*, in C. PISANI-

Di particolare rilievo, in merito alla protezione dei dati dei lavoratori, è una sentenza della Grande Camera della Corte EDU[102] che si è espressa, in senso contrario alla decisione emanata in precedenza dalla terza sezione della stessa Corte[103], dimostrando come il principio di proporzionalità sia sempre il filo da seguire (anche) nelle controversie in tema di *privacy* in ambito lavorativo.

Il caso riguardava l'ammissibilità dell'installazione di telecamere nascoste, realizzata al fine di risolvere un problema di sospetti furti all'interno di un supermercato. Nella specie, il direttore del supermercato aveva fatto installare un sistema di videosorveglianza composto da alcune telecamere visibili, riguardo alle quali veniva fornita un'appropriata informativa, e da altre che erano state appositamente nascoste senza che ne venisse data alcuna notizia ai dipendenti: proprio grazie ai filmati di queste ultime, era stato possibile individuare e licenziare i responsabili dei furti.

Tra i profili su cui verteva il ricorso dei lavoratori, quello che interessa maggiormente ai fini del presente studio, è quello relativo alla violazione dell'art. 8 CEDU e, segnatamente, quello del diritto alla riservatezza. Tale censura era stata accolta dalla Camera semplice che, sottolineando l'ampiezza del concetto di vita privata, aveva affermato che la videosorveglianza occulta di un dipendente nel luogo in cui presta il proprio lavoro, configurasse una considerevole intrusione nella sua vita privata. La decisione aveva prestato particolare attenzione al principio di proporzionalità che, nel caso in questione, secondo la terza sezione, non si era ritenuto rispettato, stante l'estesa durata della videosorveglianza operata e la sua potenzialità di controllo indiscriminato dell'intero gruppo dei dipendenti. Di più, sarebbe stato, a parere della Corte, possibile, *rectius*, preferibile adottare mezzi differenti e meno intrusivi per i lavoratori: l'interesse datoriale poteva essere efficacemente conseguito anche fornendo una adeguata informativa ai lavoratori.

La pronuncia della Camera semplice si poneva in linea con altre due[104], precedenti, in cui il giudice di Strasburgo, rimarcando l'ampiezza di significato racchiusa nella disposizione giusta l'art. 8 CEDU – non relegabile al solo *inner cirle* dal quale l'individuo può decidere di escludere il mondo esterno, ma concetto nel quale devono essere ricompresi tutti gli aspetti idonei a sviluppare l'identità sociale di ogni

G. Proia-A. Topo (a cura di), Privacy *e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, cit., pp. 61-62.

[102] Corte EDU, *Grand Chamber*, 17 ottobre, 2019, *Case of López Ribalda and others v. Spain*, in *Riv. it. dir. lav*., 2020, 1, pp. 193 ss.

[103] Corte EDU, *Third Section*, 9 gennaio, 2018, *Case of López Ribalda and others v. Spain*, in *Guida al dir*., 2018, 6, pp. 41 ss.

[104] Il riferimento è a Corte EDU, *Grand Chamber*, 5 settembre 2017, *Case of Bărbulescu v. Romania*, in *Riv. dir. int*., 2017, 4, pp. 1201 ss. che a sua volta aveva ribaltato la precedente decisione Corte EDU, *Fourth Section*, 12 gennaio 2016, *Case of Bărbulescu v. Romania*, in *Mass. Giur. Lav*., 2016, pp. 209 ss.; e a Corte EDU, 28 novembre 2017, *Second Section*, *Case of Antovič e Mirkovič v. Montenegro*, in *Giuda al dir*., 2018, 2, pp. 92 ss. Il primo caso riguardava la richiesta fatta da una società datrice ai propri dipendenti di attivazione di un *account* personale su *Yahoo messenger* da utilizzare per assistere i clienti, ma che non poteva essere utilizzato dai lavoratori per conversazioni di carattere personale durante l'orario di lavoro. Ne derivava il licenziamento di chi avesse contravvenuto a detto divieto. Il secondo caso aveva invece ad oggetto la legittimità della decisione di sottoporre a videosorveglianza i locali universitari a fini di sicurezza.

individuo –, riteneva, appunto, sproporzionata la sorveglianza operata. La concezione di vita privata non può essere, infatti, limitata unicamente alla sfera personale del soggetto, ma ricomprende ogni aspetto indirizzato a permettergli di sviluppare la propria identità sociale (includendo quindi la possibilità di comunicare con il mondo esterno): per tali ragioni risulta importante, e ciò viene sottolineato nella sentenza, la previsione di una *policy* aziendale che regoli i controlli datoriali[105]. Le attività svolte nel contesto lavorativo, anche se pubblico, rientrano, come affermato dai giudici, nella concezione di vita privata, costituendo una dimensione in cui il soggetto esplica la propria personalità, e godono pertanto della protezione accordata *ex* art. 8 CEDU. Le aule universitarie (che interessano il caso *Antovič*) ne sono un esempio: non sono infatti solamente il luogo in cui i docenti fanno lezione agli studenti, ma un contesto in cui i primi interagiscono con i secondi «*developing mutual relations and constructing their social identity*»[106].

In queste decisioni, il giudice non riscontrava un corretto bilanciamento tra gli interessi perseguiti attraverso i controlli posti in essere ed il diritto alla *privacy* dell'interessato. In particolare, la registrazione delle attività lavorative deve essere considerata come forte ingerenza nella vita privata del lavoratore. Inoltre, seppure le ragioni datoriali fossero legittime, il test di proporzionalità non è stato approfondito nella ricerca del *least restrictive means*, dal momento che, si ricorda, il principio di proporzionalità viene sempre affiancato a quelli di pertinenza e non eccedenza rispetto allo scopo, principi relativi alla proiezione dinamica dei dati personali.

Diversamente, nel caso *Köpke*[107], anch'esso riferito alla valutazione sulla legittimità di una sorveglianza occulta operata all'interno di un supermercato, i giudici hanno considerato la misura intrapresa dal datore di lavoro, proporzionata, in quanto limitata ad un ridotto arco temporale e ad una ristretta area di ripresa nonché diretta unicamente nei confronti di due soggetti, sospettati di essere responsabili di alcuni furti. L'accesso alle registrazioni era stato, nelle specie, consentito ad uno stretto numero di operatori dell'agenzia investigativa.

Nel caso *López Ribalda*, la Grande Camera, tuttavia, approda ad un'opposta soluzione, e nega la fondatezza del ricorso in quanto la videosorveglianza si poteva considerare limitata nello spazio e nel tempo: precisamente, da un lato, le telecamere (nascoste) non riprendevano l'intero negozio, ma solo la zona delle casse e, dall'altro, l'attività di monitoraggio era durata solo il tempo necessario per scoprire i responsabili dei furti.

---

[105] Sul punto cfr. A. PIZZOFERRATO, *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore*, cit., p. 1054, in cui l'A., commentando la sentenza *Bărbulescu v. Romania,* afferma: «in tale quadro, le comunicazioni per *e-mail* rientrano nella nozione di corrispondenza, protetta dall'articolo 8 CEDU. Il datore di lavoro può quindi effettuare un controllo sulle *e-mail* inviate da un dipendente dal computer aziendale per fini personali solo nel rispetto di precisi parametri, quali un'informazione preventiva, l'impossibilità di ricorrere a misure meno intrusive, l'esistenza di gravi motivi che spingono l'azienda al controllo medesimo».

[106] Corte EDU, 28 novembre 2017, *Second Section*, *Case of Antovič e Mirkovič v. Montenegro*, cit., par. 44.

[107] Corte EDU, *Fifth Section*, 5 ottobre 2010, *Case Köpke v. Germany*, cit.

Il perno utilizzato dai giudici è rappresentato dal principio di proporzionalità che, nel caso di specie, è stato ritenuto, dalla Grande Camera, applicato. Posta l'importanza, in via generale, di una informativa fornita preventivamente, essa costituisce solo uno dei criteri da considerare per valutare la proporzionalità di una misura, motivo per cui un *overriding requirement* relativo alla protezione di un ulteriore interesse significativo può giustificare la mancanza di detta informativa. Nella fattispecie, il datore di lavoro aveva a che fare con una grave condotta, per la quale il sospetto ricadeva non su un isolato soggetto, ma su una pluralità di lavoratori: proprio per tali ragioni, l'istallazione di telecamere nascoste, seppur non preceduta da adeguata informativa, è stata comunque ritenuta una misura proporzionata e giustificata[108].

Il bilanciamento, tra i diritti dei dipendenti e quelli del datore, cui addiviene la Corte si riferisce al rispetto dell'art. 8 CEDU. La *ratio decidendi* tiene in considerazione i due nuclei che compongono la norma: il diritto tutelato (par. 1) e le *interferences* (par. 2) che possono causare una restrizione di un diritto che, come quello al rispetto della vita privata e familiare, non ha carattere assoluto. Restrizione che può trovare giustificazione laddove sia atta al raggiungimento di un ulteriore e legittimo fine e rispettosa del principio di proporzionalità.

Del resto, non ammettendosi uno svuotamento dei diritti fondamentali del lavoratore, ma non potendosi permettere neppure una smodata compressione della tutela del patrimonio aziendale, si deve evidenziare come appaia nettamente diverso, (anche) alla luce del canone di proporzionalità, un controllo dei lavoratori posto in essere *ex post*, e quindi rispetto a condotte illecite già avvenute o delle quali vi è un concreto ed attuale timore, rispetto ad un controllo *ex ante*, diretto ad una vigilanza non specifica ed occasionale, ma continua. I controlli difensivi, se realmente fondati su una necessità di tutela dei beni aziendali (e quindi, più in generale, dell'iniziativa economica) a causa di comportamenti illeciti o di un concreto sospetto di tale genere di condotte, potrebbero infatti risultare, nel caso di specie, legittimi se proporzionati rispetto alle istanze del lavoratore che, mai annullate, possono essere ragionevolmente compresse.

L'allora presidente dell'autorità Garante per la protezione dei dati personali, data l'eco del caso *López* e le sue possibili ripercussioni sulla successiva giurisprudenza anche interna, in un suo comunicato[109], ha affermato che la videosorveglianza occulta non deve essere intesa come possibile prassi ordinaria, ma come *extrema ratio*, aggiungendo che la Corte EDU ha ritenuto legittima la misura nel caso di specie solo perché ricorrevano i presupposti e le circostanze di cui si è detto in precedenza.

---

[108] Corte EDU, *Grand Chamber*, 17 ottobre, 2019, *Case of López Ribalda and others v. Spain*, cit., in particolare parr. 131-133-134 in cui la Corte, d'altro canto, afferma che: «*it cannot accept the proposition that, generally speaking, the slightest suspicion of misappropriation or any other wrongdoing on the part of employees might justify the installation of covert video-surveillance by the employer*»; in merito agli obblighi di trasparenza e informazione in caso di videosorveglianza v. EDPB, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, versione 2.0*, del 29 gennaio 2020, pp. 26-27. Sul tema cfr. pure Cass., 22 settembre 2021, n. 25732, in *Dir. relaz. ind.*, 2022, 1, pp. 271 ss.; e Cass., 23 febbraio 2012, n. 2722, in *Foro it.*, 2012, 1, cc. 1421 ss.

[109] Telecamere sul luogo di lavoro: dichiarazione di Antonello Soro, Presidente del Garante per la *privacy*, su sentenza Corte di Strasburgo, Roma, 17 ottobre 2019.

Una simile dichiarazione pare potersi intendere come monito per i datori di lavoro affinché questi non ritengano legittimo qualsivoglia controllo sui lavoratori, ma comprendano come un'eventuale sorveglianza (anche difensiva) debba essere riconducibile entro binari che ne limitino la possibile adozione e ne disciplinino le modalità attuative. Il comunicato ha inoltre rappresentato l'occasione per ribadire l'assoluta importanza del principio di proporzionalità quale caposaldo del diritto alla protezione dei dati personali e cardine fondamentale su cui basare ogni giudizio in merito alla legittimità dei controlli sul lavoro, tema per il quale il bilanciamento tra diritti deve essere particolarmente attento, al fine di coniugare riservatezza ed iniziativa economica, libertà e sorveglianza, in forza della funzione sociale che caratterizza la tematica della *data protection*.

Certamente, l'innovazione tecnologica, anche in ambito lavorativo, non può essere frenata o scoraggiata, alla luce della sua importanza quale fattore di crescita sociale. Non sembrano infatti condivisibili considerazioni che diano rilievo ai soli aspetti negativi del fenomeno: pare invece più opportuno affrontare il tema nell'ottica di una regolazione delle nuove sfide poste dall'avanzamento tecnologico, al fine di correggere possibili dinamiche distorsive[110]. Sembra infatti più corretto ritenere che non siano le innovazioni tecnologie a disposizione in sé considerate a creare possibili squilibri sul luogo di lavoro e rischi per i diritti fondamentali del lavoratore, ma le loro applicazioni, spesso sproporzionate.

A causa dei controlli che, ormai, appaiono possibili in modo incessante, delocalizzato ed indiscriminato, si manifesta con rinnovato vigore la necessità di tutelare il singolo soggetto ed ai suoi diritti fondamentali. È pertanto doveroso ricercare quel corretto bilanciamento che consenta di trovare un equilibrio tra la vita privata del lavoratore e le esigenze aziendali. Nonostante la prevenzione di illeciti e la salvaguardia del patrimonio (materiale ed immateriale) siano interessi di primaria importanza, adeguata tutela deve essere garantita ai lavoratori, alla loro riservatezza e alla loro autodeterminazione informativa.

Un simile equilibrio deve essere condotto – e così accade alla luce delle pronunce che si sono richiamate – in base al principio di proporzionalità, architrave per dirimere le controversie scaturenti dalle nuove declinazioni dell'art. 8 CEDU, dovute alle applicazioni tecnologiche.

3.2.2. *L'applicazione del principio di proporzionalità nel settore pubblico in seguito alla sentenza n. 20/2019 della Corte costituzionale: dal bilanciamento tra riservatezza e trasparenza, al diritto all'oblio quale "questione di proporzionalità"*

La nota decisione 20/2019[111] rappresenta per la Corte costituzionale, oltre che l'occasione per pronunciarsi sul tema della doppia pregiudizialità, tornato in auge

[110] Cfr. S. CIUCCIOVINO, *Le nuove questioni di regolazione del lavoro nell'industria 4.0 e nella* gig economy: *un* problem framework *per la riflessione*, in *Dir. relaz. ind*. 2018, 4, p. 1043.

[111] Corte cost., 21 febbraio 2019, n. 20, tra le altre in *Giur. cost*., 2019, 1, pp. 226 ss. con nota di G. REPETTO; e in *Giuda al dir*., 2019, 12, pp. 90 ss., con nota di D. PONTE; in commento v. anche A.

con rinnovato interesse e nuove prospettive[112], l'opportunità di esprimersi sul rapporto e sul bilanciamento tra diritti e principi di interesse costituzionale ed europeo[113],

Averardi, *La Corte costituzionale e gli obblighi di pubblicazione dei redditi dei dirigenti pubblici*, in *Giorn. dir. amm*., 2019, 5, pp. 601 ss.; sull'analisi delle questioni sottese alla pronuncia in esame e, in particolare, in rapporto al principio di proporzionalità, sia consentito rinviare a C. Basunti, *Il proporzionale bilanciamento tra diritto di accesso alle informazioni della p.a. e* privacy *dei singoli*, in *Contratto e impr*., 2021, 4, pp. 1085 ss.

[112] A margine delle tematiche che si affrontano in questa sede, pare opportuno ricordare che la sentenza in oggetto riprende il tema della doppia pregiudizialità il cui percorso è stato storicamente tracciato dalla sentenza *Simmenthal* (Corte di giustizia UE, 9 marzo 1978, c 106/77) e *Granital* (Corte cost., 5 giugno 1984, n. 170). Sul punto, la pronuncia in commento segue l'altrettanto noto *obiter dictum*, contenuto in Corte cost., 14 dicembre 2017, n. 269, tra le altre in *Giur. cost*, 2017, 6, pp. 2925 ss., con nota di G. Scaccia, nella quale, in via di estrema sintesi, si afferma come non debbano essere i giudici interni a disapplicare le norme nazionali in contrasto con la Carta di Nizza, ma che debba essere la Corte costituzionale ad intervenire, operando un controllo *erga omnes*, secondo il modello accentrato di costituzionalità (punto 5.2). Si tratta, in altri termini, di un incoraggiamento al giudice comune a preferire la formulazione di una questione di legittimità costituzionale anziché operare un rinvio pregiudiziale alla Corte di giustizia (facoltà sempre possibile che tra l'altro diviene obbligo nel caso di giudice di ultima istanza) laddove i diritti ed i principi sanciti dalla Carta di Nizza si intersechino con quelli tutelati dalla Costituzione: è infatti possibile che «la violazione di un diritto della persona infranga, ad un tempo, sia le garanzie presidiate dalla Costituzione italiana, sia quelle codificate dalla Carta dei diritti dell'Unione». Tutto ciò comunque in un'ottica di «costruttiva e leale cooperazione fra i diversi sistemi di garanzia, nel quale le Corti costituzionali sono chiamate a valorizzare il dialogo con la Corte di giustizia (…), affinché sia assicurata la massima salvaguardia dei diritti a livello sistemico». Sul punto si inserisce il timore, avanzato da autorevole dottrina, A. Barbera, *La Carta dei diritti: per un dialogo fra la Corte italiana e la Corte di giustizia*, in *Quaderni cost*., 2018, 1, p. 157, che l'asse tra i giudici comuni e la Corte di giustizia rischi di «*erodere*, per quanto concerne la tutela dei diritti fondamentali, ruolo e poteri della giurisdizione costituzionale». Tali preoccupazioni, seppur condivisibili, non devono comunque condurre a legittimare la Corte costituzionale ad una interpretazione unilaterale della Carta, che abbia riguardo unicamente alle proprie tradizioni costituzionali, dal momento che il dialogo con la Corte di Giustizia può offrire un importante contributo al fine di rendere i valori della Costituzione, tradizioni comuni. Nella vastissima letteratura che si è occupata di analizzare la sentenza 269/2017 ed i suoi risvolti sul tema, si richiamano inoltre, per tutti, G. Scaccia, *L'inversione della "doppia pregiudiziale" nella sentenza della Corte costituzionale n. 269 del 2017: presupposti teorici e problemi applicativi*, in *Forum di Quad. cost*., 2018, pp. 1 ss.; A. Guazzarotti, *La sentenza n. 269 del 2017: un «atto interruttivo dell'usucapione» delle attribuzioni della Corte costituzionale?*, in *Quad. cost*., 2018, 1, pp. 194 ss.; L.S. Rossi, *La sentenza 269/2017 della Corte costituzionale italiana:* obiter *"creativi" (o distruttivi?) sul ruolo dei giudici italiani di fronte al diritto dell'Unione europea*, in *Federalismi.it*, 2018, 3, pp. 1 ss. Con la sentenza 20/2019, la Corte costituzionale torna a riflettere, sul tema, operando delle «significative messe a punto» ed un «complessivo riassestamento dell'equilibrio precedente» come afferma G. Repetto, *Il significato europeo della più recente giurisprudenza della corte costituzionale sulla "doppia pregiudizialità" in materia di diritti fondamentali*, in *Riv. aic*, 2019, 4, pp. 6., lasciando libertà di scelta per il giudice comune in merito al rimedio pregiudiziale da attivare, rendendo la doverosità della preventiva rimessione alla Corte costituzionale una "opportunità" (punto 2.1); prevedendo inoltre, con l'esclusione di «ogni preclusione» (punto 2.3), la facoltà di rinvio pregiudiziale sulla stessa disciplina oggetto del sindacato di costituzionalità e non più solo, come si era affermato nella decisione del 2017, «per altri profili». Il giudice comune dovrà, pertanto, calarsi direttamente nel rapporto tra Corte costituzionale e Corte di giustizia, il cui funzionamento deve necessariamente essere improntato al meta-principio di leale collaborazione di cui all'art. 4 TUE.

[113] Si fa riferimento alla Carta dei diritti fondamentali dell'Unione europea che, come afferma Corte cost., 14 dicembre 2017, n. 269, cit., è «dotata di caratteri peculiari in ragione del suo contenuto di

che necessitano di un'opportuna valorizzazione e che non sono suscettibili di una compressione che esuli dai binari del principio di proporzionalità. Precisamente, mi riferisco alla riservatezza nelle sue più moderne declinazioni e alla trasparenza quale corollario del principio democratico ed intesa come diritto dei cittadini al libero accesso alle informazioni in possesso della pubblica amministrazione nonché criterio guida per il buon funzionamento della stessa.

Posto che uno dei principi fondamentali dello stato costituzionale è quello secondo cui «la pubblicità è la regola, il segreto l'eccezione, e a ogni modo è un'eccezione che non deve far venir meno la regola»[114], le esigenze di controllo del potere pubblico hanno reso sempre più difficile operare un attento e corretto bilanciamento tra gli opposti interessi di accesso alle informazioni e di riservatezza delle stesse[115], entrambi rilevanti e meritevoli di tutela. Devono infatti esistere dei limiti alla trasparenza la quale si sostanzia nel passaggio da mera conoscibilità a conoscenza effettiva, finalizzata alla formazione di una opinione strutturata, ed il cui approdo finale consiste nel controllo diffuso sull'agire amministrativo[116]. È quindi necessario comprendere quali siano questi limiti della trasparenza amministrativa, dal momento che aree di segretezza nella pubblica amministrazione vi devono necessariamente essere e permanere a salvaguardia di altri diritti o interessi costituzionalmente tutelati[117].

impronta tipicamente costituzionale. I principi e i diritti enunciati nella Carta intersecano in larga misura i principi e i diritti garantiti dalla Costituzione italiana».

[114] L'espressione è di N. BOBBIO, *La democrazia e il potere invisibile*, in *Riv. it. sc. pol*., 1980, 2, p. 184.

[115] Sul tema v. C. COLAPIETRO, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla* privacy*: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *Federalismi.it*, 2020, 14, pp. 64-65, in cui l'Autore sottolinea come *privacy* e trasparenza siano «elementi essenziali per mantenere in buona salute la vita democratica di uno Stato (…) la cui azione combinata permette allo stesso tempo di preservare la libertà dei privati dagli abusi del potere e di favorire la libera partecipazione dei cittadini, i quali possono informarsi sull'azione della pubblica amministrazione, celando però gli aspetti della propria vita privata che, se rivelati, potrebbero potenzialmente condurre a conseguenze indesiderate e talvolta discriminatorie».

[116] Cfr. C. COLAPIETRO, *Trasparenza e democrazia: conoscenza e/è potere*, in L. CALIFANO e ID. (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2014, pp. 21 ss.

[117] Sul punto v. M. CAPORALE, *Trasparenza, accesso civico e riutilizzo dei dati pubblicati. I limiti a tutela di interessi pubblici giuridicamente rilevanti*, in B. PONTI (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni. Commento sistematico al D.Lgs. 33/2013 dopo le modifiche apportate dal D.Lgs 25 maggio 2016, n. 97*, Rimini, 2016, p. 135, in cui l'A. sottolinea correttamente come molto si sia detto sull'estensione della trasparenza, ma poco ci si sia soffermati sul suo perimetro esterno, e quindi «sulle necessarie aree di segretezza che permangono nella nostra amministrazione a tutela di altri diritti costituzionalmente riconosciuti»; v. inoltre ID., *Segreto di Stato, segreto amministrativo e sistema di classificazione delle informazioni*, Bologna, 2013, in particolare pp. 123 ss., per i richiami e le riflessioni in merito alla distinzione tra trasparenza e pubblicità, e pp. 126-127, in cui si evidenzia come le riforme della pubblica amministrazione siano state indirizzate alla massima trasparenza «imponendo limiti più puntuali alla discrezionalità della pubblica amministrazione nell'utilizzo del segreto, strumento che costituisce sempre più un'eccezione laddove pubblicità e trasparenza diventano la regola». In argomento, vedi anche la differenza tra limiti *della* trasparenza e limiti *alla* trasparenza prospettata da F. MERLONI, *Trasparenza delle istituzioni e principio democratico*, in ID. (a cura di), *La trasparenza amministrativa*, Milano, 2008, pp. 13-16, secondo il quale, i primi sono quelli che mostrano le «insufficienze della trasparenza nel raggiungere i risultati ai quali essa è strumentale»; i secondi, invece, si sostanziano principalmente nella riservatezza privata e nella riservatezza pubblica. Nella vasta letteratura sul tema, cfr. pure

Proprio sul perimetro che si deve tracciare attorno agli obblighi di pubblicazione, soprattutto in rapporto alla tutela della riservatezza, la sent. 20/2019 offre un prezioso punto di vista, capace di spiegare importanti effetti sul rapporto in questione. Si fronteggiano, da un lato, l'esigenza di trasparenza amministrativa che si manifesta anche quale forma di controllo dell'azione pubblica con particolare riguardo all'uso delle risorse e all'integrità personale dei soggetti responsabili del loro utilizzo; dall'altro, invece, l'esigenza di tutelare la riservatezza, intesa non solo come esclusione del prossimo dalla propria sfera privata, ma anche quale diritto al controllo della circolazione delle proprie informazioni: all'autodeterminazione informativa.

Il caso prendeva le mosse da una questione di legittimità costituzionale sollevata dal Tar del Lazio[118], con riguardo all'art. 14, co. 1-*bis* e 1-*ter*[119], d.lgs. 14 marzo 2013, n. 33 giusta i quali, a fini di trasparenza amministrativa, si imponevano obblighi di pubblicazione a titolari di incarichi politici, di amministrazione, di direzione o di governo e a titolari di incarichi dirigenziali. L'incidente di costituzionalità sollevato dal Collegio si incentrava sulla violazione degli artt. 2, 3, 13 e 117, co. 1 Cost., nonché degli artt. 7, 8 e 52 della Carta di Nizza e di varie norme della direttiva 95/46/CE, oggi sostituita dal GDPR.

Nella specie, il ricorso veniva proposto da alcuni dirigenti del Garante per la protezione dei dati personali avverso un provvedimento del Segretario generale dell'Autorità, che imponeva ad un ampio numero di soggetti (oltre 140.000) la pubblicazione *online* di informazioni patrimoniali che li riguardavano. In particolare, quelle previste *ex* art. 14, co. 1, lett. *c)* ed *f)* d.lgs. 33/2013. Da un lato, veniva criticata la totale equiparazione dei dirigenti pubblici con i titolari di incarichi politici, senza che venissero puntualizzate differenziazioni tra le figure dirigenziali, compiendo così una «erronea assimilazione di condizioni non equiparabili fra loro» che inoltre prescindeva «dall'effettivo rischio corruttivo insito nella funzione svolta»[120]; dall'altro si metteva in discussione l'obbligo di pubblicazione delle informazioni senza alcun filtro in grado di scongiurare la diffusione di dati non necessari (per i fini della normativa) o comunque suscettibili di interpretazioni distorte.

Cruciale, nell'argomentazione del Tar, era il contrasto delle norme impugnate con il principio di *proporzionalità*, soprattutto nella sua prospettiva legata alla *privacy*, che, insieme a quelli di pertinenza e non eccedenza, al primo strettamente connessi, costituisce «il canone complessivo che governa l'equilibrio del rappor-

I. Nicotra, *La dimensione della trasparenza tra diritto alla accessibilità totale e protezione dei dati personali: alla ricerca di un equilibrio costituzionale*, in *Federalismi.it*, 2015, 11, pp. 2 ss.; C. Colapietro, *La terza generazione della trasparenza amministrativa*, Napoli, 2016; A. Corrado, *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, 2018.

[118] TAR Lazio, 19 settembre 2017, n. 9828, in *Federalismi.it*, 2017.

[119] Il ricorso avverso il co. 1-*ter* della norma (limitatamente alla prescrizione dell'ultimo periodo secondo cui «l'amministrazione pubblica sul proprio sito istituzionale l'ammontare complessivo dei suddetti emolumenti per ciascun dirigente») è stato aggiunto d'ufficio dal Tar dopo aver valutato come non manifestamente infondate le questioni sollevate in merito al co. 1-*bis*.

[120] Così TAR Lazio, 19 settembre 2017, n. 9828, cit. che aggiunge: «la previsione in contestazione assimila condizioni che, all'evidenza, non sono equiparabili fra loro, stante l'enorme diversità tra le condizioni giuridiche facenti capo, nel vigente ordinamento nazionale, da un lato, ai titolari di incarichi politici e, dall'altro, ai titolari di incarichi dirigenziali».

to tra esigenza, privata, di protezione dei dati personali, ed esigenza, pubblica, di trasparenza»[121].

Nel nuovo scenario digitale, il principio di proporzionalità assume una nuova centralità con riguardo alla decisione di legittimità inerente alla diffusione dei dati personali: nel caso in esame, infatti, oltre ad essere la natura dei dati di cui si chiedeva la pubblicazione a sollevare interrogativi circa l'ammissibilità della richiesta, Internet e le nuove tecnologie permettono una diffusione quanto mai capillare dei dati la cui circolazione può avvenire in modo indiscriminato se, come in questa vicenda, non vengono introdotte misure che ne impediscano l'indicizzazione generalizzata da parte dei motori di ricerca. Posto infatti che è proprio la più ampia circolazione possibile dei dati a permettere una maggiore possibilità di informazione da parte dei cittadini (e quindi una maggior trasparenza della pubblica amministrazione), non può certo «riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali»[122]. La trasparenza non può essere considerata un valore assoluto, ma deve essere soggetta ad un attento bilanciamento, che abbia riguardo primariamente al principio di proporzionalità e agli altri diritti e valori costituzionali, e tra questi, quello alla riservatezza.

L'acuito contrasto tra trasparenza e protezione dei dati personali, sintomo del preponderante impiego delle nuove tecnologie, è il fulcro della sentenza in esame ed il principio di proporzionalità è la chiave per approdare ad una soluzione del caso concreto.

La macroscopica differenza di *status* tra le categorie in esame per genesi, funzioni, struttura e poteri, non rende ragionevole la loro riconduzione nell'ambito dello stesso regime. La loro totale (forzata) equiparazione non può infatti giustificarsi (in quanto non proporzionata) in vista dei fini di trasparenza amministrativa.

La Corte costituzionale dichiara non fondata la questione di legittimità sollevata in relazione all'obbligo, imposto a carico di ciascun titolare di incarico dirigenziale di pubblicare i compensi di qualsiasi natura connessi all'assunzione della carica, nonché gli importi di viaggi di servizio e missioni pagati con fondi pubblici [art 14, co. 1, lett. *c)* d.lgs. 33/2013]. Un regime di piena conoscibilità così previsto viene giudicato proporzionato rispetto alle finalità perseguite, in quanto ragionevolmente connesso all'esercizio di un controllo riguardante la corretta esecuzione degli incarichi istituzionali e le giuste modalità di impiego delle risorse pubbliche. Appare convincente la Corte nel ritenere che non ci sia fondato motivo di considerare la

[121] Corte cost., 21 febbraio 2019, n. 20, cit., punto 1.6.

[122] Corte cost., 21 febbraio 2019, n. 20, cit., punto 3.1 in cui la Corte richiama la Corte di giustizia UE (Grande Sezione), 9 novembre 2010, cause riunite C-92/09 e 93/09, *Volker und Markus Schecke e Eifert*, in cui al par. 85 si afferma che: «si deve ricordare che le istituzioni, prima di divulgare informazioni riguardanti una persona fisica, devono soppesare l'interesse dell'Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta. Orbene, non può riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali (…), anche qualora siano coinvolti rilevanti interessi economici»; sul punto, per la Corte costituzionale, punto 2.2, il nuovo contesto digitale rappresenta «un ambito nel quale, da un lato, i diritti personali possono essere posti in pericolo dalla indiscriminata circolazione delle informazioni, e, dall'altro, proprio la più ampia circolazione dei dati può meglio consentire a ciascuno di informarsi e comunicare».

pubblicazione di tali dati come rischio per la sicurezza o la libertà degli interessati, o come fonte di una lesione alla dignità personale degli stessi. Si tratta infatti di dati direttamente collegati allo svolgimento dell'incarico dirigenziale e alle spese pubbliche a ciò destinate. Ben si comprende, quindi, la ragione profonda (qui assolutamente presente) su cui si basa il diritto dell'intera *societas* alla conoscenza di tali informazioni senza che, d'altra parte, si possa addurre la violazione del diritto alla riservatezza degli incaricati.

Diverse sono, invece, le conclusioni della Corte costituzionale in merito alle pubblicazioni previste *ex* art. 14, co. 1, lett. *f)* d.lgs. 33/2013 che, ai sensi del censurato co. 1-*bis* della norma, vengono imposte a tutti i titolari di incarichi dirigenziali senza alcuna distinzione. Uguale però è il principio alla base del giudizio: quello di proporzionalità. Ad essere sproporzionato, a parere della Corte, è infatti il mezzo in rapporto al fine: la richiesta di pubblicazione di tali dati non trova giustificazione, *rectius*, non è proporzionata al perseguimento del fine di contrastare la corruzione della pubblica amministrazione[123]. Questo dal momento che tali informazioni non consentono, in concreto, né di avere contezza della organizzazione e delle attività svolte dalle pubbliche amministrazioni né di poter effettuare un controllo sulla spesa pubblica. Ne deriva che il detrimento della tutela offerta (e legittimamente attesa) con riguardo al diritto alla riservatezza, non comporta, in questo caso, un corrispondente incremento né del diritto dei cittadini ad una adeguata informazione sul punto né dell'interesse pubblico alla repressione dei fenomeni corruttivi. La norma viene pertanto dichiarata costituzionalmente illegittima per violazione dell'art. 3 Cost. nella parte in cui prevede l'obbligo a carico della P.A. di pubblicare i dati *ex* art. 14, co. 1, lett. *f)*, d.lgs. 33/2013, riguardanti tutti i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti[124]. La richiesta di pubblicare le informazioni in questione non può prescindere da una differenziazione fondata sul ruolo, sulle responsabilità e sulla carica ricoperta dal dirigente, al fine di comprendere il concreto livello di potere decisionale e gestionale del soggetto, così da decidere in merito alla pervasività e completezza dei dati da pubblicare. Il menzionato livello di potere, infatti, non può che influenzare profondamente la gravità del rischio corruttivo e le conseguenti necessità di trasparenza e informazione.

L'indiscriminata conoscibilità dell'ampio ventaglio di dati personali di cui si impone la pubblicazione non risulta essere il *least restrictive means* adottabile.

Nell'ottica di un bilanciamento solo parzialmente effettuato, secondo la Consulta, in riferimento a due categorie di dirigenti pubblici, non pare irragionevole il mantenimento dei suddetti obblighi di pubblicazione *ex* art. 14, co. 1, lett. *f)*, d.lgs. 33/2013: il Segretario generale dei ministeri, di direzione di strutture articolate al

[123] Precisa Corte cost., 21 febbraio 2019, n. 20, cit., punto 5.3, che tali dati non sono necessariamente in diretta connessione con l'espletamento dell'incarico. Quello che deve essere valutato è se quel «ventaglio di informazioni e dati personali di natura reddituale e patrimoniale contenuti nella documentazione oggetto di pubblicazione appaia necessaria e proporzionata rispetto alle finalità perseguite dalla legislazione sulla trasparenza».

[124] Sono invece dichiarate inammissibili per difetto di rilevanza le questioni di legittimità sollevate con riferimento al co. 1-*ter* dell'art. 14 del citato d.lgs. dal momento che i provvedimenti impugnati nel giudizio principale sono stati adottati solamente in applicazione del co. 1-*bis*.

loro interno in uffici dirigenziali generali; e coloro che sono deputati alla direzione di uffici di livello dirigenziale generale. Sono proprio i compiti svolti da tali soggetti, indicati rispettivamente all'art. 19, co. 3 e 4 del d.lgs. 30 marzo 2001, n. 165, che possono giustificare un obbligo così incisivo.

Si sottolinea come, ad aggravare la frustrazione del diritto alla riservatezza, siano le modalità previste per la pubblicazione dei dati. La libera rintracciabilità delle informazioni sulla rete, che per di più non sembrano connesse funzionalmente al controllo (del corretto espletamento) dell'incarico affidato ai dirigenti, pare infatti incorrere nel rischio di stimolare ricerche basate sulla mera «*public's thirst for information about the private life of others or to an audience's wish for sensationalism or even voyeurism*»[125]. Di più, la massa di dati pubblicata, senza un previo controllo a monte (basato sui criteri di ragionevolezza e proporzionalità) rischia di creare una sorta di «opacità per confusione»[126] tale da ostacolare la ricerca delle informazioni realmente utili per i fini perseguiti. La digitalizzazione dei più svariati aspetti della vita di ogni individuo, anche nella sua forma associata, rende ancora più centrale, per le politiche pubbliche, bilanciare gli interessi giuridici, di natura individuale o metaindividuale, in gioco con il diritto alla riservatezza, sempre nell'ottica della natura "non tiranna" di quest'ultimo[127].

Da qui il monito al legislatore, lanciato dal Giudice delle leggi, in una prospettiva *de iure condendo*, di attuare una revisione complessiva, definita urgente, della materia, in modo tale da soddisfare le esigenze di trasparenza in relazione alle differenti tipologie di incarico dirigenziale, senza violare, *rectius*, limitare sproporzionatamente la *privacy* dei singoli. In attesa del necessario intervento legislativo in materia, la Corte costituzionale ha inteso quindi garantire un nucleo, seppur minimo, di tutela per questi due diritti per i quali i termini di bilanciamento appaiono senz'altro mobili. Pare opportuno che il legislatore affronti il compito cui è stato chiamato, oltrepassando i limitati parametri forniti dalla Corte costituzionale, dal momento che tali parametri originano da mere questioni processuali, ossia dalla risposta alla (circoscritta) questione sollevata dal Tar Lazio sulla base dell'impugnativa dei ricorrenti. Il legislatore dovrebbe, infatti, soffermarsi anche sulle modalità di pubblicazione dei dati, e precisamente sulla possibilità, in capo ai motori di ricerca, di operare un'indicizzazione dei dati, senza ostacoli o filtri di sorta (art. 9 d.lgs. 33/2013) e di riutilizzarli (art. 7 d.lgs. 33/2013). La revisione dovrebbe, quindi, essere complessiva: puntuale sulla richiesta (diretta) della Corte costituzionale e avere, al contempo, riguardo al quadro d'insieme, all'interno del quale non sono mancate note critiche della Consulta in merito alle suddette modalità di pubblicazione, in quanto esse accrescono la rigorosità della norma impugnata. Bisogna infatti chiedersi se tali modalità possano rappresentare un *quid pluris*, risultando davvero necessarie per le finalità di trasparenza amministrativa, anche in rapporto alla (indiscutibile) compres-

[125] Così, Corte EDU, *Grand Chamber*, 8 novembre 2016, *Case of Magyar Helsinki Bizottság v. Hungary*, par. 162.

[126] L'immagine è offerta dalla stessa Corte cost., 21 febbraio 2019, n. 20, cit., punto 5.3.1.

[127] O. POLLICINO-F. RESTA, *Trasparenza amministrativa e riservatezza, verso nuovi equilibri: la sentenza della Corte costituzionale*, in *Agenda digitale*, 25 febbraio 2019.

sione del diritto alla riservatezza degli interessati, con il quale, si è detto, le esigenze di trasparenza devono comunque porsi in equilibrio. Non potendosi, a parere di chi scrive, prospettare una risposta positiva, è anche su questi aspetti che si dovrebbe concentrare l'attenzione del legislatore.

Di più, pare che il "riutilizzo" dei dati, sancito *ex* art. 7 d.lgs. 33/2013 e recentemente promosso dal *Data Governance Act*[128], non sia propriamente legato ai doveri di trasparenza amministrativa quanto, piuttosto, allo sfruttamento (anche) economico dei dati stessi. Da questa angolazione, il bilanciamento da effettuarsi dovrà tenere in considerazione diversi fattori: il diritto alla *privacy* e la possibilità di sfruttare i dati personali, senza che la trasparenza giochi un ruolo di rilievo.

La sentenza 20/2019 rappresenta, quindi, un'ulteriore conferma di quanto la proporzionalità costituisca un principio fondamentale che «dovrebbe guidare ogni operazione di bilanciamento tra diritti fondamentali antagonisti»[129] e che riveste una importanza particolare nell'ambito del diritto alla protezione dei dati personali. Nel ragionamento dei giudici, il principio di proporzionalità rappresenta il cuore, lo strumento attraverso il quale tratteggiare correttamente i confini relativi agli obblighi di pubblicazione gravanti sui dirigenti amministrativi. Anche se animate da fini indiscutibilmente nobili, come la repressione del fenomeno corruttivo all'interno della pubblica amministrazione e, più in generale, il buon andamento della stessa, le limitazioni ai diritti fondamentali della persona, e segnatamente quello alla riservatezza, devono sempre operare entro i binari dello stretto necessario, assicurandosi di utilizzare il mezzo che ne determini la minor compressione.

All'orizzonte pare, inoltre, potersi scorgere il ruolo, di una certa importanza, che il diritto all'oblio riveste nell'ambito della trasparenza amministrativa, specialmente laddove la massima reperibilità delle informazioni venga perpetrata attraverso motori di ricerca esterni ai siti *web* istituzionali. Infatti, un simile metodo – ribadito dal legislatore all'art. 9 d.lgs. 33/2013 giusta il quale l'amministrazione non può disporre filtri o altro genere di soluzioni idonee ad impedire ai motori di ricerca di indicizzare ed effettuare ricerche sul materiale pubblicato –, senza rappresentare un *quid pluris* in favore della trasparenza amministrativa, rischia di divenire la fonte di pregiudizi per la *privacy* degli interessati. A fronte di ciò, il Garante per la protezione dei dati personali ha da tempo prospettato, come soluzione più opportuna, l'utilizzo di funzionalità di ricerca interne al sito stesso, in modo da assicurare accessi più selettivi e coerenti con le finalità sottese alla pubblicazione[130].

---

[128] Reg. UE 868/ 2022 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il Reg. UE 1724/2018 (regolamento sulla *governance* dei dati). Il «riutilizzo», cui il *Data Governance Act* dedica l'intero capo II, viene definito *ex* art. 2 del regolamento stesso come «l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico».

[129] In questo senso Corte cost., 21 febbraio 2019, n. 20, cit., punto 5.4.

[130] Cfr. le Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul *web* da soggetti pubblici e da altri enti obbligati, del GPDP, Provv. 28 maggio 2014, doc. *web*. n. 3134436 secondo cui è infatti preferibile «evitare, ove possibile, la reperibilità dei dati personali da parte dei motori di ricerca

Si prospetta come possibile (o forse probabile) il rischio di una "cristallizzazione" dei dati nel *web*, aggravata dalla loro indicizzazione massiva: è infatti facile che un documento informatico possa essere copiato, riprodotto o alterato anche solo parzialmente, rendendo quanto mai ardua la possibilità di ottenerne una cancellazione effettiva, anche dopo che sia decorso il termine di pubblicazione, travalicando così le garanzie approntate dal d.lgs. 33/2013[131]. Sul punto si inserisce l'art. 1, co. 7-*ter* del d.l. 30 dicembre 2019, n. 162, convertito nella l. 28 febbraio 2020, n. 8, recante «disposizioni urgenti in materia di proroga dei termini legislativi, di organizzazione delle pubbliche amministrazioni, nonché di innovazione tecnologica». Secondo tale disposizione, non è consentita l'indicizzazione delle informazioni oggetto di un regolamento di delegificazione (di adeguamento alla sentenza 20/2019) la cui adozione, prevista per il 31 dicembre 2020, e posticipata al 30 aprile 2021, risulta al momento in cui si scrive, ancora inattuata[132]. Tale regolamento dovrebbe essere finalizzato a ridefinire gli obblighi di trasparenza e pubblicità, a carico delle P.A., con riguardo ai compensi e ai dati reddituali e patrimoniali dei titolari amministrativi di vertice, dei titolari di incarichi dirigenziali, nonché dei dirigenti sanitari e di coloro che rivestono posizioni organizzative ad essi equiparate, nel rispetto di criteri indicati dal decreto legislativo stesso *ex* art. 1, co. 7[133].

esterni»; sul collegamento tra diritto all'oblio e trasparenza amministrativa v. L. FEROLA, *Conservazione, indicizzazione e rintracciabilità dei dati, tra diritto all'oblio e dovere di trasparenza*, in L. CALIFANO-C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, cit., pp. 243 ss.; *ivi* anche il contributo di L. CALIFANO, *Trasparenza e* privacy: *la faticosa ricerca di un bilanciamento mobile*, pp. 57-58 nonché pp. 64-65, con riferimento anche alla giurisprudenza del Garante.

[131] Cfr. il *Parere su uno schema di decreto legislativo concernente la revisione e semplificazione delle disposizioni di prevenzione della corruzione, pubblicità e trasparenza*, del GPDP, PROVV. 3 marzo 2016, doc. *web* n. 4772830; e V. FANTI, *La trasparenza amministrativa tra principi costituzionali e valori dell'ordinamento europeo: a margine di una recente sentenza della Corte costituzionale (n. 20/2019)*, in *Federalismi.it*, 2020, 5, pp. 55-56.

[132] La proroga della data di adozione del regolamento è stata effettuata con il d.l. 183/2020 (art. 1, co. 16).

[133] I criteri individuati dalla legge nell'adozione del regolamento sono: «a) graduazione degli obblighi di pubblicazione (…) in relazione al rilievo esterno dell'incarico svolto, al livello di potere gestionale e decisionale esercitato correlato all'esercizio della funzione dirigenziale, tenuto anche conto della complessità della struttura cui è preposto il titolare dell'incarico (…); b) previsione che i dati di cui all'articolo 14, co. 1, lettera f), del decreto legislativo 14 marzo 2013, n. 33, possano essere oggetto anche di sola comunicazione all'amministrazione di appartenenza; c) individuazione, anche in deroga all'obbligo di pubblicazione per i titolari di incarichi dirigenziali (…), dei dirigenti dell'amministrazione dell'interno, degli affari esteri e della cooperazione internazionale, delle forze di polizia, delle forze armate e dell'amministrazione penitenziaria per i quali non sono pubblicati i dati di cui all'articolo 14 del decreto legislativo 14 marzo 2013, n. 33, in ragione del pregiudizio alla sicurezza nazionale interna ed esterna e all'ordine e sicurezza pubblica, nonché in rapporto ai compiti svolti per la tutela delle istituzioni democratiche e di difesa dell'ordine e della sicurezza interna ed esterna». Fino all'entrata in vigore del regolamento di adeguamento alla pronuncia della Corte costituzionale, la norma dispone che non si applicano le misure di responsabilità di cui all'art. 46 (a carico delle pubbliche amministrazioni obbligate alla pubblicazione dei dati reddituali e patrimoniali) e delle sanzioni *ex* art. 47 (per i dirigenti chiamati a comunicare i dati) del d.lgs. 33/2013, ad eccezione dei titolari di incarichi dirigenziali *ex* art. 19, co. 3 e 4 del d.lgs. 165/2001 per i quali, invece, le misure in questione trovano, appunto, applicazione. Sul punto cfr. la Circolare n. 12 del 22

Il diritto all'oblio è strettamente connesso alla qualità dei dati di cui si occupa l'art. 6 d. lgs. 33/2013: la presenza di dati risalenti e non aggiornati, ma nei quali ci si può comunque facilmente imbattere in rete, tramite la ricerca di parole chiave, mal si concilia con l'esigenza di garantire una amministrazione trasparente, dal momento che informazioni di tal genere non presentano certo il carattere tecnico della qualità.

Internet, massimo collettore di dati, fa dunque sorgere il problema relativo alla protezione dei dati personali che vengono indicizzati dai motori di ricerca, restando disponibili per l'utente per un tempo tutt'altro che limitato. Ad essere criticabile – oltre l'eccessività in sé della richiesta di pubblicazione di determinati dati, come nel caso prospettato nella sentenza 20/2019 – può essere anche il fatto che determinati dati, legittimamente pubblicati *ab origine*, relegati poi in una dimensione atemporale, possono divenire obsoleti e non più attinenti alla attualità dei fatti, creando così una discrasia tra la realtà *online* e quella *offline*.

Partendo dall'assunto secondo il quale non si può intendere il diritto all'oblio come un diritto della personalità, come tale assoluto e inviolabile (oltre che imprescrittibile ed inalienabile)[134], le fondamentali esigenze di trasparenza a tutela di interessi individuali e generali[135], richiedono un proporzionale bilanciamento con le esigenze del singolo, non solo a non veder pubblicati i suoi dati personali perché non funzionalmente connessi alle finalità di controllo dell'operato amministrativo, ma anche a che i suoi dati pubblicati siano aggiornati e contestualizzati.

È pertanto indubbiamente necessario ricercare un giusto equilibrio, soppesando le opposte esigenze del caso concreto, utilizzando senz'altro il principio di proporzionalità, in modo da comprendere se l'interesse pubblico alla memoria sia quello preminente.

In quest'ottica sembra quindi possibile parlare del diritto all'oblio quale "questione di *proporzionalità*" perché è proprio il principio di proporzionalità a permearlo e ad indicare la strada da intraprendere per bilanciare correttamente la libera circolazione delle informazioni con il diritto a non veder travisata la propria immagine sociale.

---

marzo 2023 del Ministero dell'Economia e delle Finanze. Secondo A. Corrado, *Gli obblighi di trasparenza dei dirigenti amministrativi: il lento e "incerto" incedere del legislatore*, in *Federalismi.it*, 2021, 20, p. 103, data l'attuale inattuazione del decreto di delegificazione, comincia «una fase di interregno nella quale i principali protagonisti della trasparenza amministrativa (…) cercheranno di individuare, con faticosa interpretazione, la portata degli obblighi di pubblicazione (a fini di trasparenza) previsti per i dirigenti amministrativi, con particolare riguardo alla situazione reddituale degli apicali di tutte le amministrazioni e dei soggetti alle stesse equiparate».

[134] In questo senso, v. G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 2014, 4-5, p. 600, ove, secondo l'A., «non pare che il diritto all'oblio costituisca un diritto in sé e che si debba ampliare il catalogo dei diritti della personalità, dal momento che esso appare comunque strumentale, o al diritto all'identità personale o al diritto alla protezione dei dati personali. Da un punto di vista metodologico, non serve in questo caso procedere alla creazione e alla formulazione di un nuovo diritto, dal momento che i diritti già consolidati sono idonei ad accogliere le esigenze nuove»; dello stesso avviso M. Tampieri, *Il diritto all'oblio e la tutela dei dati personali*, in *Resp. civ. e prev*., 2017, 3, p. 1018.

[135] Cfr. F. Bravo, Software *di intelligenza artificiale e istituzione del registro per il deposito del codice sorgente*, in *Contratto e impr*., 2020, 4, p. 1412, in cui l'A. sottolinea come il principio di trasparenza configuri un «baluardo della democrazia così come di insopprimibili esigenze di tutela della persona, nei suoi diritti e nelle sue libertà fondamentali».

Capitolo XII

Il principio di *privacy by design* e di *privacy by default*

Stefano Faillace

SOMMARIO: 1. Inquadramento normativo. – 2. Portata del principio. – 2.1. La ricostruzione della portata del principio nella dottrina e nei documenti istituzionali: l'impostazione predefinita di misure di protezione dei dati (*privacy by design*) da parte del titolare. Dalla valutazione del contesto alla scelta della tecnologia più adeguata. – 2.2. Le impostazioni di controllo dei dati oggetto del trattamento (*privacy by default*) e il consenso consapevole dell'interessato. – 2.3. L'integrazione contenutistica dei principi di cui all'art. 25 GDPR ad opera delle Linee Guida n. 4/2019 dell'*European Data Protection Board* (EDPB). – 2.4. La fonte delle obbligazioni *ex* art. 25 GDPR e la natura della responsabilità per il loro inadempimento. – 3. Applicazione del principio nella casistica. – 3.1. I provvedimenti del Garante nei confronti di privati: *a)* la *privacy by design* nei rapporti di lavoro. – 3.2. (*segue*): *b)* attività promozionali dell'impresa e obblighi da rispettare in conformità alle prescrizioni del GDPR. – 3.3. La violazione delle norme di cui all'art. 25 del GDPR da parte della pubblica amministrazione.

1. Inquadramento normativo

Il Regolamento europeo per la protezione dei dati personali (GDPR) impone al titolare l'adozione di misure tecniche ed organizzative adeguate, al fine di tutelare i dati personali da trattamenti illeciti. Sistematicamente collocato all'interno del Capo IV, Sezione I, ove si rinviene la disciplina degli obblighi del titolare e del responsabile, l'art. 25 introduce e prevede i concetti di *privacy by design* e *privacy by default*, qualificabili come criteri fondamentali volti a realizzare un'architettura del trattamento dei dati mirata a garantire il rispetto dei principi di cui all'art. 5 del Regolamento[1]. Data la portata trasversale di tale norma, i concetti di *privacy by*

[1] Tra i promotori della *privacy by design*, vi è Ann Cavoukian, *Information and Privacy Commissioner* dell'Ontario, che già negli anni 90 ne elaborò i concetti base (cfr. A. CAVOUKIAN, *Privacy by Design. The 7 Foundational Principles*, Ottawa, 2009, disponibile *online* all'indirizzo www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf). Il concetto di *privacy by design* è stato poi oggetto di discussione in seno alla 32ª Conferenza mondiale dei Garanti per la protezione dei dati personali tenutasi a Gerusalemme il 27-29 ottobre del 2010, all'esito della quale è stata adottata una specifica *Resolution on Privacy by design*. In estrema sintesi, questo documento poneva l'accento su sette principi fondamentali: *a)* agire in modo proattivo e non reattivo, prevenendo anziché correggendo; *b)* la privacy come impostazione di *default*; *c)* la privacy incorporata nella progettazione; *d)* massima funzionalità: valore positivo, non valore zero; *e)* tutela fino alla fine dei processi, protezione piena per l'intero ciclo vitale; *f)* visibilità e trasparenza; *g)* rispetto per la *privacy* dell'utente e dunque centralità del ruolo dell'interessato. In posizione critica su tali principi si veda U. PAGALLO,

design e *privacy by default* possono, peraltro, a loro volta essere qualificati come principi[2], anche se il dato testuale e sistematico sembrerebbe escluderlo, non essendo menzionati tra quelli indicati dall'art. 5 del GDPR[3]. Tuttavia, conferma la succitata interpretazione, da un lato, il fatto che il *considerando* n. 78 del Regolamento si riferisca alla *privacy by design* proprio come ad un «principio», dall'altro, il fatto che il diritto vivente adotti tale qualificazione, a cominciare dalle plurime menzioni rinvenibili nei provvedimenti dell'Autorità Garante[4]. Del resto, in tale endiadi vi è il senso più profondo della legge, che promuove il comportamento proattivo del titolare del trattamento per la tutela dei diritti dell'interessato[5]. Che si tratti, peraltro, di

On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law, in S. GUTWIRTH et al. (ed. by), *European Data Protection: In Good Health?*, Springer Science-Busness media, 2012, pp. 333 ss. Nella dottrina italiana, per tutti vedi BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO *(a cura di) I dati personali nel diritto europeo*, 2019, Torino, pp. 775 ss. Per la dottrina straniera sull'argomento, vedi, *ex multis*, L.A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in *Oslo Law Review*, IV, 2, 2017; D. KLITOU, *A solution, but not a panacea for defending privacy: the challenges, criticism and limitations of privacy by design*, in B. PRENEEL-D. IKONOMOU (eds), *Privacy technologies and policy: first annual privacy forum*, APF 2012, Springer Verlag, 2014, p. 86; A. LEVIN, *Privacy by Design by Regulation: The Case Study of Ontario*, in *Canadian Journal of Comparative and Contemporary Law* 4, 1, 2018, p. 115; C. QUELLE, *Not just user control in the General Data Protection Regulation*, in A. LEHMANN et al. (eds), *Privacy and Identity Management - Facing up to Next Steps*, IFIP AICT, 2017, p. 498; I. RUBINSTEIN-N. GOOD, *The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default*, in *International Data Privacy Law* (2020); A.E. WALDMAN, *Data protection by design? A critique of article 25 of the GDPR,* in *Cornell International Law Journal*, Vol. 53, 2021 Northeastern University School of Law Research Paper No. 411-2021.

[2] Cfr., in tal senso, in dottrina, E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, 1, p. 106; M. RATTI, *commento all'art. 25*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection,* Milano, 2021, p. 414. Si veda anche, al capitolo I del presente volume, F. BRAVO, *I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, alla luce delle* rules of construction.

[3] Sulla distinzione tra norma-principio e norma-regola v. P. PERLINGIERI-P. FEMIA, *Nozioni introduttive e principi fondamentali del diritto civile*, Napoli, 2004, p. 15 ss. Per una riflessione completa e sistematica sui principi nell'ordinamento giuridico nazionale ed europeo, v. G. ALPA, *I principi generali*, in *Trattato di diritto privato*, diretto da G. IUDICA-P. ZATTI, 2ª ed., Milano, 2006.

[4] L'Autorità garante per la protezione dei dati personali, in molti suoi provvedimenti, ha, infatti, qualificato i concetti di *privacy by design* e *privacy by default* come principi del trattamento dei dati personali (cfr., a riguardo, *ex multis*, GPDP, 19 luglio 2018, n. 9069072; GPDP, 19 luglio 2018, n.9039945; GPDP, 28 giugno 2018, n. 9023246 e GPDP, 18 ottobre 2018, n. 9084531, tutti in *garanteprivacy.it*). Si veda anche quanto illustrato, *amplius*, al par. 3 del presente scritto.

[5] Come affermato da F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 792, anche se concettualmente distinte, la *privacy by design* e la *privacy by default* possono essere intese unitariamente, come una sorta di endiadi, in quanto la prima richiede la seconda. Cfr., a riguardo pure le Linee Guida EPDB 4/2019 al par. 2.5, disponibili al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_enhttps://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, secondo cui «la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita sono concetti complementari che si rafforzano vicendevolmente. Gli interessati trarranno maggiori benefici dalla protezione dei dati per

principi ormai immanenti nell'ordinamento transnazionale, che travalicano i solchi del regolamento in oggetto, lo si può infine dedurre da altre disposizioni normative, quali la proposta di regolamento *e-privacy* e la direttiva sui contratti di fornitura di contenuti e servizi digitali n. 770/2019, che tutte richiamano tale concetto[6].

L'idea di fondo accolta nel nuovo Regolamento europeo sulla *privacy*, visto il contesto attuale, caratterizzato dalla rapidità dell'evoluzione tecnologica e dalla globalizzazione, è quella di ricorrere ad una soluzione di tutela della protezione dei dati personali che possa iniziare proprio in fase di progettazione, al fine di riuscire a predisporre un'architettura (del *software*, ma anche del dispositivo, del sistema informatico nel suo complesso, etc.) in grado di offrire adeguate garanzie per la protezione dei dati personali[7].

Con un più marcato intervento rispetto al previgente assetto normativo, nel Regolamento 2016/679 si è voluto, insomma, porre l'accento sull'esigenza di assicurare un adeguato livello di protezione dei dati personali, sin dalla fase della sua «progettazione»[8].

---

impostazione predefinita se verrà attuata contestualmente la protezione dei dati fin dalla progettazione, e viceversa».

[6] Nel *considerando* n. 48 della dir. n. 770/2019, si afferma che «Il regolamento (UE) 2016/679 o qualsiasi altra fonte di diritto dell'Unione in materia di protezione dei dati dovrebbero applicarsi pienamente al trattamento dei dati personali in relazione ai contratti che rientrano nell'ambito di applicazione della presente direttiva. La presente direttiva non dovrebbe inoltre pregiudicare i diritti, gli obblighi e i rimedi extracontrattuali di cui al regolamento (UE) 2016/679. È altresì possibile considerare, in funzione delle circostanze del caso, che gli elementi che determinano un difetto di conformità rispetto ai requisiti di cui al regolamento (UE) 2016/679, inclusi principi fondamentali quali i requisiti in materia di minimizzazione dei dati, *protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*, costituiscano un difetto di conformità del contenuto digitale o del servizio digitale rispetto ai requisiti di conformità soggettivi od oggettivi di cui alla presente direttiva». Anche nella proposta di regolamento *e-privacy* (versione 10 gennaio 2017) al *considerando* n. 23 si fa riferimento ai «principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita». Per la differenza tra «regola» e «principio», L. Mengoni, *Spunti per una teorìa delle clausole generali*, in *Riv. crit. dir. priv.*, 1986, p. 3 ss.; Id., *I principi generali del diritto e la scienza giuridica*, in *Dir. lav*., 1992, I, pp. 3 ss.

[7] Si legge nel considerando 6 del Regolamento 2016/679 che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento della loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazione internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali».

[8] Cfr. A. Principato, *Verso nuovi approcci alla tutela della* privacy: privacy by design *e* privacy by default settings, in *Contratto e impresa/Europa*, 2015, pp. 197 ss. ed, ivi, spec. p. 199, ove si rimarca che il concetto di *privacy by design* (…) si fonda su un approccio proattivo alla tutela dei dati personali nel contesto di prodotti e servizi informatici, basato sull'inserimento degli strumenti a tutela della *privacy* in tali prodotti sin dall'inizio della loro progettazione. Non si tratta di principi introdotti *ex novo* nel Regolamento, essendo già presenti nelle disposizioni del Codice in materia di protezione dei dati personali, in particolare ove venivano normati il principio di stretta necessità,

La disposizione dell'art. 25 è dunque tra le norme più ambiziose dell'intera riforma. In essa, forse più che altrove, mira a realizzarsi uno tra i principali obiettivi posti dal GDPR: quello della responsabilizzazione del titolare, cui competerà, secondo criteri di ragionevolezza e diligenza, valutare l'adeguatezza delle misure tecniche ed organizzative prescelte[9].

Gli obblighi di protezione, aventi ad oggetto l'applicazione di adeguate misure tecniche ed organizzative funzionali all'attuazione dei principi ed alla garanzia dei diritti che la disciplina intende salvaguardare, pervadono tutte le fasi del trattamento sin dal momento ideativo e progettuale ed in maniera strutturale, costante e dinamica, dovendo essere applicate per l'intero ciclo di vita del trattamento, con gli aggiornamenti eventuali dovuti in relazione all'evolversi sia della caratteristiche del trattamento nel corso del tempo, sia delle tecniche di protezione[10].

La disciplina concernente gli obblighi di adozione delle misure di sicurezza possiede peraltro una valenza plurima, in relazione alle diverse esigenze che è protesa a soddisfare, nella sua prospettiva polifunzionale. Infatti, le misure richieste non proteggono solo i dati personali dell'interessato e le connesse situazioni giuridiche soggettive, ma assolvono contestualmente all'ulteriore funzione di garantire il corretto raggiungimento delle finalità del trattamento volute dal titolare o che il titolare è tenuto a raggiungere nello svolgimento di funzioni pubbliche o di compiti

all'art. 3 Codice *privacy*, e il principio di pertinenza e non eccedenza rispetto alle finalità (legittime) del trattamento, anche con riguardo al periodo di conservazione, *ex* art. 11, co. 1, lett. *d)* ed *e)*, Codice *privacy*. F. BRAVO, *L'architettura del trattamento e la sicurezza dei dati e dei sistemi*, cit. p. 809, con riferimento alla *privacy by design*, rileva, peraltro, come nel *considerando* n. 46 della direttiva 96/45/CE, ora abrogata, veniva evidenziato «che la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento dei dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento (…)», e come nel nostro diritto interno si trovassero invece disposizioni di segno opposto. Si consideri, peraltro, che nel Codice in materia di protezione dei dati personali, nel testo ante-riforma del 2018, non vi era alcun riferimento espresso a tecniche di tutela dei dati personali *by design*.

[9] Il principio di responsabilizzazione prevede che il titolare sia responsabile della conformità a tutti i principi esplicitati nella normativa e sia in grado di dimostrare tale conformità; in tal modo può comprovare gli effetti delle misure adottate per tutelare i diritti degli interessati e i motivi per cui tali misure sono considerate adeguate ed efficaci, dimostrando ad esempio in che modo una determinata misura sia adeguata a garantire efficacemente il principio di limitazione della conservazione. Per poter trattare i dati responsabilmente, il titolare dovrebbe sia conoscere le norme in materia di protezione dei dati sia essere in grado di darvi attuazione. Ciò comporta che egli comprenda gli obblighi in materia di protezione dei dati imposti nei suoi riguardi dal GDPR e sia in grado di adempiere a tali obblighi. Con il termine "adeguate" si intende che le misure e le necessarie garanzie devono essere idonee a conseguire la finalità prevista, ossia devono attuare efficacemente i principi di protezione dei dati. Il requisito di adeguatezza è quindi strettamente connesso al requisito di efficacia. Standard, migliori prassi e codici di condotta riconosciuti da associazioni e da altri organismi che rappresentano categorie di titolari del trattamento possono essere utili ai fini della determinazione di misure adeguate. Tuttavia, il titolare deve verificare l'adeguatezza delle misure con riguardo allo specifico trattamento.

[10] Cfr. in tal senso e per ulteriori approfondimenti, F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 790 ss.

di pubblico interesse[11]. Del resto, il diritto alla protezione dei dati personali «non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (…)»[12].

Si pensi ad esempio all'esercizio dei diritti fondamentali di cui è portatore il titolare del trattamento, incluso il diritto alla manifestazione del pensiero, il diritto di cronaca, il diritto di impresa; si pensi ancora, sul versante più strettamente patrimoniale, all'utilizzazione economica delle «informazioni»[13].

Del resto, il titolare è da individuare in colui che determina non solo le finalità ma anche i mezzi e le modalità del trattamento (v. art. 4, par. 1, n. 7, e art. 26, par. 1, Regolamento 2016/679), esercitando prerogative che gli competono in ragione dell'esercizio di un diritto (ad es. quello di iniziativa economica) o di pubblici poteri

[11] Cfr. F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 779. Già con riguardo al codice in materia di protezione dei dati personali era stato messo in evidenza come la sicurezza del trattamento, imposta *in primis* a tutela dei diritti dell'interessato, fosse funzionale – al contempo – anche alla tutela del patrimonio informativo del titolare ed al perseguimento delle proprie finalità. Cfr., ad es., G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit., p. 250, per la quale «l'intero Codice può essere letto come una legge sull'utilizzo dell'informazione: esso non disciplina soltanto i dati riservati ma, più in generale, [la circolazione de]i dati e [del]le informazioni. Esso ha ad oggetto l'intero flusso informativo nell'impresa e nell'ente e non soltanto il singolo dato. Il Codice, come già la L. 675/1996, va nel senso di una tutela dell'informazione in senso lato e costituisce uno stimolo per il soggetto che tratta dati personali, soggetto pubblico o privato, ad acquisire consapevolezza del proprio patrimonio informativo. L'informazione rappresenta dunque un bene del quale tanto gli enti pubblici quanto le imprese private devono acquisire piena consapevolezza: un bene da tutelare e da proteggere con gli strumenti giuridici che ormai la normativa impone di adottare (…). L'implementazione e la corretta applicazione delle misure di sicurezza consentono non solo di rispettare il dettato normativo ma anche di migliorare la struttura organizzativa del soggetto titolare delle operazioni di trattamento».

[12] Cfr., in tal senso, il *considerando* n. 4, Regolamento UE 2016/679. Sul concetto di «funzione sociale» di cui al considerando da ult. cit. cfr. A. Ricci, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2017, 2, pp. 586 ss. Tra i diritti fondamentali da contemperare con il diritto alla *privacy* vi sono «(…) la libertà di pensiero, di coscienza e di religione, la libertà di espressione e di informazione, la libertà d'impresa (…)» (sempre *considerando* n. 4) Ne danno poi conto anche i *considerando* nn. 5 e 6, ove viene fatto riferimento alla necessità di garantire i flussi transfrontalieri di dati personali in tutta l'UE tra attori pubblici e privati, nonché tra autorità nazionali degli Stati membri, garantendo il processo continuo di integrazione sociale ed economica all'interno dell'Unione medesima.

[13] Per F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 815, la norma si presenta come ontologicamente «duale», racchiudendo in sé la dimensione dell'obbligo, espressamente enunciato nell'art. 25 cit. e quella del «potere», ricavabile dall'interpretazione sistematica: le misure tecniche e organizzative ivi prescritte trascenderebbero la mera dimensione dell'obbligo, traducendosi in un «assetto materiale» organizzato (predisposto) dal titolare medesimo nell'ambito della propria attività, non privo di significatività per il diritto in termini di «poteri» e riconducibile per lo più al diritto alla libertà di iniziativa economica o all'esercizio di pubblici poteri o funzioni, rispettivamente per i trattamenti posti in essere da soggetti privati e/o pubblici, fatti salvi i necessari distinguo. Sulla tutela dell'iniziativa economica e delle funzioni pubbliche (che necessitano del trattamento dei dati per poter essere svolte), nonché la salvaguardia di interessi di carattere generale e di ordine sociale, cfr. G. Corasaniti, *Esperienza giuridica e sicurezza informatica*, Milano, 2003, pp. 52 ss., nonché F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, *passim*.

(come avviene ad es. nel caso di svolgimento di pubbliche funzioni da parte della p.a.)[14]. Sicché, rientra nelle di lui prerogative stabilire di porre in essere un «trattamento di dati personali» nell'ambito dello svolgimento dell'attività da questi svolta (imprenditoriale, libero professionale, connessa all'esercizio di pubbliche funzioni), e di decidere quali strumenti tecnologici, quali assetti organizzativi e quali procedure adottare per realizzare le finalità (lecite) dal medesimo individuate, nel rispetto – ovviamente – dei principi, delle «garanzie» e dei diritti (per l'interessato) previsti dalla normativa in parola[15]. Anche là dove la condizione di liceità del trattamento sia il «consenso» fornito dall'interessato, quest'ultimo è in grado solamente di fornire o meno il proprio assenso al trattamento, per le finalità e con le modalità stabilite dal titolare e comunicate all'interessato tramite l'informativa di cui all'art. 13 (e s.) del Regolamento, senza alcun potere di intervento nella determinazione delle modalità del trattamento, normalmente spettanti al titolare, nel rispetto dei principi fissati in materia di protezione dei dati personali[16].

Nel momento in cui il titolare determina le modalità del trattamento, predisponendo un assetto materiale per la raccolta e la gestione dei dati, esercita un «potere» giuridicamente rilevante con il quale fissa, anche in maniera fattuale, le «regole» con cui i dati vengono trattati: si tratta di «regole» osservate nei confronti dei terzi (gli interessati a cui i dati personali si riferiscono), sia nel caso in cui il trattamento sia legittimato dal consenso, sia nel caso in cui le condizioni di liceità operanti prescindano da esso[17].

Peraltro, la prospettiva «funzionale» di tutela delineata dalla normativa europea mira a salvaguardare anche il mercato. Infatti, le reti e i sistemi informativi svolgono un ruolo vitale nella società, sicché la loro affidabilità e la loro sicurezza è «essenziale (…) per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno» (*considerando* n. 1), nonché per l'agevolazione dei movimenti transfrontalieri di beni, servizi e persone, sicché anche sotto tale profilo la «sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno» (*considerando* n. 3).

Entrambi gli obblighi di protezione dei dati personali «sin dalla progettazione» e «per impostazione predefinita» sono soggetti al principio generale – delineato all'art. 24, par. 1, del Regolamento 2016/679 – secondo cui il titolare del trattamento è tenuto a garantire e ad essere in grado di dimostrare – mediante misure tecniche e organizzative adeguate e, se necessario, aggiornate – che il trattamento sia effettuato conformemente a quanto previsto dal Regolamento. Preoccupato però delle possibili

---

[14] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., *passim* (e, ivi, spec. p. 107 ss. e p. 109, nota 115), nonché ID., *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 816.

[15] *Ibidem*, p. 816.

[16] *Ibidem*, p. 816.

[17] Cfr., ancora, F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 814 ss., che, con le lenti del civilista, ampiamente descrive e inquadra la fase di predisposizione da parte del titolare dell'assetto materiale per la raccolta e la gestione dei dati, ed elenca i rischi derivanti da quella che è stata icasticamente definita la "dittatura dell'algoritmo" (S. RODOTÀ, *Il mondo della rete. Quali i diritti, quali i vincoli,* Roma-Bari, 2014, pp. 33 ss.).

conseguenze dell'applicazione di tale norma, che nella prassi potrebbe risultare eccessivamente gravosa per il titolare, il legislatore europeo ha finito per mitigarne la portata, prevedendo – quanto agli aspetti di carattere probatorio – che un meccanismo di certificazione approvato ai sensi dell'art. 42 del Regolamento 2016/679 possa essere utilizzato come elemento utile per dimostrare la conformità ai requisiti di cui ai parr. 1 e 2[18]. Ai sensi dell'art. 25, par. 3, «l'agevolazione opera tuttavia solamente sul piano probatorio e non su quello sostanziale, attinente ai profili di responsabilità: non opera dunque come scriminante o come "*mitigating factor*"»[19]. Al riguardo s'è chiarito che «La norma in esame va letta, infatti, in uno con l'art. 42, par. 4, prima parte, là dove si prevede che la certificazione innanzi richiamata "non riduce le responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità del presente regolamento"»[20].

Il principio della *privacy by design*, di cui all'art. 25 del Regolamento 2016/679, per un verso appare efficace nell'offrire una tutela penetrante in materia di protezione dei dati personali, introducendo nell'architettura del sistema strumenti di controllo che consentano all'interessato di «governare», quantomeno in parte, le modalità e l'ambito del trattamento dei propri dati, mediante un suo intervento sui meccanismi di funzionamento del sistema[21] e sulle impostazioni[22] durante il ciclo di

[18] Sul punto cfr., *amplius*, R. Davico, *Le certificazioni nel nuovo regolamento UE sulla privacy*, relazione tenuta nell'ambito del Convegno sul tema «*Cybersecurity e data protection*», organizzato presso l'Università di Bologna l'11 maggio 2016, nell'ambito delle attività del Corso di Alta Formazione in «*Data Protection e Privacy Officer*» (https://site.unibo.it/dpo e https://www.dataprotectionprivacy.it). La certificazione di cui all'art. 42 può essere utilizzata come un elemento per dimostrare la conformità con gli obblighi di cui all'art. 25 GDPR. Parimenti, i documenti che attestano la conformità con la *privacy by design* potrebbero risultare utili durante una procedura di certificazione. Ciò significa che laddove un trattamento svolto da un titolare o un responsabile sia stato certificato ai sensi dell'art. 42, le autorità di controllo ne tengono conto nella loro valutazione della conformità con il GDPR. Quando un trattamento è certificato a norma dell'art. 42, gli elementi che contribuiscono ad attestare la conformità all'art. 25, par. 1 e 2, sono le procedure di progettazione, ossia la procedura per determinare i mezzi di trattamento, la *governance*, nonché le misure tecniche e organizzative finalizzate ad attuare i principi di protezione dei dati. I criteri di una certificazione in materia di protezione dei dati sono definiti dagli organismi di certificazione o dai titolari dello schema di certificazione e poi approvati dall'autorità di controllo competente o dall'EDPB. Anche qualora un trattamento sia certificato ai sensi dell'art. 42, il titolare è comunque tenuto a garantire il monitoraggio costante e il miglioramento della conformità ai criteri di cui all'art. 25.

[19] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 804. Si pensi, ad esempio, all'ipotesi in cui un titolare aderisca ad un codice di condotta *ex* art. 40 del Regolamento 2016/ 679 oppure ottenga la certificazione di cui all'art. 42, ma non adotti poi concretamente – o cessi di adottare – le misure tecniche e organizzative previste dal codice di condotta o dal sistema di gestione posto a base dell'ottenuta certificazione.

[20] *Ibidem*

[21] Per esempio, inserendo o disinserendo le funzionalità di geolocalizzazione e tracciamento di un *electronic device*, oppure la memorizzazione o meno «*on cloud*» di dati, comprese *email*, foto, ecc.

[22] Ad es., consentendo di cifrare o meno i dati presente su un'area di memoria; di scegliere se utilizzare o meno le credenziali biometriche per l'accesso ad un dispositivo o ad un'altra risorsa informatica; di selezionare l'ambito di diffusione dei propri dati contrassegnando i contenuti come «privati» ad accesso riservato, «pubblici» senza restrizioni di accesso o «semi-privati»/«semi-pubblici», con accesso condiviso a soggetti predeterminati o a categorie di soggetti predeterminati.

vita dei propri dati personali, ma, per altro verso, pone dubbi in ordine alle situazioni giuridiche configurabili riguardo ad esso[23].

Alcune criticità vanno certamente considerate nell'approccio alla normativa in commento. In particolare, la realizzazione di interventi «architetturali» sul *software* o sull'*hardware* utilizzati per il trattamento dei dati personali al fine di garantire la *compliance* alla normativa in materia di *data protection* (c.d. *hardcoding*) è un'operazione non agevole da tradurre nella prassi operativa[24], sussistendo diversi ostacoli che ne compromettono la realizzabilità[25]. Si pensi alla complessità del sistema normativo che si occupa di protezione dei dati personali, non confinabile alle sole disposizioni del Regolamento (ad esempio, in ambito europeo, si pensi all'art. 8 della Carta dei diritti fondamentali dell'UE, nonché alla proposta di Regolamento *e-Privacy* in materia di comunicazioni elettroniche; in ambito nazionale, tra le altre norme, alle disposizioni relative al controllo a distanza dei lavoratori). Peraltro, risulta francamente arduo, dal punto di vista tecnico, tradurre la regola «giuridica» in regola «tecnica» incorporata nel *software* o nell'*hardware*, per via delle modalità con cui viene formulata, della necessità di interpretazione, spesso non univoca e cangiante nel tempo, anche in relazione agli orientamenti giurisprudenziali o alle decisioni e ai pareri dell'autorità di controllo[26].

[23] Cfr. F. BRAVO, *Data Management Tools and Privacy by Design and by Default*, in R. SENIGAGLIA-C. IRTI-A. BERNES (ed. by), *Privacy and Data Protection in Software Services*, Springer, 2022, pp. 85-95.

[24] F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 830.

[25] Secondo il *report* «*Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*» dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), la *privacy by design* è un concetto poliedrico: nei documenti giuridici è generalmente descritta in termini molto ampi come principio generale; dagli informatici e dagli ingegneri, è spesso equiparata all'uso di specifiche tecnologie di miglioramento della *privacy* (c.d. *privacy-enhancing technologies* o PET). Si tratta, infatti, di un processo che coinvolge varie componenti tecnologiche e organizzative, con il fine di tradurre in termini pratici e operativi i principi della *privacy by design*, incorporando i principi all'interno del ciclo di vita dei sistemi informatici dedicati al trattamento dei dati personali. Questo processo richiede un approccio sistematico e metodologico, per trasferire le proprietà e le funzionalità *privacy* individuate nelle fasi di analisi del *concept* (requisiti di *privacy* individuati) nella progettazione dell'architettura e realizzazione degli elementi del sistema (strategie e soluzioni concrete), lavorando così in modo sequenziale secondo diversi livelli di astrazione. Sul punto è interessante il documento recentemente pubblicato dell'ENISA, che fornisce chiarimenti e delucidazioni utili circa l'implementazione pratica degli aspetti tecnici della *privacy by design* e *by default* e ad esso si rinvia (*Data protection engineering, From Theory to Practice*, gennaio 2022, in *https://www.enisa.europa.eu/publications/data-protection-engineering*).

[26] Così F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 830-831.

2. Portata del principio

2.1. La ricostruzione della portata del principio nella dottrina e nei documenti istituzionali: l'impostazione predefinita di misure di protezione dei dati (*privacy by design*) da parte del titolare. Dalla valutazione del contesto alla scelta della tecnologia più adeguata

Con l'espressione «impostazione predefinita», nell'ambito del trattamento di dati personali, ci si riferisce alle scelte compiute dal titolare rispetto a valori di configurazione od opzioni di un'applicazione informatica, un servizio o una periferica o una procedura di trattamento manuale, tali da incidere sulla quantità dei dati personali raccolti[27], sulla portata del trattamento[28], sul periodo di conservazione e sull'accessibilità[29].

Il Regolamento impone che le misure tecniche ed organizzative identificate dal titolare siano tese al duplice scopo di attuare con efficacia i principi di protezione dei dati personali – innanzitutto quello di minimizzazione – nonché ad integrare nel trattamento le relative garanzie. Si tratta di una finalità che si somma, sovrapponendovisi, a quella originariamente e primariamente perseguita dal titolare, dalla quale si differenzia proprio per il carattere cogente che la norma vi imprime, al punto da

[27] Occorre valutare sia la quantità dei dati raccolti, in senso stretto, sia la pertinenza dei dati per le finalità di trattamento perseguite. Il titolare dovrà optare per la raccolta del numero minimo di dati necessari per l'attivazione di un servizio o di un prodotto, mentre potrà dare la possibilità all'utente di condividere più dati attraverso le impostazioni. Ad esempio, un'applicazione che aiuta l'utente a navigare in città non dovrebbe raccogliere di default i dati relativi ai posti preferiti dell'utente, ma potrebbe offrire all'utente l'opzione di memorizzare tali luoghi per consentirgli di selezionare più velocemente quelli maggiormente frequentati (ad esempio, lavoro, casa, aeroporto, ecc.). All'interno delle Linee guida EDPB n. 4/2020, in materia di *contact tracing*, emanate nel contesto dell'emergenza epidemiologica da COVID-19, si sottolinea che nell'utilizzo di un'applicazione *software* per il tracciamento dei contatti è necessario assicurare, oltre al rispetto del c.d. principio di "minimizzazione dei dati", *ex* art. 5 del GDPR, l'adeguata attuazione dei principi di protezione *by design* e *by default*, attraverso le seguenti attività: utilizzo dei soli dati di prossimità, senza tracciare la posizione dei singoli utenti; adozione di misure adeguate per prevenire la reidentificazione degli interessati, poiché l'applicazione può funzionare senza necessariamente identificare direttamente la persona; memorizzazione delle informazioni raccolte nell'apparecchiatura terminale dell'utente, assicurando il rispetto del principio di minimizzazione.

[28] A questo riguardo, si consideri, ad esempio, che il fornitore di un'applicazione ludica su dispositivi mobili non dovrebbe trattare i dati personali relativi all'utilizzo del dispositivo da parte dell'utente, salvo che sia quest'ultimo a scegliere di condividere tali informazioni con il fornitore attraverso opzioni tra cui l'utente può liberamente scegliere.

[29] Secondo le Linee guida EDPB n. 4/2019, i dati personali raccolti non devono essere conservati se non sono necessari per la finalità del trattamento e non sussista un'altra finalità compatibile, né altro fondamento giuridico ai sensi dell'art. 6, par. 4. Qualsiasi conservazione dovrebbe essere obiettivamente giustificabile da parte del titolare del trattamento in quanto necessaria, in base al principio di responsabilizzazione. Il titolare del trattamento deve limitare il periodo di conservazione all'arco di tempo necessario per il raggiungimento della specifica finalità. Se i dati personali non sono più necessari ai fini del trattamento, allora per impostazione predefinita devono essere cancellati o resi anonimi. Il titolare, inoltre, dovrebbe disporre di procedure sistematiche, integrate nel trattamento, per la cancellazione o l'anonimizzazione dei dati.

rendere un'eventuale inottemperanza sanzionabile anche severamente ai sensi degli art. 83 ss. Peraltro, la mancata conformità alle norme del regolamento comporterà anche l'assunzione di responsabilità nei confronti degli interessati. La selezione di quali siano, in concreto, le necessarie, aggiuntive attività di trattamento è oggetto di una libera scelta del titolare.

L'art. 25, par. 1, impone al titolare una serie ben definita di obblighi[30]. Innanzitutto, questi deve valutare le circostanze relative al trattamento nel contesto delle sue attività, vale a dire: lo stato dell'arte[31], i costi di attuazione[32], la natura, il contesto e le finalità del trattamento[33], nonché possibili rischi per diritti e libertà degli inte-

[30] L'art. 25 gioca un ruolo importante nei riguardi di numerose disposizioni del regolamento, nelle quali esso viene direttamente o indirettamente richiamato. Si pensi, ad esempio, in relazione alla comunicazione all'interessato di un *data breach*, a quanto previsto dalla lett. *a)*, par. 3, dell'art. 34, secondo cui il titolare può essere esonerato da tale comunicazione se «ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione»; lo stesso valga per la disposizione di cui al par. 2 dell'art. 83, lett. *d)*, ai sensi del quale la determinazione delle sanzioni applicabili per il caso di violazioni dovrà tener conto, tra l'altro, del «grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto» ai sensi dell'art. 25. E ancora: al fine di determinare la compatibilità tra le finalità perseguite da due distinti trattamenti di dati personali, l'art. 6, par. 4, lett. *e)* richiede che si tenga conto, tra l'altro, «dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione». Analoghe considerazioni valgono anche per la previsione del par. 1 dell'art. 32 [«Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: *a)* la pseudonimizzazione e la cifratura dei dati personali; (…)]; per gli adempimenti richiesti al momento dell'effettuazione di una valutazione preliminare di impatto di cui all'art. 35 o per procedere alla designazione del responsabile della protezione dei dati, c.d. *data protection officer* o DPO, ai sensi degli artt. 37 ss.

[31] Le Linee guida 4/2019 dell'EDPB precisano che il riferimento allo «stato dell'arte» impone l'obbligo ai titolari, allorché determinano le misure tecniche e organizzative adeguate, di tenere conto degli attuali progressi compiuti dalla tecnologia disponibile sul mercato e di rimanere sempre aggiornati sulle opportunità e i rischi per il trattamento. Lo «stato dell'arte» è un concetto dinamico che non può essere definito staticamente con riguardo a un determinato momento, bensì dovrebbe essere oggetto di una valutazione continuativa nel contesto dei progressi tecnologici. La mancanza di misure organizzative adeguate può ridurre o compromettere del tutto l'efficacia di una tecnologia scelta. Possono costituire esempi di misure organizzative: l'adozione di politiche interne, la formazione aggiornata in materia di tecnologia, sicurezza e protezione dei dati, nonché politiche di gestione e di *governance* della sicurezza informatica. Quadri di riferimento standard, certificazioni, codici di condotta ecc. esistenti e riconosciuti possono contribuire a indicare l'attuale «stato dell'arte» nello specifico ambito di utilizzo. Qualora tali standard esistano e prevedano un livello elevato di protezione per l'interessato in conformità (o in misura superiore) ai requisiti giuridici, i titolari dovrebbero tenerne conto nella progettazione e nell'attuazione delle misure di protezione dei dati.

[32] Il titolare può tenere conto del costo di attuazione allorché sceglie e applica misure tecniche e organizzative adeguate e garanzie necessarie che mettono efficacemente in atto i principi al fine di tutelare i diritti degli interessati. Il costo si riferisce alle risorse in generale, compresi il tempo e le risorse umane. Il fattore costo implica che il titolare non impieghi una quantità sproporzionata di risorse nel caso in cui esistano misure alternative, meno dispendiose, ma efficaci.

[33] Secondo le Linee guida EPDB n. 4/2019, il concetto di natura coincide con le caratteristiche intrinseche del trattamento. Ne sono esempi le categorie particolari di dati personali, il processo decisio-

ressati. Compiuta la valutazione dello *status quo*, incombe sul titolare una seconda serie di obblighi. Egli dovrà considerare, sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, quali misure tecniche e organizzative possono reputarsi adeguate per soddisfare i requisiti previsti dal GDPR. Se il titolare utilizza *software* commerciali o di terzi, dovrà eseguire una valutazione dei rischi del prodotto e accertarsi che siano disattivate le funzioni che non hanno una base giuridica o che non sono compatibili con le finalità previste del trattamento[34]. Infine,

nale automatizzato, i rapporti di forza asimmetrici, l'imprevedibilità del trattamento, la difficoltà per l'interessato di esercitare i propri diritti, ecc. L'ambito di applicazione fa riferimento alla dimensione e all'ampiezza del trattamento. Il contesto riguarda le circostanze nel trattamento che possono influenzare le aspettative degli interessati, mentre la finalità si riferisce agli obiettivi del trattamento.

[34] Il Regolamento non può trovare applicazione nei confronti dei produttori di strumenti tecnologici se non rivestano, almeno in parte, la qualità di titolari o contitolari del trattamento. Il *considerando* n. 78 del Reg. 2016/679, infatti, si rivolge ai «produttori» non come destinatari diretti di tali obblighi, ma come soggetti nei cui confronti va operata un'azione di «incoraggiamento», secondo le logiche della moral suasion, tipiche della «responsabilità sociale». Il titolare del trattamento, che non abbia la possibilità tecnica di intervenire egli stesso in fase di progettazione, determinando l'architettura «*privacy-compliant*» dello strumento da utilizzare, è pur sempre obbligato, in fase di determinazione dei mezzi da impiegare per il trattamento, ad organizzarsi per attuare in modo efficace il principio di *privacy* (o *data protection*) *by design*, ricorrendo a strumenti che, in base allo stato dell'arte, siano stati approntati dal produttore conformemente alle prescrizioni del Regolamento (art. 25, co. 1). Come evidenziato dal Garante privacy (GPDP, Provv. 28 giugno 2018 n. 396), i fornitori dovranno essere selezionati dal titolare del trattamento anche valutando il livello di conformità che il titolare potrà raggiungere utilizzando tali servizi o prodotti. Pertanto, il titolare, che delega alcune attività di progettazione di un servizio o che seleziona il prodotto di un fornitore destinato a processi di trattamento di dati personali, dovrà assicurarsi che tale prodotto o servizio sia già stato ideato in modo da garantire la protezione dei dati fin dalla progettazione e per impostazione predefinita. Al fornitore o al responsabile del trattamento però potrà essere richiesto di massimizzare ogni sforzo in termini di trasparenza nei confronti della propria clientela circa le funzionalità *privacy* dei propri prodotti o servizi, in modo che il titolare possa avvalersene al meglio. Vi è inoltre la possibilità di una concreta incorporazione della *data protection* nelle maglie dei rimedi contrattuali (*ex multis*, vedi F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in *I dati personali nel diritto europeo*, cit., pp. 835 ss. A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ*., 2020, p. 889). Questa evenienza, seppur non ribadita espressamente nel corpo della dir. n. 770/2019, viene esplicitata nell'ambito del *considerando* n. 48 della medesima direttiva, recepita poi con d.lgs. n. 282 del 26 novembre 2021, ove si afferma che «il regolamento (UE) 2016/679 o qualsiasi altra fonte di diritto dell'Unione in materia di protezione dei dati dovrebbero applicarsi pienamente al trattamento dei dati personali in relazione ai contratti che rientrano nell'ambito di applicazione della presente direttiva. La presente direttiva non dovrebbe inoltre pregiudicare i diritti, gli obblighi e i rimedi extracontrattuali di cui al regolamento (UE) 2016/679. È altresì possibile considerare, in funzione delle circostanze del caso, che gli elementi che determinano un difetto di conformità rispetto ai requisiti di cui al regolamento (UE) 2016/679, inclusi principi fondamentali quali i requisiti in materia di minimizzazione dei dati, protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita, costituiscano un difetto di conformità del contenuto digitale o del servizio digitale rispetto ai requisiti di conformità soggettivi od oggettivi di cui alla presente direttiva». In argomento, vedi Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ*., 2019, p. 517. Basti ricordare il caso di *software* di cifratura inadeguati che comportino la divulgazione non autorizzata a terzi o l'ipotesi in cui le informazioni personali di chi si accinge ad acquisire un prodotto o servizio siano esposte a *spyware* e rischino dunque un utilizzo abusivo da parte di terzi (lo stesso *consideran-*

terminata la complessa fase di valutazione, il titolare dovrà "integrare nel trattamento le necessarie garanzie" per soddisfare i requisiti previsti dal GDPR e tutelare i diritti degli interessati.

Va ricordato come l'obbligo legale imposto dal regolamento sarà assolto se il trattamento, comprensivo delle attività ulteriori necessarie per una configurazione di "*privacy by design*", sarà condotto alla luce di tutti i principi disciplinati all'art. 5 GDPR. Si tratta innanzitutto dei principi menzionati al par. 1 di tale disposizione, alle lettere da *a)* a *f)*, e dunque liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, cioè sicurezza, conservazione sicura[35]; il par. 2 dell'art. 5 introduce poi un ulteriore principio cui è improntato l'intero Regolamento, quello dell'*accountability*, o responsabilizzazione del titolare, sul quale peraltro grava l'onere di comprovare la conformità del proprio agire ai principi enumerati al paragrafo precedente.

Il principio sul quale, lo si è accennato, il regolamento pone un accento specifico e di cui l'art. 25 fa, ancorché esemplificativamente, espressa menzione, è quello codificato alla lett. *c)* dell'art. 5, che impone che i dati oggetto di trattamento siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati")». Deve essere sottolineato che il rispetto del principio di minimizzazione va interpretato come riferito tanto ad una dimensione quantitativa dei dati, dal momento che ne impone il trattamento esclusivamente nella misura indispensabile al conseguimento dello scopo, quanto ad una qualitativa, che

do n. 48 cit. offre una casistica esemplificativa a tal riguardo). Analogo ragionamento si applicherà qualora i contenuti digitali siano forniti su supporti materiali, nonché al supporto materiale stesso, purché quest'ultimo sia esclusivamente il contenuto del vettore digitale (Si pensi al caso in cui il contenuto sia fornito su DVD, CD, chiavi USB, schede di memoria, ecc.). Qui, infatti, si assiste ad una forma di integrazione fra la dir. n. 770/2019 in discorso e la coeva dir. n. 771/2019, in materia di beni di consumo (in tal senso, vedi i *considerando* n. 13-14 della dir. n. 771/2019, nell'ottica di rispondere alle aspettative dei consumatori e garantire un quadro giuridico semplice e chiaro per gli operatori economici della direttiva), dovuta alla circostanza che i contenuti digitali si interconnettono ai beni materiali.

[35] La conservazione dei dati deve essere protetta da modifiche e accessi non autorizzati. Dovrebbero essere previste procedure per valutare il rischio di conservazione centralizzata o decentrata, e le categorie di dati personali cui si applicano. Alcuni dati potrebbero richiedere misure di sicurezza supplementari rispetto ad altri o l'isolamento da questi ultimi; i dati personali e i *backup*/registri di eventi dovrebbero essere pseudonimizzati come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni dei dati, ad esempio utilizzando l'*hashing* o la cifratura; conservare *backup* e registri di eventi nella misura necessaria per la sicurezza delle informazioni, utilizzare registri delle attività (*audit trails*) e il monitoraggio degli eventi come controlli di sicurezza su base routinaria, proteggendoli da modifiche e accessi non autorizzati e accidentali e rivedendoli periodicamente, oltre a gestire in modo tempestivo eventuali incidenti; soddisfare i requisiti per il ripristino del sistema informativo in caso di disastro e per la continuità operativa, al fine di ripristinare la disponibilità dei dati personali a seguito di incidenti rilevanti; tutte le categorie di dati personali dovrebbero essere protette con misure adeguate contro il rischio di violazioni della sicurezza. I dati che comportano rischi particolari dovrebbero, ove possibile, essere tenuti separati dagli altri dati personali; occorre disporre di metodologie, procedure e risorse per rilevare, limitare, gestire e segnalare le violazioni dei dati e trarne insegnamenti; al fine di rendere più solido il sistema di trattamento, il titolare deve disporre di procedure per gestire violazioni e incidenti, ivi comprese procedure di notifica quali la gestione delle notifiche (per l'autorità di controllo) e delle informazioni (per gli interessati).

meglio consenta di assicurare il duplice obiettivo della conformità alla legge e della tutela degli interessati, attivamente privando le informazioni personali, fino al punto in cui è possibile, del loro potere identificativo.

Ai sensi dell'art. 5, par. 1, lett. *c)*, dunque, un'informazione personale non strettamente necessaria rispetto al fine perseguito dal trattamento non potrà certamente essere utilizzata; ma è altrettanto vero che, sempre alla stregua di tale norma, i dati che, invece, risulteranno funzionali al trattamento dovranno essere impiegati, in tutte le diverse operazioni che quel trattamento prevede, nella modalità meno identificativa possibile. Ci si dovrà avvalere, quindi, delle tecniche che consentano di affievolire progressivamente il potere identificativo delle informazioni personali[36]. Decidere se l'adozione di una metodologia di *privacy by design* si risolva in una tecnica di minimizzazione (che comporta ancora un trattamento di dati personali), ovvero di anonimizzazione è scelta non tanto di carattere tecnico, ma piuttosto fondata su un'analisi di tipo costi-benefici. In altri termini, in base all'interesse concretamente perseguito, il titolare che otterrà benefici dal trattamento di dati personali dovrà anche farsi carico dei rischi che vi sono connessi, specie in un quadro di riuso del dato classico dell'attuale contesto di *big data*, *internet of things* (IoT) e intelligenza artificiale (AI). In questa prospettiva, il titolare dovrà allora integrare nel trattamento medesimo il livello appropriato di salvaguardie: fino, se del caso, a quella estrema, che è costituita appunto dall'anonimizzazione. Con l'avvertenza, tuttavia, che, in tal caso, qualora l'adozione di una tecnica di anonimizzazione non sufficientemente

[36] Da un punto di vista pratico, la minimizzazione dei dati può essere ottenuta attraverso l'applicazione di tecniche diverse, le quali possono essere sostanzialmente raggruppate in due grandi famiglie. Innanzitutto, va citata la randomizzazione, che modifica il grado di veridicità del dato allo scopo di ridurre la correlazione sussistente tra dati e individui. Le tecniche che rientrano in questa categoria sono la permutazione, l'aggiunta di rumore statistico e la *privacy* differenziale. La seconda grande famiglia è poi costituita dalla generalizzazione, la quale consiste nel diluire gli attributi dell'interessato modificandone le rispettive scale o ordini di grandezza. Si consideri, ad esempio, l'indicazione di un intervallo di età in luogo dell'età precisa, o la regione al posto della città in cui vive la persona, e così via. Aggiungere elementi di incertezza ai dati, sia per il tramite della randomizzazione, sia per mezzo della generalizzazione, è procedimento che, se condotto alle estreme conseguenze, può consentire di pervenire all'anonimizzazione del dato, trattamento cioè che, a meno di uno sforzo irragionevole, ha l'obiettivo di precludere l'identificazione dell'interessato. Pur non trovando un'espressa definizione nel regolamento, i dati anonimizzati sono sottratti, ai sensi del *considerando* n. 26, all'applicabilità della disciplina di protezione dei dati. La menzionata inidoneità del dato anonimizzato quale mezzo per pervenire all'identificazione dell'interessato va valutata in relazione ai mezzi nella disponibilità di chi (il titolare medesimo ovvero un terzo) provi ad utilizzare quelle informazioni per identificare la persona. Tali mezzi, seguendo le indicazioni del *considerando*, possono dunque essere distinti in mezzi "ragionevolmente utilizzabili" e "irragionevolmente utilizzabili". In tal modo, se disponendo del dato anonimizzato e soltanto con l'ausilio di mezzi "irragionevolmente utilizzabili" sarà possibile identificare la persona, il trattamento di dati anonimizzati non rientrerà nell'ambito di applicazione della direttiva. Il *considerando* n. 26 GDPR afferma pure che «per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici».

efficace esponesse i dati al rischio della re-identificazione, il titolare, nuovamente soggetto alle norme del regolamento, sarebbe responsabile di aver effettuato un trattamento illecito, con ogni riflesso anche in termini di sanzioni applicabili.

L'art. 25 cita pure la tecnica della «pseudonimizzazione», che consiste nell'insieme delle operazioni di trattamento idonee ad evitare che i dati personali possano «essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile»[37]. Utili, in fase progettuale, sono anche i c.d. «*privacy design patterns*» (o «*privacy pattern*s»), ossia delle porzioni modulari di «codice» con cui i programmatori o gli sviluppatori realizzano – e mettono a disposizione di tutti per un successivo riutilizzo – determinate funzioni volte ad assicurare, in maniera strutturale, il rispetto della protezione dei dati personali, evitando che il codice debba essere riscritto ogni volta da capo in fase di progettazione del *software*[38].

[37] L'esemplificazione proposta dal legislatore europeo non ha carattere esaustivo e lo si deduce anche dalla lettura del *considerando* n. 28, ai sensi del quale «l'introduzione esplicita della pseudonimizzazione nel presente regolamento non è (…) intesa a precludere altre misure di protezione dei dati». Non sempre la pseudonimizzazione può essere sufficiente, o anche solo necessaria, per dimostrare la conformità al principio dell'art. 25 del GDPR. La natura delle misure tecniche e organizzative da adottare per garantire la conformità al principio di protezione dei dati fin dalla progettazione dovrà essere determinata in base al contesto specifico e seguendo un approccio basato sull'identificazione (e conseguente mitigazione) dei rischi per le persone interessate. Ad esempio, la profilazione di dati relativi alla salute di persone vulnerabili (si pensi ai bambini) richiede certamente cautele maggiori rispetto ad un mero elenco di clienti di una carrozzeria. Cfr., in tal senso, G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.,* 2017, 1, p. 1 *(commento alla normativa).* Una compiuta illustrazione del concetto, anche con riferimento alle rispettive origini concettuali, è offerta da A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy*:* privacy by design *e* privacy by default settings, cit., p. 197 ss., ove si trovano ulteriori riferimenti sul punto. Vedi inoltre R. D'ORAZIO, *Protezione dei dati by default e by design*, in AA.VV., *La nuova disciplina*, cit., p. 79 ss. Tra le tecniche di pseudonimizzazione maggiormente utilizzate possono menzionarsi il ricorso alla crittografia con chiave segreta, che prevede che si possa risalire all'identificazione di ogni persona interessata decrittando l'insieme di dati, purché ci sia conoscenza della chiave; l'impiego di una funzione di *hash*, la *tokenizzazione*, ecc. Si tratta tuttavia in ogni caso di tecniche che non precludono l'individuazione della persona, in quanto le relative informazioni personali sono ancora identificate da un attributo unico che è il risultato della funzione di pseudonimizzazione (l'attributo pseudonimizzato). L'esperienza ha mostrato come, in molti casi, identificare una persona all'interno di un insieme di dati pseudonimizzato può essere facile, a volte addirittura più che per il tramite dei dati originali o delle informazioni anagrafiche. Se infatti il nominativo di una persona è sostituito da un codice (ad esempio una stringa o un *QR code*), esso potrà forse non essere immediatamente intellegibile per un essere umano, ma potrebbe esserlo – con maggior facilità e minori rischi di fraintendimenti – per un apparato o un dispositivo elettronico.

[38] Cfr., in argomento, F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 795 ss. e, ivi, spec. p. 800, laddove precisa che il ricorso a *privacy patterns* predeterminati, così come lo sviluppo di nuovi *privacy patterns*, dispiega tutta la propria efficacia grazie alla replicabilità di «metodologie» e «modelli» adattabili, in fase di progettazione, ai diversi sistemi utilizzati per il trattamento dei dati personali. I *privacy patterns* rientrano dunque tra le modalità di realizzazione di quella che è stata definita come «*privacy by design*» (o «*data protection by design*»),

2.2. Le impostazioni di controllo dei dati oggetto del trattamento (*privacy by default*) e il consenso consapevole dell'interessato

Accanto alla «protezione dei dati fin dalla progettazione» (*data protection by design*), il legislatore europeo s'è premurato di normare anche la c.d. «protezione per impostazione predefinita» (*data protection by default*). Questo concetto, delineato dall'art. 25, par. 2, del Regolamento 2016/679, focalizza la propria attenzione esclusivamente sulle impostazioni di controllo dei dati oggetto di trattamento, richiedendo che gli stessi vengano in qualche modo «filtrati» per l'intero ciclo di vita del trattamento, sin dalla fase della loro acquisizione, mediante accorgimenti tecnici e organizzativo-procedurali[39].

Si tratta di una tecnica di protezione complementare alla prima, basata sempre sull'utilizzo di procedure e tecnologie funzionali alla tutela della *privacy*, con ricorso a strategie orientate «ai dati»: non si richiede di intervenire qui sulla «struttura» del *software*, del dispositivo o del sistema informatico, né di utilizzare in fase di programmazione (o sviluppare *ex novo*) «*design patterns*» dedicati alla protezione dei dati; si richiede invece di intervenire operando un «controllo» sul trattamento dei dati personali, sia in fase di acquisizione che in fase di loro successiva rielaborazione. In particolare, le tecnologie ideate in fase di progettazione per la tutela della *privacy* – presenti, dunque, sul sistema informatico in ossequio all'obbligo di cui all'art. 25, par. 1, Reg. 2016/679 – devono essere poi «impostate» di *default* per limitare il trattamento ai soli dati necessari per raggiungere le finalità del trattamento[40]. Si tratta, in

facendo parte del più complesso genere di tecnologie con cui ci si propone di realizzare o rafforzare le esigenze di protezione dei dati personali.

[39] Come rimarcato da A. Principato, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, cit., pp. 202 e 203, l'«utilità dei *default settings* si fonda sull'idea che al momento di effettuare una scelta, ove un'impostazione sia già preselezionata, i soggetti tendono a restare sugli stessi *default settings*, pur avendo possibilità di cambiarli e pur avendo opzioni migliori "a portata di mano", a causa di un'inerzia riconducibile a svariati fattori. Emerge come, in definitiva, le impostazioni di default siano strumentali a condizionare il comportamento dei soggetti, e come abbiano notevole influenza sulle loro scelte. Da ciò discende come il modo in cui si impostano i *default settings* sia determinante, vista la possibilità di "pilotare" le scelte degli utenti. In genere, la mancata consapevolezza di quanto si condivide, che comporta spesso quasi un cieco affidamento alle impostazioni predeterminate, implica la necessità di tutelare la riservatezza dei dati personali oltre che dall'inizio anche in modo automatico».

[40] Cfr., in tal senso, F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 802 ss., che, inoltre, sottolinea che tale forma di protezione non è in realtà innovativa. Infatti, nel codice in materia di protezione dei dati personali, nel testo precedente alla riforma del 2018, se ne riscontrava una chiara enunciazione. All'art. 3 (ora abrogato) del d.lgs. n. 196/2003, infatti, si prevedeva testualmente che «i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità». Significativo era il riferimento alla «configurazione» (*setting*) dei sistemi e dei programmi utilizzati per il trattamento e l'approccio «ai dati» (richiedendosi che venisse minimizzato l'utilizzo dei dati personali e identificativi, escludendo che il loro trattamento avvenisse là dove le finalità potessero essere raggiunte ugualmente con dati anonimi o pseudonimizzati). La presa d'atto della pervasività delle tecnologie e dei rischi ad essa connessi non ha portato, invece, nell'art. 3 Codice

altre parole, della *summa* dei principi di "minimizzazione dei dati" e di "limitazione della finalità", da cui discende a sua volta il principio della "limitazione della conservazione", il quale impone di limitare nel tempo quanto più possibile il trattamento e l'archiviazione dei dati raccolti.

Il principio di *privacy by default* prevede, appunto, che per impostazione predefinita i titolari debbano trattare i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento garantendo la non eccessività dei dati raccolti, in modo che l'interessato riceva un alto livello di protezione anche se non si attiva per limitare la raccolta dei dati (es. tramite *opt out*). In definitiva, è ancora una volta il rispetto del principio di minimizzazione a costituire una modalità di trattamento *by default*, idonea a impostare *ex ante* la massima protezione dei dati possibile attraverso il loro trattamento minimo, tanto nella fase di raccolta quanto in quelle successive. L'utilizzo di informazioni per l'accesso ad un servizio o prodotto dovrà pertanto essere inizialmente limitato al minimo indispensabile per consentirne la fruizione, di modo che sia rimesso interamente all'interessato un effettivo, concreto potere di scelta in ordine alla possibilità di consentire o meno un utilizzo eventualmente più ampio dei suoi dati. Non più, dunque, impostazioni che prevedano vincoli, indebite forzature, imposizioni. Questa idea di tutela riguarda, infine, anche l'accessibilità dei dati dell'interessato. A tal proposito, infatti, il par. 2 dell'art. 25 obbliga i titolari all'adozione di misure che garantiscano che, di *default* appunto, essi non siano diffusi, e cioè resi accessibili a un numero indefinito di persone in assenza di una specifica decisione dell'interessato che gli consenta pertanto di controllarne la distribuzione[41].

In definitiva, i principi di *privacy by design* e *by default* differiscono per diversi aspetti. Il primo interessa un numero più ampio di misure di protezione dei dati ed è maggiormente riconducibile all'identificazione ed implementazione di un insieme di garanzie "di sistema", attinenti al processo ed integrate in esso; il secondo è orientato al conseguimento del risultato che i dati oggetto di trattamento siano,

privacy (nel testo vigente prima della riforma avutasi con il d.lgs. 101/2018), a quel capovolgimento di prospettiva registratosi con la *privacy by design*: si richiedeva infatti che il trattamento avvenisse riducendo al minimo l'utilizzo dei dati, intervenendo non «a monte» sull'architettura stessa delle tecnologie (cioè nella fase di *design*, al momento della progettazione), ma dopo che la stessa fosse stata già progettata, configurandone le impostazioni in modo da minimizzare l'utilizzo di dati personali e quelli identificativi (*default setting*). Inoltre, a differenza dell'art. 25 del Reg. UE 2016/679 (la cui violazione è espressamente collegata alla previsione di una sanzione amministrativa pecuniaria pari, nel massimo edittale, a dieci milioni di euro o, per le imprese, al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore), l'art. 3 del d.lgs. n. 196/2003, ora abrogato, non era norma direttamente provvista di sanzione, anche se concorreva a determinare il confine di liceità del trattamento, con conseguenze sui diversi rimedi applicabili.

[41] Precisano le linee guida EDPB n. 4/2019 (par. 2.2.2.4) che rendere disponibili i dati personali a un numero indefinito di persone potrebbe comportare una divulgazione dei dati ancora più ampia rispetto a quella inizialmente prevista, il che è particolarmente pertinente nel contesto di internet e dei motori di ricerca; perciò i titolari dovrebbero, per impostazione predefinita, dare agli interessati l'opportunità di intervenire prima che i dati personali vengano messi a disposizione pubblicamente su internet. Questo aspetto è particolarmente importante nel caso di minori e gruppi vulnerabili.

quantomeno nella loro fase iniziale, soltanto quelli essenziali, da conservarsi in modo da non essere liberamente accessibili, e dunque mantenuti confidenziali. È appena il caso di notare allora che la *privacy by default*, tutelando e rafforzando l'atto volitivo che compete all'interessato in ordine al trattamento delle proprie informazioni personali, è uno degli strumenti idonei a conferire maggiore rilievo al consenso quale presupposto di liceità del trattamento. Se si pongono a confronto infatti la definizione che del consenso offre, all'art. 2, lett. *h)*, la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati («qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento»), con quella contenuta al GDPR, par. 4, n. 11 («qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento»), si osserva che la seconda non è meramente riproduttiva della prima, poiché contiene, tra l'altro, una più marcata sottolineatura della caratteristica di inequivocabilità di cui il consenso dovrà essere, ora, dotato. Se ne deduce che l'eventuale scelta dell'interessato tesa alla consapevole modifica delle impostazioni di base dei sistemi per consentire l'utilizzo dei propri dati anche in misura ulteriore rispetto a quella minima indispensabile per la fruizione del bene o servizio – come la *privacy by default* richiede – è, in questa prospettiva, un elemento che rende più concreto l'ulteriore attributo del consenso contenuto nel regolamento. In termini più generali, può dunque affermarsi che il diritto dell'interessato ad una selezione preliminare dei dati da sottoporre a trattamento, valorizzando la scelta, favorisce una manifestazione del consenso meno *routinaria* e più consapevole[42].

2.3. L'integrazione contenutistica dei principi di cui all'art. 25 GDPR ad opera delle Linee Guida n. 4/2019 dell'*European Data Protection Board* (EDPB)

Il Regolamento 2016/679, per disciplinare la protezione dei dati personali, ha disegnato regole compatibili con le varie possibilità tecnologiche, anche non prevedibili al momento dell'entrata in vigore della norma, onde evitare che l'obsolescenza propria del settore tecnologico potesse investire anche le norme chiamate a disciplinarlo[43]. D'altro canto, la dottrina ha mostrato profonda preoccupazione per l'ec-

[42] In tal senso, in maniera del tutto condivisibile, vedi F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 814 ss.

[43] Cfr. D. Farace, *Privacy by design e privacy by default*, in E. Tosi (a cura di), *Privacy Digitale*, Milano, 2019, p. 495. Per G. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in G. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 122, "*privacy by design*" è un concetto aperto destinato ad essere attuato in modo dinamico.

cessiva genericità della norma in questione[44], soprattutto se rapportata alla diversa soluzione contenuta nella «Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati»[45].

[44] Alcuni commentatori hanno criticato l'art. 25, lamentando – anche con l'ausilio di *case studies* – le difficoltà interpretative riguardanti il concreto adempimento degli obblighi che la norma impone. Secondo A.E. WALDMAN, *Data Protection by Design? A Critique of Article 25 of the GDPR* (January 25, 2021), in *Cornell International Law Journal*, Vol. 53, 2021, Northeastern University School of Law Research Paper No. 411-2021, disponibile all'indirizzo: https://ssrn.com/abstract=3773143, «*although privacy by design is not a new doctrine, having been the subject of academic debate, legal, and regulatory discussions for more than a decade, the final draft of Article 25(1) reflects little, if any, of that history. Relying on multiple forms of statutory interpretation commonly used to interpret European Community legislation, this Article argues that Article 25 of the GDPR lacks any meaningful connection to privacy by design under textualist, contextual, purposive, and precedential interpretations. Only teleological reasoning offers a meaningful way forward. This means that it is up to the European Court of Justice to determine if Article 25(1) will have any chance of protecting European Union citizens and limiting the power of data controllers. Article 25 is hopelessly vague. Neither the text nor its context offers any clarity about Article 25's requirements, scope, or limitations. Only a teleological approach can rescue Article 25 from obscurity and obsolescence. Only a teleological approach, which gives the CJEU vast interpretive leeway, can rescue the provision. As it is today, Article 25(1) is so vague that it cannot inform corporate behavior. vague mandates leave extraordinary interpretive latitude to regulated entities on the ground, many of whom would seek to minimize their obligations rather than take on pro-consumer responsibilities. Only a robust teleological interpretation can rescue Article 25(1) from its purgatory*». Vedi anche I. RUBINSTEIN-N. GOOD, *The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default* (September 30, 2019). *International Data Privacy Law* (2020) doi: 10.1093/idpl/ipz019, consultabile in https://ssrn.com/abstract=3773333, secondo cui «*article 25 as drafted has multiple shortcomings. It overlaps with several "accountability" provisions in confusing ways; fails to define its scope; offers very few examples of relevant technical and organisational measures other than pseudonymisation, which is a poor choice; is written in vague and abstract language; and— probably in the name of technological neutrality—avoids any mention of specific privacy engineering methodologies, tools, or techniques, which only heightens the confusion over what the provision means or requires. Article 25 as presently conceived is poorly aligned with privacy engineering methods and related privacy-enhancing technologies (PETs). This is especially true of "hard" PETs that place limited trust in third parties (including data controllers) and instead rely on cryptographic techniques to achieve data minimisation. In order to advance data protection in its own right rather than merely reinforce the general principles of the GDPR, Article 25 must be interpreted as requiring the implementation of privacy engineering and hard PETs. A bold way to achieve this is by mandating that data controllers use available hard PETs for data minimisation. More gradual steps include data protection regulators insisting on a central role for privacy engineering and PETs in public sector projects; issuing guidance on Article 25 in very forceful terms that clearly require the implementation of "state of the art" privacy technology; and using their enforcement powers to reward good examples of privacy engineering rather than to penalize failures*».

[45] All'art. 23 di tale proposta – corrispondente all'attuale art. 25 del Reg. UE 2016/679 –, erano previsti, infatti, due paragrafi espunti nel testo definitivo, all'interno dei quali, dopo le prescrizioni volte a garantire gli obblighi di *privacy by design* e *by default* (art. 23, parr. 1 e 2, prop. cit.), era stato contemplato il conferimento alla Commissione del «potere di adottare atti delegati al fine di precisare i criteri e i requisiti riguardanti la protezione dei dati fin dalla progettazione applicabili in materia trasversale a vari settori, prodotti e servizi» (art. 23, par. 3, prop. cit.), nonché dell'ulteriore potere di «stabilire norme tecniche riguardanti i requisiti di cui ai paragrafi 1 e 2» (art. 23, par. 4, prop. cit.). La retromarcia del legislatore europeo, ben colta dalla dottrina estera che si è occupata del tema, è stata giustificata per via della difficoltà a legittimare, ai sensi dell'art. 290(1) TFUE, i poteri delegati

Si è potuto comprensibilmente ritenere che il dettato normativo rendesse il precetto concretamente inattuabile in tutte le sue possibili applicazioni, se non addirittura evanescente. La traduzione della norma in un «codice» informatico (e, prima ancora, in un algoritmo), poi, diventa estremamente complicata, se non concretamente inattuabile, essendo molteplici e tra loro diversificate le modalità con cui è possibile interpretare e dare concreta attuazione alle previsioni dell'attuale art. 25 del Reg. 2016/679. La soluzione che si è prospettata, così stando le cose, è stata quella di un intervento dell'autorità di controllo attraverso propri provvedimenti, non solo a seguito di ricorso o di ispezione *ex officio*, ma anche in occasione della consultazione preventiva (*ex* art. 36, Reg. 2016/679) o di emanazione di provvedimenti di carattere generale, ove ammessi. A queste istanze e alle menzionate critiche, anche con il dichiarato intento di fornire orientamenti utili ai titolari del trattamento, ha dato risposta l'*European Data Protection Board* (EDPB), attraverso la predisposizione di specifiche Linee Guida 4/2019, le quali, a seguito di consultazione pubblica, sono state adottate nella versione definitiva in data 20 ottobre 2020. L'EDPB, esaminati nel dettaglio i singoli aspetti che devono costituire oggetto di attenta valutazione da parte del titolare (lo stato dell'arte, i costi di attuazione, la natura, l'ambito di applicazione, il contesto e la finalità del trattamento, i suoi rischi, il tempo dell'adempimento), ha delineato uno scenario metodologico che, in termini concreti, va rapportato a quei principi di protezione dei dati, enunciati all'art. 5 GDPR, il cui rispetto è obbligo ineludibile del titolare. Per ciascuno di quei principi, le Linee guida identificano, anche attraverso l'indicazione di esempi pratici, gli elementi chiave della *privacy by design* e *by default*. Così, per quanto riguarda il principio della trasparenza, tra gli elementi chiave della progettazione e dell'impostazione predefinita vengono annoverati la semantica, intendendo con essa che la comunicazione deve avere un significato chiaro per i soggetti cui è rivolta; la pertinenza, cioè la rilevanza dell'informazione per il caso specifico; l'approccio multilivello e multicanale, atto ad incrementare le probabilità di conseguire una reale consapevolezza dell'interessato in ordine al trattamento dei propri dati personali, attraverso mezzi di comunicazione diversi[46].

alla Commissione, ammessi solamente per atti «non legislativi» di portata generale, che integrano o modificano determinati elementi «non essenziali» di un atto legislativo, delimitando esplicitamente obiettivi, contenuto, durata, portata e condizioni della delega (Cfr. B.J. Koops, R.E. Leenes, *Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law*, in *International Review of Law Computers & Technology*, 2013, pp. 2 ss.).

[46] Le Linee Guida EDPB n. 4/2019 chiariscono che il titolare deve essere chiaro e trasparente con l'interessato in ordine alla fase di raccolta, utilizzo e condivisione dei dati personali. Trasparenza significa consentire agli interessati di comprendere e, se necessario, avvalersi dei propri diritti come fissati negli articoli da 15 a 22. Il principio trova fondamento negli articoli 12, 13, 14 e 34. Gli elementi chiave della progettazione e dell'impostazione predefinita per quanto riguarda il principio della trasparenza possono includere: *a)* chiarezza – le informazioni sono fornite in un linguaggio chiaro e semplice, conciso e comprensibile; *b)* semantica – la comunicazione deve avere un significato chiaro per il pubblico a cui è rivolta; *c)* accessibilità – le informazioni sono facilmente accessibili per l'interessato; *d)* contestualità – le informazioni devono essere fornite al momento opportuno e nella forma adeguata; *e)* pertinenza – le informazioni devono essere pertinenti e applicabili all'interessato specifico; *f)* progettazione universale – le informazioni sono accessibili a tutti gli interessati, compreso l'utilizzo di linguaggi leggibili da una macchina per agevolare e automatizzare la leggibilità e la chiarezza; *g)* comprensibilità – gli interessati devono avere una buona comprensione di ciò che

Con riferimento al principio di liceità, le Linee Guida enumerano, tra gli altri, gli elementi del bilanciamento degli interessi, cioè, nel caso in cui il trattamento si fondi sulla base giuridica del legittimo interesse, è necessaria una ponderazione tra tutti quelli in gioco, con particolare attenzione alla necessità di ridurre gli squilibri e attenuare l'impatto negativo sulle persone; l'autonomia dell'interessato, che si riferisce al potere di controllo esercitabile sulle proprie informazioni personali; la pertinenza, inerente la necessità che al trattamento sia applicata la base giuridica corretta[47]. In relazione al principio di correttezza, sono invece annoverati la libertà di scelta dell'interessato, per contrastare forme di *lock-in* indebito; la non discriminazione, che presuppone un trattamento non ingiustamente diversificato tra interessati;

possono aspettarsi dal trattamento dei loro dati personali, in particolare quando si tratti di minori o di soggetti appartenenti ad altre categorie vulnerabili; *h)* multicanalità – le informazioni dovrebbero essere fornite attraverso canali e mezzi di comunicazione diversi, non solo quelli testuali, per aumentare la probabilità che raggiungano efficacemente l'interessato; *i)* approccio multilivello – le informazioni devono essere fornite in modo da garantire un equilibrio tra completezza e comprensibilità, rispecchiando le ragionevoli aspettative degli interessati. Esempio: la politica sulla *privacy* di un sito *web* non deve contenere una quantità eccessiva di informazioni di difficile comprensione per l'interessato medio, deve essere scritta in un linguaggio chiaro e conciso e consentire all'utente del sito di comprendere le modalità di trattamento dei suoi dati personali. Il titolare fornisce pertanto informazioni secondo un approccio multilivello, evidenziando i punti più importanti. Vengono rese facilmente accessibili informazioni più dettagliate e sono messi a disposizione menu a discesa e collegamenti ad altre pagine per spiegare ulteriormente i vari punti e i concetti contenuti nella politica. Il titolare fa anche in modo che le informazioni siano fornite con più canali, prevedendo video che illustrano i punti più importanti delle informazioni in forma testuale.

[47] Le Linee Guida EDPB n. 4/2019, nel ribadire che il titolare deve identificare una base giuridica valida per il trattamento dei dati personali, precisa che le misure e le garanzie dovrebbero concorrere all'obbligo di assicurare che l'intero ciclo di vita del trattamento sia in linea con la pertinente base giuridica. Tra gli elementi principali della progettazione e dell'impostazione predefinita ai fini della liceità possono figurare: *a)* pertinenza –al trattamento è applicata la corretta base giuridica; *b)* differenziazione – occorre differenziare la base giuridica utilizzata per ciascuna attività di trattamento; *c)* finalità specifica – la corretta base giuridica deve essere chiaramente connessa alla specifica finalità di trattamento; *d)* necessità – il trattamento deve essere necessario e non soggetto a condizioni affinché la sua finalità sia lecita; *e)* autonomia – all'interessato dovrebbe essere garantito il massimo grado possibile di autonomia in relazione al controllo dei propri dati personali nel quadro della base giuridica; *f)* ottenimento del consenso – il consenso deve essere liberamente espresso, specifico, informato e inequivocabile. Occorre considerare, in particolare, la capacità dei minori di fornire un consenso informato; *g)* revoca del consenso – se il consenso è la base giuridica, il trattamento dovrebbe agevolarne la revoca. La revoca del consenso deve essere altrettanto facile quanto la sua prestazione. In caso contrario, il meccanismo del consenso attuato dal titolare non è conforme al GDPR; *h)* bilanciamento degli interessi – se la base giuridica è costituita da interessi legittimi, il titolare deve effettuare un bilanciamento ponderato, considerando in particolare lo squilibrio tra i rapporti di forza, specificamente nel caso di minori e altri gruppi vulnerabili. Devono essere previste misure e garanzie per attenuare l'impatto negativo sugli interessati; *i)* predeterminazione – la base giuridica è stabilita prima che il trattamento abbia luogo; *l)* cessazione – se la base giuridica non è più valida, il trattamento cessa di conseguenza; *m)* adeguamento – se vi è una modifica valida della base giuridica per il trattamento, quest'ultimo deve essere adeguato in base alla nuova base giuridica; *n)* attribuzione di responsabilità – ogniqualvolta sia prevista la contitolarità del trattamento, le parti devono suddividersi in modo chiaro e trasparente le rispettive responsabilità nei confronti dell'interessato ed elaborare le misure del trattamento conformemente a tale attribuzione di responsabilità.

l'eticità, che si concreta nella considerazione dell'impatto complessivo del trattamento sugli aspetti relativi ai diritti e soprattutto alla dignità delle persone[48].

Appartengono, invece, al principio della limitazione della finalità, tra gli altri, gli elementi della compatibilità, che deve caratterizzare le eventuali finalità successive a quella originaria al fine di orientare le modifiche rilevanti nella progettazione; la predeterminazione, cioè la necessità che le finalità siano individuate prima della progettazione del trattamento; il riesame periodico, necessario per valutare se, nel corso del trattamento, i dati che ne costituiscono oggetto permangono indispensabili per il conseguimento dello scopo che ci si è prefissi[49]. Quanto al principio di minimizza-

[48] Le Linee guida EDPB n. 4/2019 precisano che la correttezza è un principio di natura trasversale, secondo cui i dati personali non devono essere trattati in modo ingiustificatamente dannoso, illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato. Le misure e le garanzie che attuano il principio della correttezza supportano anche i diritti e le libertà degli interessati, in particolare il diritto all'informazione (trasparenza), il diritto di intervenire nel trattamento (accesso, cancellazione, portabilità dei dati, rettificazione) e il diritto di limitazione del trattamento (il diritto a non essere sottoposto a un processo decisionale automatizzato e non subire discriminazioni nel contesto di tali processi). Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla correttezza, possono figurare: *a)* autonomia – agli interessati dovrebbe essere garantito il massimo grado possibile di autonomia nel determinare l'utilizzo cui sono sottoposti i loro dati personali, nonché l'ambito di applicazione e le condizioni di tale utilizzo o trattamento; *b)* interazione – gli interessati devono essere in grado di comunicare ed esercitare i propri diritti in relazione ai dati personali trattati dal titolare; *c)* aspettativa – il trattamento dovrebbe corrispondere alle aspettative ragionevoli degli interessati; *d)* nessuna discriminazione – il titolare non discrimina ingiustamente gli interessati; *e)* nessuno sfruttamento – il titolare non deve sfruttare le esigenze o le vulnerabilità degli interessati; *f)* libertà di scelta – il titolare non dovrebbe «catturare» (*lock-in*) i propri utenti in modo scorretto. Qualora un servizio che prevede il trattamento di dati personali abbia natura proprietaria, gli utenti potrebbero essere "catturati" rispetto a tale servizio, il che può essere scorretto qualora pregiudichi la possibilità per gli interessati di esercitare il diritto alla portabilità dei dati ai sensi dell'articolo; *g)* equilibrio dei rapporti di forza – tale equilibrio dovrebbe essere un obiettivo chiave della relazione tra titolare e interessato. Occorre evitare gli squilibri nei rapporti di forza e, qualora ciò non sia possibile, è necessario individuarli e tenerne conto al fine di adottare adeguate contromisure; *h)* assenza di trasferimento di rischi – i titolari non dovrebbero trasferire i rischi di impresa agli interessati; *i)* assenza di prassi ingannevoli – le informazioni e le opzioni relative al trattamento dei dati devono essere fornite in modo obiettivo e neutrale, evitando formulazioni o meccanismi ingannevoli o manipolatori; *l)* rispetto dei diritti – il titolare deve rispettare i diritti fondamentali degli interessati e attuare misure e garanzie adeguate, senza comprimere tali diritti se non ove ciò sia espressamente giustificato dalla legge; *m)* eticità – il titolare dovrebbe guardare all'impatto complessivo del trattamento sui diritti e sulla dignità delle persone; *n)* veridicità – il titolare deve dichiarare le proprie modalità di trattamento dei dati personali e deve agire secondo quanto dichiarato in merito, senza fuorviare gli interessati; intervento umano – il titolare deve integrare un intervento umano qualificato in grado di individuare le distorsioni (*bias*) che le macchine possono generare, conformemente al diritto di non essere sottoposto a un processo decisionale automatizzato di cui all'art. 2232; *o)* imparzialità degli algoritmi – valutare periodicamente se gli algoritmi funzionino in linea con le finalità e adeguarli per attenuare le distorsioni individuate e garantire l'imparzialità del trattamento. Gli interessati dovrebbero essere informati in merito al trattamento dei dati personali attraverso algoritmi che ne facciano oggetto di analisi o previsioni, per esempio riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti.

[49] Per le Linee Guida EDPB n. 4/2019, il titolare deve raccogliere dati per finalità specifiche, esplicite e legittime e non trattarli ulteriormente in modo incompatibile con le finalità per le quali sono stati raccolti. La progettazione del trattamento dovrebbe pertanto essere definita da quanto necessario

zione dei dati, le *Linee* Guida considerano, tra gli altri, gli elementi dell'aggregazione, che impone che i dati siano appunto aggregati ogniqualvolta ciò sia possibile; la pseudonimizzazione, esplicitamente menzionata dalla lettera dell'art. 25, e di cui si è ampiamente argomentato; il flusso dei dati, la cui efficienza consente al titolare di evitare la creazione di copie non indispensabili[50].

per conseguire le finalità. In caso di trattamento ulteriore, il titolare deve prima assicurarsi che tale trattamento abbia finalità compatibili con quelle originarie e progettarlo di conseguenza. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla limitazione delle finalità, possono figurare: *a)* predeterminazione – le finalità legittime sono determinate prima della progettazione del trattamento; *b)* specificità – le finalità sono specificate ed esplicite in merito al motivo per cui i dati personali vengono trattati; *c)* orientamento in base alla finalità – la finalità del trattamento dovrebbe orientare la progettazione del trattamento e determinarne i limiti; *d)* necessità – la finalità determina quali sono i dati personali necessari per il trattamento; *e)* compatibilità – qualsiasi nuova finalità deve essere compatibile con la finalità originaria per la quale sono stati raccolti i dati e orientare le modifiche rilevanti nella progettazione; *f)* limitazione di trattamenti ulteriori – il titolare non dovrebbe collegare set di dati o effettuare ulteriori trattamenti per finalità diverse che sono incompatibili; *g)* limitazioni del riutilizzo – il titolare dovrebbe adottare misure tecniche, tra cui l'*hashing* e la cifratura, per limitare la possibilità di riutilizzare i dati personali. Il titolare dovrebbe inoltre prevedere misure organizzative, quali politiche e obblighi contrattuali, che limitino il riutilizzo di dati personali; *h)* riesame periodico – il titolare dovrebbe verificare periodicamente se il trattamento sia necessario per le finalità per le quali sono stati raccolti i dati e testare la progettazione di tale trattamento con riguardo al principio di limitazione delle finalità.

[50] Solo i dati personali che sono adeguati, pertinenti e limitati a quanto necessario per la finalità sono sottoposti a trattamento. Di conseguenza, il titolare deve predeterminare quali caratteristiche e parametri dei sistemi di trattamento, nonché quali funzioni di supporto siano consentiti. La minimizzazione dei dati realizza e rende operativo il principio di necessità. Nel proseguire il trattamento, il titolare dovrebbe valutare periodicamente se i dati personali trattati siano ancora adeguati, pertinenti e necessari o se occorra cancellarli o renderli anonimi. I titolari dovrebbero, in primo luogo, valutare se abbiano bisogno o meno di trattare i dati personali per le finalità che interessano loro. Il titolare dovrebbe verificare se sia possibile conseguire le finalità pertinenti trattando una quantità inferiore di dati personali o disponendo di dati personali meno dettagliati o aggregati, oppure senza doverli trattare affatto. Questa verifica dovrebbe essere eseguita prima di qualunque trattamento, ma potrebbe anche aver luogo in qualsiasi momento nel corso del ciclo di vita del trattamento. La minimizzazione può anche riferirsi al grado di identificazione. Se la finalità del trattamento non richiede che i set di dati definitivi si riferiscano a una persona fisica identificata o identificabile (come nelle statistiche), ma lo richiede il trattamento iniziale (ad es. prima dell'aggregazione dei dati), il titolare cancella o rende anonimi i dati personali non appena non sia più necessaria l'identificazione. Oppure, se l'identificazione continua a essere necessaria per le altre attività di trattamento, i dati personali dovrebbero essere pseudonimizzati al fine di ridurre i rischi per i diritti degli interessati. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla minimizzazione dei dati, possono figurare: *a)* evitare il trattamento dei dati – evitare del tutto il trattamento dei dati personali quando ciò sia possibile per la finalità pertinente; *b)* limitazione – la quantità di dati personali raccolti va limitata a ciò che è necessario per la specifica finalità; *c)* limitazione dell'accesso – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per esercitare le proprie funzioni, e limitare l'accesso di conseguenza; *d)* pertinenza – i dati personali devono essere pertinenti al trattamento in questione e il titolare deve essere in grado di dimostrare tale pertinenza; *e)* necessità – ogni categoria di dati personali deve essere necessaria per le finalità specificate e dovrebbe essere trattata soltanto se non è possibile conseguire la specifica finalità con altri mezzi; *f)* aggregazione – quando possibile, utilizzare dati aggregati; *g)* pseudonimizzazione – pseudonimizzare i dati personali quando non è più necessario disporre di dati personali identificabili e memorizzare le chiavi di identificazione separatamente; *h)* anonimizzazione e cancel-

In relazione al principio di esattezza, l'EDPB menziona poi l'importanza della verifica, strumento che mira ad asseverare, anche nel tempo, la persistenza di determinati attributi della persona (ad esempio la minore età); la fonte dei dati, elemento di *compliance* per verificarne la precisione; la misurabilità dell'esattezza, che si avvale dell'eliminazione di falsi positivi e negativi, ad esempio nell'ambito delle decisioni automatizzate e dell'intelligenza artificiale[51]. In relazione al principio della limitazione della conservazione, tra gli elementi di *privacy by design* e *by default* da considerare, vengono in rilievo l'automatizzazione, cioè la modalità automatizzata di cancellazione dei dati non più necessari; la giustificazione, ossia la capacità del titolare di spiegare, dimostrandole, le ragioni delle scelte effettuate in relazione alla conservazione dei dati; il ricorso a *back up*/registri di eventi di cui siano predeterminati quali dati e quali tempi di conservazione siano strettamente necessari[52]. Da

lazione – se i dati personali non sono necessari per la specifica finalità (o non lo sono più), devono essere resi anonimi o cancellati; *i)* flusso dei dati – il flusso dei dati deve essere efficiente così da non creare copie ulteriori rispetto a quanto necessario; *l)* «stato dell'arte» – il titolare dovrebbe applicare tecnologie aggiornate e adeguate per evitare o minimizzare il trattamento dei dati.

[51] Secondo le Linee Guida EDPB n. 4/2019, i dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati. I requisiti dovrebbero essere esaminati in relazione ai rischi e alle conseguenze derivanti dall'utilizzo concreto dei dati. I dati inesatti potrebbero costituire un rischio per i diritti e le libertà degli interessati, ad esempio quando conducono a una diagnosi errata o a un trattamento errato di un protocollo sanitario, oppure un'immagine errata di una persona può portare a decisioni erronee sia attraverso processi manuali sia attraverso un processo decisionale automatizzato o l'impiego di tecniche di intelligenza artificiale. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'esattezza, possono figurare: *a)* fonte dei dati – le fonti dei dati personali dovrebbero essere affidabili in termini di esattezza dei dati; *b)* grado di esattezza – ciascun elemento dei dati personali deve essere il più esatto possibile in base alle necessità delle finalità specifiche; *c)* esattezza misurabile – occorre ridurre il numero di falsi positivi/negativi, per esempio le distorsioni generate nell'ambito delle decisioni automatizzate e dell'intelligenza artificiale; *d)* verifica – a seconda della natura dei dati, e in relazione alla frequenza delle relative modifiche, il titolare dovrebbe verificare la correttezza dei dati personali presso l'interessato prima del trattamento e nelle sue diverse fasi (per esempio rispetto ai requisiti di età); *e)* cancellazione/rettifica – il titolare dovrebbe cancellare o rettificare tempestivamente i dati inesatti e, in particolare, agevolare questa procedura se gli interessati sono o erano minori e successivamente desiderano eliminare i suddetti dati personali; *f)* evitare la propagazione di errori – i titolari dovrebbero attenuare l'effetto di un errore accumulato nella catena di trattamento; *g)* accesso – gli interessati dovrebbero ricevere informazioni sui dati personali e disporre di un accesso efficace agli stessi, ai sensi degli articoli da 12 a 15 del GDPR, per controllarne l'esattezza e apportare le rettifiche ove necessario; *h)* esattezza permanente – i dati personali dovrebbero essere esatti in tutte le fasi del trattamento e nelle fasi critiche dovrebbero essere effettuate verifiche di esattezza; *i)* aggiornamento – i dati personali sono aggiornati qualora ciò sia necessario per la specifica finalità; *l)* progettazione dei dati – impiego di caratteristiche organizzative e tecnologiche di progettazione per ridurre le eventuali inesattezze, per esempio proponendo scelte concise e predeterminate anziché campi a testo libero.

[52] Per le Linee Guida EDPB n. 4/2019, il titolare deve garantire che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario per le finalità per le quali i dati personali sono trattati. È fondamentale che il titolare sappia esattamente quali dati personali sono trattati e perché. La finalità del trattamento è il criterio principale per stabilire la durata della conservazione dei dati personali. Le misure e le garanzie che attuano il principio della limitazione della conservazione integrano i diritti e le libertà degli interes-

ultimo, per rispettare il principio di integrità e riservatezza, tra gli indici suggeriti ci sono la manutenzione di *hardware*, *software*, sistemi e servizi, con l'obiettivo di identificarne eventuali vulnerabilità; la gestione del controllo degli accessi, con differenziazione dei privilegi di accesso in modo da riservarli a specifici agenti o categorie di personale, nonché a limitati dati o categorie di dati, strettamente indispensabili per le operazioni richieste[53].

sati, in particolare il diritto alla cancellazione e il diritto di opposizione. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi alla limitazione della conservazione, possono figurare: *a)* cancellazione e anonimizzazione – il titolare dovrebbe disporre di procedure interne e di funzionalità ben definite per la cancellazione e/o l'anonimizzazione dei dati; *b)* efficacia dell'anonimizzazione/cancellazione – il titolare si assicura che non sia possibile reidentificare i dati anonimizzati o recuperare quelli cancellati e dovrebbe verificare che tali misure funzionino; *c)* automatizzazione – la cancellazione di determinati dati personali dovrebbe essere automatizzata; *d)* criteri di conservazione – il titolare deve stabilire la durata della conservazione e quali dati sono necessari per la specifica finalità; *e)* giustificazione – il titolare deve essere in grado di motivare perché il periodo di conservazione sia necessario per la finalità e per i dati personali in questione, nonché di spiegare le ragioni e i fondamenti giuridici alla base del periodo di conservazione; *f)* applicazione delle politiche di conservazione – il titolare dovrebbe far valere determinate politiche di conservazione interne e verificare se l'organizzazione le mette in pratica; *g) backup*/registri di eventi – i titolari devono stabilire quali dati personali e quale periodo di conservazione siano necessari per i *backup* e i registri di eventi; *h)* flusso di dati – i titolari dovrebbero prestare attenzione al flusso di dati personali e alla conservazione delle loro copie, cercando di limitarne la conservazione «temporanea».

[53] Secondo le Linee guida EDPB n. 4/2019, il principio di integrità e riservatezza prevede la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. La sicurezza dei dati personali richiede misure appropriate concepite per prevenire e gestire incidenti di violazione dei dati, garantire la corretta esecuzione dei compiti di trattamento dei dati e la conformità agli altri principi, nonché facilitare l'esercizio effettivo dei diritti delle persone. Il *Considerando* n. 78 stabilisce che una delle misure della *privacy by design* potrebbe consistere nel consentire al titolare «di creare e migliorare caratteristiche di sicurezza». Parallelamente alle altre misure, il *Considerando* n. 78 suggerisce ai titolari di valutare costantemente se stiano utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità esistenti. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati. Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare: *a)* sistema di gestione della sicurezza delle informazioni – occorre disporre di uno strumento operativo per gestire le politiche e le procedure per la sicurezza delle informazioni; *b)* analisi del rischio – valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti delle persone, e contrastare quelli identificati, nonché, ai fini dell'utilizzo nella valutazione dei rischi, sviluppare e gestire una «modellizzazione delle minacce» esaustiva, sistematica e realistica e un'analisi della superficie di attacco riferita al *software* specifico così da ridurre i vettori di attacco e le opportunità di sfruttare eventuali punti deboli e vulnerabilità; *c)* sicurezza fin dalla progettazione – tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti; *d)* manutenzione – rivedere e verificare periodicamente il *software*, l'*hardware*, i sistemi e i servizi, ecc. per scoprire eventuali vulnerabilità dei sistemi di supporto del trattamento; *e)* gestione del controllo degli accessi – solo il personale autorizzato che ne ha necessità dovrebbe avere accesso ai dati personali necessari ai loro compiti di trattamento. Inoltre, il titolare dovrebbe differenziare i privilegi di accesso del personale autorizzato; *f)* limitazione dell'accesso (agenti) – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie

2.4. La fonte delle obbligazioni *ex* art. 25 GDPR e la natura della responsabilità per il loro inadempimento

È evidente la volontà del legislatore europeo di introdurre, in maniera sistematica, obblighi «di sicurezza» o «di protezione», per esigenze di salvaguardia dell'interesse individuale o collettivo. Oltre agli obblighi informativi, che richiedono un comportamento attivo e valutativo del soggetto in favore del quale sono previsti, in quanto funzionali all'esercizio della sua piena e libera autodeterminazione, negli ultimi anni sono stati previsti obblighi di protezione che impongono l'adozione di misure di sicurezza tecniche e organizzative, quali quelli qui descritti concernenti la tutela dei dati personali sin dalla progettazione e per impostazione definita[54].

Certamente, l'esistenza di un obbligo giuridico di adozione delle misure di sicurezza in capo al titolare comporta una correlata «pretesa» giuridica per l'interessato, da questi direttamente azionabile a prescindere dall'esperibilità o meno del rimedio risarcitorio: in particolare, con riguardo alle disposizioni del Codice in materia di protezione dei dati personali, si è ritenuto «che, ai sensi dell'art. 7, n. 4, lett. *a)*, la mancata adozione delle idonee preventive misure di sicurezza rappresenti

funzioni, e limitare l'accesso di conseguenza; *g)* limitazione dell'accesso (contenuto) – nel contesto di ciascuna operazione di trattamento, limitare l'accesso per ogni set di dati ai soli attributi che sono necessari allo svolgimento di tale operazione. Limitare inoltre l'accesso ai dati relativi agli interessati di competenza del rispettivo dipendente; *h)* segregazione dell'accesso – definire il trattamento dei dati in modo tale che nessuno necessiti di accedere a tutti i dati raccolti sull'interessato, tanto meno a tutti i dati personali di una categoria specifica di interessati; *i)* trasferimenti sicuri – i trasferimenti sono protetti da modifiche e accessi non autorizzati e accidentali.

[54] Tali obblighi sono strettamente correlati a quelli di sicurezza enunciati dall'art. 32 GDPR (cfr., in tal senso, F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 804). Questa ultima disposizione, a differenza di quanto previsto in tema di *data protection by design* e *by default*, è applicabile non solo nei confronti del titolare ma anche del responsabile del trattamento dei dati personali. Entrambi tali soggetti sono infatti destinatari di obblighi di protezione – nei confronti degli interessati e di altri soggetti terzi – obblighi che devono essere assolti mediante la messa in atto di «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio» (art. 32, par. 1). La connessione è indicata dallo stesso legislatore europeo nella prima parte del *considerando* n. 78, ove viene rimarcato che «La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente Regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default (…)». Peraltro, la disciplina della sicurezza emerge anche in altri articoli: risalta, ad esempio, anche all'interno dell'art. 24 («*Responsabilità del trattamento*»), al cui par. 1 si prevede l'obbligo, per il titolare del trattamento, di mettere «in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento (…)», con la precisazione che tali «misure sono riesaminate e aggiornate qualora necessario», richiedendosi una gestione non statica ma dinamica della sicurezza, che ha la funzione non solo di tutelare i diritti dell'interessato (*in primis*, il diritto alla protezione dei dati personali enunciato formalmente all'art. 8, par. 1 della Carta dei diritti fondamentali dell'UE e all'art. 16, par. 1 del TFUE) ma, si noti, anche quello di garantire la *compliance* all'intero regolamento. Sul rapporto tra «sicurezza» e diritto alla «protezione» dei dati personali cfr. G. CORASANITI, *La sicurezza dei dati personali*, in F. CARDARELLI-S. SICA-V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, p. 113.

un motivo legittimo che consenta all'interessato di opporsi "al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta" e lo legittima anche all'esperimento di azioni inibitorie pur in assenza di un danno attuale»[55], e così ritengo si debba ragionare nel vigore delle nuove norme. Inoltre, il carattere di indisponibilità del diritto fondamentale che la norma tutela pare essere di ostacolo alla possibilità che l'interessato possa concordare o autorizzare standard di sicurezza inferiori rispetto a quanto previsto dalla disciplina sugli obblighi di adozione delle misure di sicurezza[56].

Nell'analizzare tale normativa, il civilista deve peraltro valutare il fatto che la medesima è dettata dal legislatore europeo mediante un Regolamento, direttamente applicabile in tutti i Paesi dell'Unione, senza necessità della mediazione dei legislatori nazionali, stante il processo di progressiva europeizzazione del nostro diritto privato. Le norme ivi presenti poggiano, quindi, sotto il profilo teorico, su categorie giuridiche e concetti non riducibili unicamente a quelli di elaborazione domestica, sicché gli istituti giuridici che si vanno a delineare risentono dell'inevitabile circolazione dei modelli maturati in seno all'esperienza giuridica degli altri Stati membri, frutto della costruzione di un *droit pluriel*[57].

---

[55] Cfr., in tal senso, V. RICCIUTO, *Le finalità del Codice*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, cit., p. 229 e F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 845 ss.

[56] Cfr. in particolare R. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv*., 1998, pp. 339 ss.; ma sul tema non v'è unanimità di vedute, registrandosi posizioni dottrinali di segno contrario, anch'esse autorevoli: cfr., ad es., V. ZENO ZENCOVICH, voce *Cosa*, in *Dig. disc. priv., sez. civ*., IV, Torino, 1990, spec. par. 13, e anche ID., *Sull'informazione come "bene" (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv*., 1999, pp. 485 ss. Sulla possibilità di utilizzazione economica degli attribuiti della personalità, anche grazie all'utilizzo delle tecnologie, alimenta le riflessioni sui confini – oggi mobili – dell'indisponibilità dei diritti, G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, *passim*, e, ivi, spec. la sez. II del cap. III, pp. 346 ss. Peraltro, in ordine all'indisponibilità delle misure di sicurezza secondo il livello adeguato, va considerato il regime sanzionatorio di cui all'art. 83, par. 4, lett. *a)* del Regolamento 2016/679, che prevede – anche in assenza di danno per l'interessato ed a prescindere da eventuali manifestazione di volontà da parte dell'interessato – sanzioni amministrative piuttosto elevate in caso di violazione degli obblighi di sicurezza, che nel massimo edittale giungono fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedete, se superiore.

[57] L'espressione «*Droit pluriel*» (ossia, letteralmente, diritto «al plurale»), è stata introdotta da André-Jean Arnaud (A.J. ARNAUD, *Pour une pensée juridique européenne*, Parigi, 1991) ed efficacemente ripresa da Alpa (G. ALPA, *Diritto privato europeo*, Milano, 2016, pp. 8 s.), per il quale, il *Droit pluriel* «si basa sul processo di integrazione dei sistemi in un ordinamento unitario e di armonizzazione delle regole. È un nuovo modo di pensare all'ordinamento giuridico a cui la cultura giuridica tradizionale si deve adattare, e tentare di creare nuovi paradigmi: la flessibilità che si raggiunge attraverso la formazione di principi generali e standard; la porosità che ammette la "interlegalità", concetto fenomenologicamente contrapposto a quello di pluralismo giuridico (...). È un "sistema" diverso da quelli costruiti a livello nazionale, proprio di un "diritto post-moderno"» e per l'interpretazione del quale deve operare la dottrina. Su questa linea direttrice, in maniera convincente, cfr. F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 389 ss., secondo il quale, il ragionamento sulla natura della responsabilità scaturente dagli obblighi previsti a carico del titolare dal GDPR deve tener conto delle peculiarità del diritto privato europeo,

L'uniformazione della disciplina giuridica in materia di protezione e libera circolazione dei dati, avutasi in tutti gli Stati membri dell'Unione europea attraverso l'emanazione del Reg. UE 2016/679, come detto, ha portato all'affermazione di specifici obblighi «di protezione» a carico di chi pone in essere attività di trattamento dei dati e a beneficio degli «interessati», senza però che si sia proceduto a qualificare normativamente la natura giuridica del rapporto sussistente tra l'uno e gli altri[58]. Ciò si riflette, in particolare, sulla qualificazione giuridica della responsabilità in sede civile per danno da trattamento di dati personali, delineata dall'art. 82 Reg. UE 2016/679.

L'assenza di una puntuale regolamentazione di aspetti rilevanti in materia di responsabilità – con riferimento, ad esempio, ai termini di prescrizione dell'azione risarcitoria ed al perimetro della risarcibilità del danno – costringe l'interprete all'operazione ermeneutica volta ad individuare, *in primis*, la fonte dell'obbligazione, per poter applicare la disciplina mancante, in caso di inadempimento della medesima[59]. Ovviamente, sotto questo profilo, *nulla quaestio* potrà esservi se tra titolare e interessato sia ravvisabile un sottostante rapporto contrattuale (si pensi al trattamento dei dati effettuato dall'avvocato nei confronti del suo cliente o dalla banca nei confronti del correntista). La difficoltà interpretativa può, invece, sorgere, nel caso in cui il titolare predisponga il trattamento dei dati personali dell'interessato, senza che vi sia alcun vincolo contrattuale, come spesso accade, ad esempio nei confronti di una pubblica amministrazione.

---

nell'incontro dialettico tra norme eurounitarie e nazionali, facendo assumere a tale responsabilità una natura, per così dire, "ancipite". Questo orientamento nasce dalla constatazione del superamento tendenziale della tradizionale distinzione tra responsabilità contrattuale e responsabilità extracontrattuale nella disciplina di fonte europea, analizzata nelle pagine di N. Lipari, *Le categorie del diritto civile*, Milano, 2013, pp. 194 ss. e, ivi, spec. pp. 197-199. il quale ha evidenziato che «(...) quel che ha condotto a rompere definitivamente lo schema classico della responsabilità è stata la disciplina di derivazione comunitaria. Nelle direttive di fonte europea, infatti, si prescinde del tutto dalla considerazione se tra il produttore e il consumatore danneggiato vi sia un rapporto obbligatorio nato da un precedente contratto. Ciò che conta è il danno e l'individuazione del soggetto che dovrà sopportarne il costo (produttore o prestatore di servizi) indipendentemente dall'individuazione di un preesistente rapporto obbligatorio». Sicché, prosegue Lipari, «non avrebbe quindi rilievo, operando sulla spunta dei vecchi schemi categoriali, evidenziare, ad esempio, che la responsabilità del produttore è prevalentemente una responsabilità di tipo extracontrattuale se poi la medesima responsabilità, con conseguente applicazione della medesima disciplina, può essere attivata anche da chi, in ipotesi, abbia acquistato direttamente dal produttore. Diversamente, assumere che la responsabilità del prestatore di servizi sia una responsabilità contrattuale perde qualsiasi rilievo classificatorio se poi la medesima azione può essere esercitata anche dal terzo estraneo che ha risentito danno». La superfluità dell'indagine sulla natura della responsabilità, però, ha come corollario che la disciplina conseguentemente applicabile sia la medesima, ma non sempre è così: il legislatore europeo, ad esempio, in tema di responsabilità per trattamento dei dati personali, non ha regolamentato in maniera puntuale i diversi aspetti applicativi (ad esempio, il regime della prescrizione), costringendo quindi l'interprete a operare ugualmente una classificazione nel diritto interno, altrimenti irrilevante, al fine di "ricostruire" la disciplina da applicare concretamente nei suoi aspetti operativi.

[58] Cfr., in tal senso, F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 790 ss.

[59] Cfr. F. Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, cit., p. 394.

Sotto il vecchio regime normativo, il dato testuale era chiaro, considerato che l'art. 15 così si esprimeva: «Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile». Ciò fece propendere, pur con qualche eccezione, per la natura extracontrattuale della responsabilità[60].

Il problema interpretativo si propone, invece, in maniera più pressante ora con riguardo alla formula contenuta nell'art. 82 del Reg. 2016/679, ai sensi del quale, in forza del par. 1, «Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile».

La previsione della «violazione del regolamento» quale condizione necessaria, ancorché non sufficiente, per integrare gli estremi della responsabilità da danno materiale e immateriale derivante da trattamento di dati personali può sembrare, sotto un certo profilo, dettata dalla necessità di tener conto delle peculiarità di ordinamenti che, come quello tedesco, richiedono nella configurazione di un fatto illecito, una necessaria tipizzazione della fattispecie[61]. Da un'altra prospettiva, pare riecheggiare

[60] Per la natura extracontrattuale della responsabilità, vedi *ex multis*, E. NAVARRETTA, sub *art. 9 (Modalità di raccolta e requisiti dei dati personali)*, in *Tutela della privacy. Commentario alla legge 675/96*, a cura di C.M. BIANCA-F. BUSNELLI, cit., p. 323 ss.; A. PINORI, *Internet e responsabilità civile per il trattamento dei dati personali*, in *Contr. e impr.*, 2007, p. 1568 ss.; F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in V. CUFFARO-V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, Torino, 1997, pp. 49 ss.; M. FRANZONI, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*, 1998, pp. 902 ss. A favore della tesi «contrattuale», basata sulla constatazione dell'esistenza di un pregresso rapporto con l'interessato e sull'esistenza di uno *status* soggettivo ben delineato dalla norma (titolare, responsabile, incaricato), si è espresso, ad esempio, C. SCOGNAMIGLIO, *Buona fede e responsabilità civile*, in *Europa e dir. priv*., 2001, p. 361, che configurava la responsabilità da illecito trattamento dei dati, quale responsabilità per violazione degli obblighi di status. Vedi però G. ALPA, *I diritti della personalità*, in G. ALPA-G. RESTA, *Le persone e la famiglia, 1. Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile*, diretto da R. SACCO, Torino, 2006, p. 107, che ha efficacemente evidenziato che, di fronte all'art. 15 del Codice in materia di protezione dei dati personali, «si può (…) distinguere tra una responsabilità di natura contrattuale, che inerisce al rapporto tra l'interessato e il titolare della banca di dati, ove tale rapporto sia intervenuto mediante consenso negoziale (ad esempio nel rapporto tra banca e cliente, nell'erogazione di servizi bancari e finanziari.); una responsabilità di tipo extracontrattuale e "oggettiva", per quanto riguarda l'interessato o i terzi, e imputata a "chiunque" (non solo al titolare o al responsabile ma anche a qualsiasi terzo)».

[61] Cfr. F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, cit., p. 394. Il riferimento è, principalmente, al par. 823 BGB, dettato in tema di *Schadensersatzpflicht* («Obbligo di risarcimento del danno») derivante da «atti illeciti», ove – ai sensi del comma 1 – il risarcimento del danno è ammesso solamente nel caso in cui vi sia stata una lesione illecita dolosa o colposa di taluni beni protetti dall'ordinamento giuridico specificamente indicati dalla disposizione in esame (vita, corpo, salute, libertà, proprietà o altro diritto altrui), oppure – stando al co. 2 – nel caso in cui il danno sia stato cagionato da «chi viola una legge che protegge l'interesse di un altro (…)». Al fine di qualificare il regime che la disposizione in esame delinea, si dovrà verificare quale significato le sarà attribuito dal legislatore nazionale e dalla giurisprudenza, precisando, tuttavia, che, nel contesto di una disciplina uniforme a livello europeo, il regime di responsabilità prescelto dal legislatore nazionale dovrà essere in linea con quello previsto dagli altri Stati membri dell'Unione europea, al fine di scongiurare il verificarsi di fenomeni di *forum shopping*

il concetto di inadempimento ad obbligazioni di fonte *lato sensu* "contrattuale"[62]. In particolare, parte della dottrina ha ritenuto di poter configurare nel caso *de quo* come obbligazione di fonte legale[63], quella che forse più propriamente può essere definita come un'obbligazione derivante dalla terza categoria delle fonti di cui all'art. 1173 c.c.[64].

---

con riferimento all'introduzione di azioni per il risarcimento derivante da responsabilità civile ai sensi dell'art. 82, par. 6, del Regolamento in esame.

62 Com'è noto, quando si fa riferimento alla natura «contrattuale» della responsabilità di cui all'art. 1218 c.c., in realtà, si utilizza una semplificazione del linguaggio giuridico, in quanto – a ben guardare – si tratta di una responsabilità diversa da quella aquiliana e che ha come presupposto la violazione di un'«obbligazione» o di un altro «obbligo» di eseguire una «prestazione» non necessariamente di fonte contrattuale (cfr. C.M. Bianca, *Diritto civile, 5, La responsabilità*, 2ª ed., Milano, 2012, p. 1, ove si precisa che «La responsabilità per inadempimento è detta contrattuale a prescindere dalla fonte contrattuale o non contrattuale dell'obbligazione inadempiuta». Nello stesso senso anche G. Visintini-L. Cabella Pisu, *L'inadempimento delle obbligazioni*, in Aa.Vv., *Trattato di diritto privato*, diretto da P. Rescigno, vol. 9, *Obbligazioni e contratti*, tomo I, Torino, 1984, p. 155, per le quali la regola generale in materia di responsabilità del debitore, contenuta nell'art. 1218 c.c., viene «preferibilmente definita "contrattuale" dalla dottrina a causa del prevalere delle obbligazioni derivanti da contratto e rappresenta il tentativo del legislatore di riassumere in una disciplina uniforme una casistica, a dire il vero, molto varia a causa della diversa natura dei contratti e dei diversi modi di inadempimento»).

63 Cfr. F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, pp. 369 ss., secondo cui, in virtù degli obblighi di condotta, minuziosamente definiti in base al principio di *accountability*, previsti in capo al titolare e, in certi frangenti, direttamente in capo al responsabile del trattamento, la relazione che si instaura tra questi e l'interessato, assume la veste di un «complesso rapporto giuridico Tali obblighi di condotta, pur essendo di natura procedimentale, e non attribuendo all'interessato una specifica utilità, precedono l'eventuale produzione del danno e «rientrano nella controversa categoria delle obbligazioni *ex lege*». Secondo F. Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, cit., p. 413, siamo qui in presenza di obbligazioni con «prestazioni dovute» chiaramente individuate dalla disciplina di settore, sicché non c'è ragione di dubitare dell'applicazione diretta dell'art. 1218 c.c., senza passare per costruzioni che, pur funzionali in altri sistemi giuridici, sono apparse artificiose nel nostro sistema (con riferimento esplicito alla teoria del contatto sociale).

64 Sulla categoria dell'obbligazione *ex lege*, si consenta il rinvio a S. Faillace, *La controversa categoria delle obbligazioni ex lege*, in P. Stanzione-D. Valentino (a cura di), *IX incontro nazionale coordinamento dei dottorati di ricerca in diritto privato*, Soveria Mannelli, 2009, p. 341 ss. Si tratta di categoria cui continua ad alludere, in modo promiscuo e confuso, la giurisprudenza e non con minori incertezze la dottrina, che denuncia singolari sfasature, giungendo non di rado a conclusioni contraddittorie. La giurisprudenza di legittimità, anche a Sezioni Unite, ha mostrato di farne uso in maniera disinvolta (sull'uso giurisprudenziale del concetto di «obbligazione *ex lege*» vedi, ad esempio, con riguardo ad una fattispecie di responsabilità dello Stato da mancata attuazione di direttive europee, Cass., 24 novembre 2020 n.26757, in *Riv. dir. internaz. priv. e proc.*, 2021, 3, p. 739; in materia di sanzioni civili conseguenti all'omesso pagamento di contributi previdenziali, vedi Cass., sez. un., 13 marzo 2015, n. 5076, in *Foro It*., 2015, 11, 3675; in materia di obbligazione avente ad oggetto l'equa riparazione per violazione del diritto ad una ragionevole durata del processo, vedi Cass. civ., sez. I, 5 settembre 2011, n. 18150, in Ced Cassazione). La dottrina è invece ben più cauta, tenendo conto della scelta operata dal legislatore italiano in materia di fonti delle obbligazioni nel passaggio dal codice civile del 1865 a quello del 1942. Peraltro, va ricordato che la legge di riforma del diritto internazionale privato n. 218 del 1995, all'art. 61, ha introdotto, tra le categorie disciplinate, le obbligazioni nascenti dalla legge, inserendo in tale ambito, a sorpresa, oltre alla gestione di affari altrui, all'arricchimento senza causa, al pagamento dell'indebito, anche «le altre obbligazioni

È, infatti, il fatto giuridico della predisposizione del trattamento di dati personali che, in forza di quanto previsto dalla disciplina in materia di protezione dei dati personali, impone al titolare del trattamento di porre in essere una serie di adempimenti per proteggere i diritti e le libertà dell'interessato[65].

L'obbligo di adozione delle misure tecniche e organizzative di cui all'art. 25 del Reg. UE 2016/679, sostanziandosi in un «dovere» previsto *ex lege* di fornire una «prestazione» rientrante in un *facere* in favore del soggetto a cui i dati personali si riferiscono, può ben rientrare nella categoria di recente censita dalla giurisprudenza [66] riguardante casi in cui, pur in assenza di un rapporto contrattuale tra le parti, può essere invocata, in caso di inadempimento, la tutela offerta dagli artt. 1218 e ss. del codice civile, che, nel caso di specie, integra, laddove lacunosa, la disciplina di cui all'art. 82 del Reg. 2016/679[67]. Del resto, non può negarsi che la costruzione, operata prima dalla dottrina e poi dalla giurisprudenza, di una responsabilità da "contatto sociale" abbia agevolato il formarsi di una linea evolutiva della responsabilità civile

legali». Ma per capire il motivo per il quale la giurisprudenza persiste con ostinazione nell'indicare la legge tra le fonti di queste obbligazioni, dimenticandosi che dietro di esse si può scorgere sempre la presenza di un fatto, bisogna tentare un approccio meno razionalistico. In questo caso, la qualifica di obbligazione legale ricorda che a fianco dell'interesse individuale, di cui strumento è il contratto, esistono altri aspetti da considerare nell'ambito di una classificazione delle fonti, quali la volontà generale, l'interesse comune, la buona fede, l'affidamento legittimo.

[65] Va chiarito, infatti, che, anche quando si parla di obbligazioni *ex lege*, non deve intendersi che la fonte dell'obbligazione sia la legge medesima, ma il fatto (o l'atto) contemplato dalla legge come generativo dell'obbligo giuridico contemplato nella norma (vedi F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1971, p. 111). Sul trattamento dei dati personali come fatto giuridico, si veda G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit., p. 80, nonché F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, pp. 41 ss. e, ivi, spec. pp. 51 ss. e pp. 104 ss.

[66] Si veda, ad esempio, Cass. civ., sez. I, 10 agosto 2012, n. 14392, in *Società*, 2013, 175, secondo cui la responsabilità per inadempimento dell'obbligo di promuovere l'offerta pubblica d'acquisto è da ricondurre non già al generale principio del *neminem laedere*, bensì nell'alveo della responsabilità da contratto (o eventualmente *ex lege*), perché essa deriva dalla violazione di un obbligo preesistente, che la legge fa scaturire da un comportamento volontario (l'acquisto di azioni di società quotata che porta a detenere una partecipazione superiore alla soglia prevista dalle legge) con cui taluno entra in contatto con una cerchia ben definita di soggetti (gli azionisti di minoranza) nell'interesse specifico dei quali la prestazione rimasta inadempiuta (consistente nel promuovere l'offerta) era dovuta. Analogamente, sulla configurazione di una responsabilità contrattuale, in caso di violazione di un'obbligazione preesistente, si veda Cass., sez. un., 26 giugno 2007, n. 14712, in *Corriere giur.*, 2007, 12, 1706 ss., con nota di A. DI MAJO, *Contratto e torto: la responsabilità per il pagamento di assegni non trasferibili.,* secondo cui è opinione condivisa pressoché unanimemente in dottrina quella secondo cui la responsabilità nella quale incorre "il debitore che non esegue esattamente la prestazione dovuta" (art. 1218 c.c.) può dirsi contrattuale non soltanto nel caso in cui l'obbligo di prestazione derivi propriamente da un contratto, nell'accezione che ne dà il successivo art. 1321 c.c., ma anche in ogni altra ipotesi in cui essa dipenda dall'inesatto adempimento di un'obbligazione preesistente, quale che ne sia la fonte.

[67] Pare della medesima idea, G. VISINTINI, *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Dir. Inf.*, 2019, pp. 1 ss., che afferma che la norma di cui all'art. 82 "sembra chiaramente presupporre una qualificazione in termini contrattuali (o meglio di inadempimento agli obblighi previsti nel Regolamento) della responsabilità del professionista che non esegue esattamente la prestazione dovuta all'interessato".

orientata verso un *favor* per la più incisiva forma di tutela rappresentata dalla responsabilità contrattuale[68].

La disciplina di cui all'art. 82 GDPR prevede, peraltro, reiterando quanto già previsto dalla Direttiva 95/46/CE, che il titolare o il responsabile «è esonerato dalla responsabilità (…) se dimostra che l'evento dannoso non gli è in alcun modo imputabile»[69].

La violazione degli obblighi di adozione delle misure tecniche e organizzative di sicurezza, da cui discenda un danno per effetto del trattamento, comporta quindi l'insorgere di una responsabilità per il titolare (e per il responsabile) del trattamento, in ordine alla quale al danneggiato è sufficiente dimostrare l'esistenza del danno ed enunciare il rapporto con il trattamento in questione: spetterà poi al titolare (o al responsabile) del trattamento fornire la prova che l'evento dannoso non è a lui «in alcun modo» imputabile, secondo criteri di tipo oggettivo che escludono il parametro di diligenza nell'assolvimento dell'obbligo di adozione delle misure di sicurezza

[68] A questo proposito, si consenta il rinvio a S. Faillace, *La responsabilità da contatto sociale*, Padova, 2004, *passim* e, da ultimo, a F. Venosta, "*Contatto sociale" e affidamento*, Milano, 2022. Non senza dimenticare che proprio tale discussa figura, che si è sostanzialmente riappropriata del terreno lasciato libero dall'eliminazione nel nostro ordinamento della figura del quasi-contratto, ha il pregio di aver dato la spinta finale verso la "contrattualizzazione" della responsabilità precontrattuale, da anni in bilico tra varie impostazioni tra loro divergenti. Cfr., a riguardo, Cass. civ., sez. I, 20 dicembre 2011, n. 27648, in *Resp. civ. prev.*, 2012, 6, con nota di C. Scognamiglio; Cass. civ., sez. I, 12 luglio 2016, n. 14188, in *Foro it.*, 2016, 9, I, c. 2685, con nota di: A. Palmieri; Cass., 13 ottobre 2017 n. 24071, in *Corr. giur.*, 2017, 12, p. 1595. Il significativo ampliamento dell'area di applicazione della responsabilità contrattuale è certamente frutto di un'evoluzione nel modo di intendere la responsabilità civile, che dottrina e giurisprudenza hanno operato, nella prospettiva di assicurare a coloro che instaurano con altri soggetti relazioni significative e rilevanti, involgenti loro beni ed interessi, una tutela più incisiva ed efficace rispetto a quella garantita dalla responsabilità extracontrattuale *ex* art. 2043 c.c. Quest'ultima resta, pertanto, limitata al solo ambito nel quale si riscontrino lesioni *ab extrinseco* a beni o interessi altrui, al di fuori di qualsiasi rapporto preesistente che si ponga come fonte di obblighi di vario genere (di prestazione e/o di protezione).

[69] La prova sulla «non imputabilità» in alcun modo dell'evento dannoso, prevista dall'art. 82 cit., è contemplata in una formula che riecheggia quella già prevista all'art. 1218 c.c. in tema di responsabilità da inadempimento, sicché si ripropone anche con riguardo a tale formula, contenuta nel Reg. UE 2016/679, l'interrogativo in ordine ai connotati della «causa non imputabile» e, in particolare, se l'assolvimento dell'onere probatorio debba essere svolto ricorrendo a criteri di colpevolezza o se, al contrario, sia preferibile un'impostazione di carattere oggettivo, scevra dai canoni di diligenza, impostata su altre fondamenta, quali ad esempio il criterio del rischio. F. Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 417, ritiene di poter accordare maggior rilievo all'impostazione basata su criteri di tipo oggettivo, in quanto maggiormente aderenti al tenore letterale della disposizione e, soprattutto, connotata da una maggior efficienza secondo i criteri dell'analisi economica del diritto (per un'ampia ed articolata ricostruzione del dibattito in ordine al concetto di causa non imputabile oggetto di prova liberatoria *ex* art. 1218 c.c., con impostazione preferenziale per una concezione oggettivistica, si rimanda a G. Visintini-L. Cabella Pisu, *L'inadempimento delle obbligazioni*, cit., pp. 158 ss. e pp. 173 ss., per le quali «la nozione di "causa non imputabile" deve essere intesa nell'ordinamento attuale, non già nel senso di "causa non riferibile alla colpa dell'obbligato" ma nel senso di "evento estraneo alla sfera di controllo dell'obbligato, inevitabile e in rapporto causale con una effettiva impossibilità ad adempiere"»). Propende invece per la tesi di una responsabilità fondata su dolo o colpa del debitore, C.M. Bianca, *Diritto civile, 5, La responsabilità,* cit., pp. 13 ss.

previste dal nuovo Regolamento. Tale disciplina, che, come già detto, risulta lacunosa, seguendo l'impostazione che vede quella di cui all'art 25 GDPR come obbligazioni di fonte *lato sensu* contrattuale, andrà integrata con quella prevista, nel diritto interno, con riguardo ai limiti di risarcibilità di cui all'art. 1225 c.c. e al termine prescrizionale decennale[70].

3. Applicazione del principio nella casistica

3.1. I provvedimenti del Garante nei confronti di privati: a) la privacy by design nei rapporti di lavoro

L'intervento "paragiurisprudenziale" del Garante, successivo all'entrata in vigore del Reg. UE 2016/679, può essere descritto lungo due diverse linee direttrici, a seconda che il titolare del trattamento sia un privato o una pubblica amministrazione, visto che la casistica tende a diversificarsi per la peculiarità strutturali e funzionali dei relativi soggetti. Nell'ambito di questa distinzione, sono rinvenibili altre sottocategorie, di cui si darà conto qui di seguito.

Il primo ambito di applicazione della normativa qui in rilievo, di cui ci si intende occupare, è relativo al rapporto di lavoro privato. Come noto, la "libertà" di decidere come strutturare l'attività economica è fortemente limitata dall'obiettivo dell'effettiva tutela della riservatezza di quanti prestino lavoro nell'organizzazione aziendale e, dunque, è vincolata al presupposto che gli impianti e/o gli strumenti produttivi adottati non determinino un controllo più penetrante di quello necessario. La scelta organizzativa o produttiva, dunque, non potrà sostanziarsi nell'adozione di strumenti che comportino un controllo diretto sulla prestazione di lavoro, dovendosi sempre scegliere l'assetto organizzativo che minimizza sin dall'origine l'invadenza nella sfera personale di chi lavora[71]. Tale tematica è stata oggetto di alcune pronun-

[70] Per un'impostazione diversa da quella esposta nel testo, si veda D. Barbierato, *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Resp. civ. prev*., 2019, p. 2151, che ritiene che la responsabilità *ex* art. 82 debba avere natura extracontrattuale. Gli obblighi conformativi, in ordine alla condotta del titolare o del responsabile del trattamento, rivestirebbero natura procedimentale metaindividuale poiché destinati a proteggere la dignità della persona e la circolazione dei dati, in accordo con quanto previsto dall'art. 1, par. 1, del Regolamento. Mediante la previsione di tali obblighi si mirerebbe, quindi, a tutelare il singolo individuo e, di riflesso, anche il mercato dei dati. E questa finalità risulterebbe coerente con il «chiunque», riportato nell'art. 82, che indicherebbe che tale norma è posta a tutela di tutti i consociati e non del solo interessato. Ad avviso di chi scrive, tale impostazione è criticabile, in quanto non tiene in considerazione quegli elementi che, invece, paiono dimostrare la natura *lato sensu* "contrattuale" del rapporto, quali la prossimità tra le parti e l'affidamento che l'interessato ha nei confronti del titolare del trattamento, sulla base degli obblighi previsti dalle disposizioni di cui all'art. 25 GDPR.

[71] Il principio della privacy *by design*, nei fatti, è stato applicato dall'Ispettorato nazionale del lavoro con una circolare sui call center antecedente all'entrata in vigore del GDPR (circolare n. 4 del 26 luglio 2017), ove si chiariva che le esigenze produttive devono giustificare «l'assoluta indispensabilità» degli applicativi, altrimenti sarebbe «difficile ricollegare l'inevitabile compressione della libertà e della dignità dei lavoratori alle prioritarie ragioni produttive». Nel caso dei *call center*, il problema riguarda proprio quei *software* che consentono il monitoraggio dell'attività telefonica e

ce che hanno posto limitazioni e vincoli alla raccolta dei dati dei *riders* da parte delle società di *delivery* che permettono prenotazioni per mezzo di applicazioni per *computer* o *smartphone*. Ad esempio, il Garante *privacy* ha ingiunto ad una società di *delivery* di conformare al Regolamento il proprio trattamento dei dati dei *riders*, in applicazione dei principi di minimizzazione e di *privacy by design* e *by default*, imponendo la specifica individuazione dei soggetti autorizzati ad accedere ai sistemi, in qualità di supervisori, definendo a priori ipotesi predeterminate e specifiche finalità che rendano necessario tale accesso e adottando misure appropriate per la verifica del medesimo[72]. Nel caso di specie, infatti, i sistemi erano stati configurati in modo da raccogliere e memorizzare tutti i dati relativi alla gestione dell'ordine (dati raccolti tramite l'applicativo in uso ai *rider*, compresa la rilevazione attraverso GPS ogni 12 secondi, nonché attraverso le interazioni con il *customer care*, dei tempi di consegna – stimati ed effettivi – per ciascuna fase dell'ordine, lo storico degli ordini relativi a ciascun *rider* – compresa la percentuale degli ordini accettati –, l'indicazione dell'ultima connessione effettuata, il numero e la tipologia di "azioni" effettuate nei confronti del *rider*, con il dettaglio di ogni "azione", la zona della città ove avviene l'ordine, la mappa dell'ordine effettuato, i dettagli degli ordini rifiutati). Gli operatori autorizzati avevano, poi, la possibilità di ottenere la condivisione dei dati raccolti nei diversi sistemi. Inoltre, il sistema era configurato in modo da consentire all'operatore di accedere direttamente al contenuto di *chat* ed e-*mail* scambiate con i *rider*, ricostruendo, per ciascuno di essi, tutte le comunicazioni effettuate. I predetti sistemi risultavano preordinati, rispettivamente, alla gestione degli ordini in tempo reale e alla visualizzazione dello storico degli ordini stessi, nonché alla gestione di problemi verificatisi nel corso dell'ordine. Tale configurazione del sistema, tenuto conto della quantità e varietà dei dati raccolti e delle modalità di trattamento, aveva dunque comportato, secondo il Garante, la violazione dell'art. 5, par. 1. lett. *c)*, del Regolamento (principio di minimizzazione dei dati) e dell'art. 25 del Regolamento relativo alla protezione dei dati fin dalla progettazione e per impostazione predefinita (*privacy by design* e *by default*). Rispetto a fattispecie analoga, il Garante ha individuato, in altra società di *delivery*, la violazione dell'art. 5, par. 1. lett. *e)*, del Regolamento che dispone che i dati personali siano conservati «in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al con-

della produttività di ciascun operatore. Essi raccolgono ed elaborano in tempo "quasi reale" i dati relativi agli stati di attività telefonica di ciascun operatore (libero, non disponibile, in pausa, ecc.) e i tempi medi di evasione delle diverse lavorazioni. Altri *software*, invece, quantificano la produttività giornaliera per ogni servizio reso, il tempo dedicato al lavoro per ciascuna commessa e le pause effettuate da ogni singolo lavoratore. I suddetti *software*, «pur funzionali a più o meno generiche esigenze produttive, consentono di realizzare un monitoraggio individualizzato costante e continuo su tutti gli operatori che finisce per dar vita a un controllo minuzioso su tutta l'attività svolta da ogni singolo lavoratore, eliminando del tutto qualunque margine spazio-temporale nel quale il lavoratore stesso possa ragionevolmente essere certo di non essere osservato, ascoltato o comunque "seguito" nello svolgimento della propria attività e dei propri movimenti». In argomento vedi V. Nuzzo, *I software che registrano la durata delle telefonate nei* call center *sono strumenti di lavoro?*, in *Riv. it. dir. lav.*, 2018, pag. 307, nota a Tribunale Pescara, 25 ottobre 2017.

[72] Provv. GPDP, su caso Deliveroo Italy S.r.l., del 22 luglio 2021, doc. *web* n. 9685994, in *www.garanteprivacy.it*.

seguimento delle finalità per le quali sono trattati» e dell'art. 25 del Regolamento, tenuto conto del numero significativo di soggetti autorizzati dalla società ad accedere ai menzionanti sistemi, nonché della quantità, varietà e natura dei dati trattati[73]. Sul titolare del trattamento grava, infatti, l'obbligo «di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario» (come stabilisce il *considerando* n. 39)[74]. Nel caso di specie, la società aveva omesso di individuare distinti tempi di conservazione dei dati riferiti ai *riders*, in relazione alle distinte e specifiche finalità perseguite, posto che solo alcuni dei trattamenti effettuati risultavano necessari per la finalità di gestione del rapporto contrattuale (es. dati identificativi e di contatto, generalità, dati bancari) mentre, rispetto ad altri, la gestione del rapporto contrattuale costituiva il contesto del trattamento effettuato[75]. Anche in questo caso, i sistemi erano configurati in modo da raccogliere e memorizzare tutti i dati relativi alla gestione dell'ordine (rilevazione della posizione geografica attraverso GPS ogni 15 secondi, nonché i dati relativi ai tempi di consegna stimati e ai tempi realmente occorsi per effettuare la consegna, dati relativi ai singoli punteggi assegnati al *rider* giornalmente; dati relativi alle comunicazioni via *e-mail* e *chat* nonché i dati esterni riferiti alle telefonate conservate dalla capogruppo con possibilità di accedere al contenuto delle conversazioni previa attivazione di una procedura di autorizzazione nei confronti della capogruppo medesima, secondo quanto dichiarato dalla società), e il sistema di gestione delle *chat* e delle *e-mail* era configurato in modo tale da consentire ad ogni operatore di accedere direttamente al contenuto delle medesime comunicazioni con i *riders*.

In altra fattispecie[76], il Garante *privacy* ha ingiunto ad un fornitore di servizi di localizzazione di incorporare il diritto alla *privacy* – per impostazione predefinita – nelle funzionalità del prodotto, dando concreto significato al principio di *privacy by design*. Il procedimento muoveva dalla segnalazione, da parte di un dipendente, dell'illecito trattamento dei propri dati personali effettuato dal suo datore di lavoro, tramite un dispositivo di geolocalizzazione, installato sull'autovettura aziendale assegnatagli con possibilità di uso promiscuo, «in assenza di una previa informativa o, comunque, della comunicazione di una *policy* aziendale»[77].

---

[73] Provv. GPDP del 10 giugno 2021 nei confronti di Foodinho S.r.l., doc. *web* n. 9675440, in *www.garanteprivacy.it*.

[74] Secondo il Garante Privacy, il titolare non deve limitarsi ad individuare "blocchi" di fasce temporali omogenee (Provv. GPDP 9 gennaio 2020, n. 8, doc. *web* n. 9263597), in *www.garanteprivacy.it*.

[75] La società aveva individuato un unico termine di conservazione pari a 4 anni dopo la cessazione del rapporto di lavoro, in relazione ad una pluralità di trattamenti effettuati per scopi diversi, nonché in relazione a distinte tipologie di dati, in alcuni casi riferiti al contenuto di comunicazioni in sé protette da particolari garanzie da parte dell'ordinamento (via *chat*, *email* e telefono).

[76] Cfr., GPDP Provv. n. 396 del 28 giugno 2018, commentato da MINISCALCO, *Uno, nessuno o centomila? Minimizzazione e privacy by default nel primo provvedimento del Garante dopo il GDPR*, in *Dir. inf.*, 2018, p. 782.

[77] L'autorità di controllo diverse volte è intervenuta, in occasione delle verifiche preliminari, di cui all'abrogato art. 17 del codice in materia di protezione dei dati personali, per prescrivere al titolare specifiche misure da adottare per configurare il sistema di trattamento in modo che risultasse conforme alle previsioni normative vigenti. Anche con Provv. GPDP del 24 maggio 2017, n. 247 (doc. *web* n. 6495708), in *www.garanteprivacy.it*, il Garante per la protezione dei dati personali, a seguito

Il trattamento consisteva nella raccolta, registrazione e consultazione, mediante il collegamento con la piattaforma *web* messa a disposizione dal fornitore del servizio, dei dati relativi «alla posizione dei veicoli acquisita dal sistema ogni 120 secondi, al loro stato (fermo/in movimento), alla velocità, nonché dati ulteriori relativi all'utilizzo del veicolo nella giornata in corso (le ore di impiego e di guida, le ore di pausa, la velocità media, indicate sia in totale che distintamente per ciascuna tratta effettuata, anche di pochi minuti)» e nella conservazione degli stessi per un periodo di 365 giorni[78]. Infine, non risultava essere stata implementata la funzione opzionale "*Privacy*", consistente in un interruttore che, una volta installato nel dispositivo di localizzazione, avrebbe permesso di disabilitare la tracciabilità e la memorizzazione, con conseguente minimizzazione dei dati raccolti.

Secondo l'Autorità di controllo, il datore di lavoro era in concreto in grado di identificare – sia per il numero limitato di mezzi di trasporto, utilizzati ciascuno per precisi servizi, sia in considerazione delle finalità perseguite dalla società – i dipendenti che, nell'espletamento delle proprie mansioni, utilizzavano i veicoli soggetti a localizzazione, con conseguente violazione del divieto di controllo a distanza dell'attività dei lavoratori. Sotto altro profilo, l'impossibilità di disattivare il sistema di geolocalizzazione comportava il trattamento di dati non rilevanti ai fini della valutazione dell'attitudine professionale del dipendente, in violazione dell'art. 8 della l. n. 300/1970. In ottica di effettività della tutela dei diritti degli interessati, il Garante prescriveva, quindi, al fornitore del servizio (responsabile esterno del trattamento), di «configurare – in base al principio di *privacy by design e by default* – la versione *standard* dei servizi offerti attraverso il sistema di localizzazione con modalità proporzionate rispetto al diritto alla riservatezza degli interessati, in particolare con

di richiesta di verifica preliminare, ha emanato specifiche prescrizioni in ordine alle modalità con cui deve essere configurato il trattamento di dati personali dei lavoratori effettuato da una società a capitale interamente pubblico e gestore per conto di vari committenti (comuni o consorzi di comuni) nell'ambito dei servizi di igiene urbana della provincia di Ancona (con particolare riguardo alla raccolta differenziata ed al trasporto di rifiuti solidi urbani). Il sistema di trattamento da utilizzare per l'erogazione dei predetti servizi prevedeva la rilevazione, ogni trenta secondi, di coordinate satellitari relative alla geolocalizzazione di apparati elettronici di tipo radio mobili e veicolari in uso da parte del personale operativo. Il Garante, pur ritenendo lecito il trattamento, ha tuttavia ritenuto che fosse necessario configurare il sistema tecnologico in maniera diversa. Nel provvedimento suddetto, viene infatti precisato che «al fine, dunque, di contemperare i principi di tutela della protezione dei dati personali con le prospettate finalità di efficiente gestione del servizio anche mediante verifica del passaggio del mezzo geolocalizzato presso tutti i punti di raccolta, in assenza di ulteriori esigenze che giustifichino il rilevamento periodico a così elevata frequenza (due rilevamenti/minuto), occorre configurare opportunamente il sistema. (…) In particolare, la rilevazione del dato di geolocalizzazione dovrà avvenire nel momento in cui l'automezzo giunga in prossimità di un punto di raccolta, vale a dire in relazione a punti predeterminati e precedentemente georeferenziati, che potranno coincidere, a seconda delle valutazioni della società, con tutti o alcuni dei punti di raccolta (c.d. rilevazione "ad eventi")».

[78] Secondo la difesa dell'incolpata, il trattamento dei dati *de quibus* era posto in essere al fine di gestire le richieste di intervento, di garantire un efficiente utilizzo del parco veicoli, per la sicurezza dei lavoratori e dei beni aziendali, per ottenere benefici in occasione della stipula di contratti di assicurazione, nonché, in caso di contestazioni di violazioni amministrative, «per ricondurre ad un autista determinato la relativa responsabilità».

riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati ed alla messa a disposizione delle mappe dei percorsi effettuati. Prescriveva pure che la società informasse i propri clienti della possibilità di modificare il sistema rispetto alla impostazione *standard* e imponeva di rendere disponibile in relazione a tutte le modalità di abbonamento la funzione che consenta la disattivazione del dispositivo di localizzazione «senza eccessivi costi aggiuntivi». L'Autorità, nel caso di specie, ha correttamente ritenuto che le modalità con cui il trattamento era stato posto in essere «e, segnatamente, la raccolta di informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti cui i veicoli sono affidati» risultassero sproporzionate rispetto alle finalità, che ben avrebbero potuto «essere utilmente e legittimamente perseguite con la raccolta di informazioni assai più limitate».

3.2. (*segue*): b) attività promozionali dell'impresa e obblighi da rispettare in conformità alle prescrizioni del GDPR

Un altro indirizzo da menzionare fa riferimento alla non corretta applicazione dei principi di cui all'art. 25 GDPR, nell'ambito di un'attività di tipo promozionale da parte di aziende private.

Il Garante *privacy*, in un recente provvedimento, ha stigmatizzato il comportamento non conforme al GDPR di una nota azienda che opera in *franchising* per l'intermediazione nelle compravendite[79]. La medesima non aveva messo in atto «misure tecniche e organizzative adeguate volte ad integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati». Inoltre, la lacunosità e genericità delle informative sulla *privacy* e sulla *newsletter* avevano messo in luce una non corretta ed inadeguata impostazione dei trattamenti in rilievo, integrando la violazione del principio di *privacy by design* individuato dall'art. 25, par. 1, del Regolamento. In particolare, l'informativa *privacy* risultava carente riguardo all'indicazione delle modalità del contatto promozionale e all'individuazione dei soggetti terzi e/o delle categorie merceologiche delle Società terze cui venivano comunicati i dati per fini promozionali; né vi era una chiara identificazione delle Società terze deputate alla rilevazione della qualità dei servizi alle quali la società comunicava i dati personali degli utenti. Inoltre, l'informativa in questione indicava espressamente che la registrazione "del nominativo" dell'interessato al sito internet comportava l'acquisizione "automatica" di un consenso alla comunicazione dei dati, nonché ai trattamenti per finalità promozionali anche da parte di Società del gruppo o di Società terze. Tale consenso, privo dei caratteri di libertà e di specificità individuati nell'art. 4, n. 11, del Regolamento, non costituiva un'idonea base giuridica per i citati trattamenti, ai sensi dell'art. 6 del Regolamento medesimo.

Anche nei confronti di primaria società del settore energetico, il Garante ha accertato la violazione degli artt. 5, par. 2, e 25, par. 1, del Regolamento, per non aver intrapreso un'efficace azione di contrasto rispetto al fenomeno degli indebiti contatti

[79] Cfr. GPDP, Ordinanza-ingiunzione resa nei confronti di Tempocasa S.p.a. del 27 maggio 2021, doc. *web* n. 9689375.

promozionali effettuati in proprio nome[80]. La mera non riferibilità delle numerazioni chiamanti alla rosa di quelle in uso da parte della società e dei propri *partner* commerciali non è valida esimente per il Garante, in ragione di *quell'ottica proattiva* che definisce il principio di responsabilizzazione del titolare del trattamento e che permea tutto il nuovo assetto normativo in tema di *data protection*. L'impresa nei cui confronti era stato attivato il procedimento innanzi al Garante non aveva esercitato nei confronti dei propri *partner* commerciali in maniera piena e consapevole le proprie attribuzioni, alle quali corrispondono i doveri di *accountability* e di *privacy by design* (attraverso elementi di prevenzione, funzionalità, sicurezza, trasparenza del trattamento e centralità dell'interessato) individuati dagli artt. 5, par. 2, e 25, par. 1 e 2 del Regolamento. In particolare, la società non aveva introdotto forme di controllo automatiche e stabili nell'ambito dell'organizzazione societaria sia interna che esterna (ci si riferisce alla rete di vendita costituita dai *partner* commerciali), nonché sui sistemi deputati ad attivare offerte e servizi verso la propria clientela. La programmazione di questi ultimi, ad esempio, secondo il Garante avrebbe potuto essere progettata in maniera predefinita, in modo da segnalare e bloccare in tempo reale i tentativi di caricamento di contratti di fornitura ottenuti in maniera poco trasparente o comunque all'esito di trattamenti eseguiti in violazione della normativa in materia di protezione dei dati personali. Le campagne promozionali, conclude il Garante, devono essere condotte nel pieno rispetto dei principi di responsabilizzazione e *privacy by design*, dovendo il titolare comprovare in qualsiasi momento che l'attivazione di offerte e servizi e la registrazione di contratti avvenga solo a seguito di contatti promozionali effettuati dalla rete di vendita della Società, attraverso numerazioni telefoniche censite e iscritte al ROC – Registro degli Operatori di Comunicazione – e previa necessaria verifica delle liste di contattabilità. Analogamente, l'Autorità Garante ha rilevato l'illiceità del trattamento dei dati personali di altro ente fornitore di energia nell'attivazione di contratti non richiesti e nello svolgimento di attività promozionali[81]. Il Garante ha individuato, nel caso di specie, la presenza di circa 7200 contratti conclusi illecitamente, senza la consapevolezza dei diretti interessati, spesso con dati personali inesatti e sottoscrizione apocrifa. I trattamenti illeciti oggetto del provvedimento erano stati effettuati dalla società mediante un'agenzia terza, che agiva tramite attività di vendita porta-a-porta e nei negozi. Tuttavia, *ex* art. 24 del Regolamento, il titolare è tenuto a mettere in atto un sistema organizzativo e gestionale adeguato al trattamento per garantire la protezione dei dati degli interes-

[80] Cfr., GPDP Provv. del 16 dicembre 2021, doc. *web* n. 9735672 nei confronti di Enel Energia S.p.a.

[81] GPDP, Provv. reso nei confronti di Eni Gas e luce S.p.A., del 11 dicembre 2019, doc. *web* n. 9244358, in *www.garanteprivacy.it*. Cfr. pure il provvedimento nei confronti di Edison energia S.p.a. del 15 dicembre 2022 doc. *web* n. 9856345*,* per aver realizzato campagne promozionali nei confronti di utenti prospect senza effettuare verifiche a campione rispetto alle singole numerazioni e, quindi, senza porre in essere adempimenti in materia di protezione dei dati personali (quali: informativa; consenso; esattezza e qualità dei dati), in contrasto ai principi di *privacy by design* ed accountability; tali violazioni sono state confermate anche in relazione alla non corretta gestione dell'opposizione effettuata dagli utenti prospect inseriti in una "lista di non contattabilità" priva di elementi circostanziati (data del diniego, dell'inserimento in lista, l'identità dell'interessato), che non consentono di ricostruire correttamente modalità e tempi di acquisizione e revoca del consenso.

sati. Ciò non si esprime soltanto negli adempimenti richiesti dal Regolamento, ma anche nella predisposizione di misure tecniche, procedure e prassi organizzative atte a conformare i trattamenti e verificarne la loro liceità. In riferimento a quest'ultimo punto, il Garante ha individuato numerose carenze di carattere sistemico nelle modalità procedurali, che hanno permesso agli agenti di agire in violazione delle istruzioni ricevute per un periodo di tempo esteso. Da tali condotte, il Garante ha rilevato ulteriori violazioni: la mancanza di un sistema organizzativo e operativo adeguato, conforme al GDPR, avrebbe permesso di evitare le suddette condotte illecite, in accordo con il principio di *accountability*, nonché di *privacy by design* e *by default*.

Anche nei confronti delle società telefoniche il Garante ha rilevato violazioni analoghe del GDPR. Si sono verificati vari episodi di opposizioni al trattamento non registrate o non rispettate dagli operatori, informative inadeguate, l'inconsapevolezza del gestore telefonico su molti degli aspetti dei trattamenti effettuati o dei dati raccolti, l'incapacità di quantificare i casi di violazione dei propri operatori e gravi incongruenze tra le dichiarazioni della Società e i *call center partner*. Tutti questi aspetti hanno determinato anche la violazione dei principi di *accountability* e *privacy by design*[82]. Il Garante ha contestato, poi, in un'altra fattispecie, l'assenza di controlli che evitassero di attivare servizi o sottoscrivere contratti sulla base dei dati ottenuti illecitamente[83]. Si era proceduto in ogni caso a raccogliere le informazioni e a inserirle nei propri *database*, senza alcun tipo di selezione: ad esempio, sarebbe bastato che i vari sistemi (di organizzazione delle campagne promozionali e di raccolta di dati per attivare contratti) avessero potuto comunicare tra loro, perché fosse

[82] GPDP, Provv. reso nei confronti di TIM S.p.A., del 15 gennaio 2020, doc. *web* n. 9256486.

[83] GPDP, Provv. n. 224 del 12 novembre 2020, doc. *web* n. 9485681, nei confronti di Vodafone S.p.A. Il Garante ha accertato una condotta elusiva dei suindicati principi anche nel comportamento di chi, nonostante avesse comunicato le esatte procedure e fosse intervenuto a correggere alcune irregolarità (anche se con poca incisività a detta del Garante), non ha svolto quei controlli più stringenti che avrebbero permesso di individuare le condotte illegittime e illegali dei propri agenti sul territorio (GPDP, Provv. del 9 luglio 2020, doc. *web* n. 943575, nei confronti di Wind Tre s.p.a. Nel caso di specie, erano emersi casi di contatti illeciti ai fini di *telemarketing* e *teleselling* effettuati: (i) senza consenso; (ii) con consenso inidoneo; (iii) con consenso non conforme al nuovo quadro normativo, perché ancora risalente alla normativa precedente; (iv) con consenso ottenuto tramite le applicazioni MyWind e My3, le quali obbligavano l'utente a fornire ad ogni accesso i consensi per tutte le finalità di trattamento, con l'opzione di poterli revocare soltanto dopo 24 ore con modalità più complesse; (v) con consenso acquisito con modalità illegittime, attraverso la precompilazione da parte degli agenti delle caselle inserite nei contratti, spesso con consensi accorpati e col testo di dimensioni minori rispetto al resto; (vi) con consenso acquisito illegalmente, a causa dell'operato di alcuni *call-center* che avrebbero ottenuto dati di clienti di altri operatori telefonici con modalità in violazione delle norme in materia di *privacy* e protezione dei dati, e delle norme fiscali, tributarie e lavorative. Il Garante ha giudicato tali condotte come indice di una modalità operativa improntata ad ottenere il consenso in ogni modo possibile, a fronte di procedure più complicate per esercitare il diritto di opposizione al trattamento. A definire un quadro complessivamente inidoneo a soddisfare gli standard di adeguatezza, oltre ai multipli episodi di misure tecniche e organizzative inidonee, e l'incapacità di dimostrare la conformità dei propri trattamenti, ha influito sia la disponibilità che la Società aveva di utilizzare strumenti adeguati e idonei, e il non averlo fatto, sia le sufficienti conoscenze in materia date dalle pronunce del Garante indirizzate alla medesima azienda in passato. Sulla violazione dei principi di cui all'art. 25 GDPR e telemarketing, vedi anche GPDP, Ordinanza-ingiunzione resa nei confronti di Douglas Italia S.p.a., del 20 ottobre 2022, doc. *web* 9825667.

più semplice verificare che tutti i dati fossero trattati nel rispetto delle norme. La mancanza di controlli e procedure di tal genere hanno evidenziato per il Garante una grave falla nell'*accountability* del gestore e nel perseguimento dei principi di *privacy by design* e *by default.*

3.3. La violazione delle norme di cui all'art. 25 del GDPR da parte della pubblica amministrazione

Nell'ambito dei rapporti tra privati e pubblica amministrazione, l'Autorità Garante si è pronunciata, in materia di fatturazione elettronica, stabilendo che l'Agenzia delle Entrate è tenuta ad adottare tecniche di cifratura per evitare che l'archiviazione includa dati la cui intelligibilità non sia necessaria a fini fiscali[84]. Anche in un successivo parere, il Garante[85], con specifico riferimento alle fatture afferenti il settore legale, si è espresso esortando la P.A. competente ad adottare misure idonee a garantire la protezione dei dati personali *by default* e comunque con modalità compatibili con la disciplina relativa all'inalterabilità di tali documenti, pretendendo che le informazioni relative alla descrizione dei beni ceduti e dei servizi prestati fossero rese inintelleggibili ed escluse dalla memorizzazione dalla banca dati dei "dati fattura integrati", fatte salve le attività di controllo svolte in relazione a richieste di detrazione/deduzione delle spese sostenute nell'occasione.

---

[84] Cfr., a riguardo, GPDP, Provv. del 20 dicembre 2018 *doc*. web n. 9069072. In altra fattispecie, ma sempre riguardante il mancato utilizzo degli strumenti di cifratura, (cfr. ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a., del 10 giugno 2021, doc. *web* n. 9685922), il Garante Privacy ha rilevato il trattamento scorretto di dati personali del dipendente che segnala illeciti (c.d. *whistleblowing*). Il quadro normativo (cfr. art. 54-*bis* del d.lgs. 30 marzo 2001, n. 165, introdotto dall'art. 1, co. 51, della l. n. 190/2012, integrata e modificata dalla l. 30 novembre 2017, n. 179, «Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato») prevede misure volte a proteggere la divulgazione dell'identità del segnalante, allo scopo di prevenire principalmente l'adozione di misure discriminatorie nei confronti dello stesso. Il titolare, quindi, nel caso, avrebbe dovuto definire il proprio modello di gestione delle segnalazioni in conformità ai principi della "protezione dei dati fin dalla progettazione" e della "protezione per impostazione predefinita", tenuto conto anche delle osservazioni presentate al riguardo dal responsabile della protezione dei dati (RPD). Per tali ragioni, il mancato utilizzo della crittografia per il trasporto e la conservazione dei dati è risultato non conforme alle disposizioni di cui all'art. 5, par. 1, lett. *f)*, e all'art. 32 del Regolamento che, al suo par. 1, lett. *a)*, individua espressamente tale tecnica come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio [v. anche cons. 83 del Regolamento nella parte in cui prevede che «il titolare del trattamento (…) dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura»]. La mancata adozione delle necessarie misure a tutela degli interessati, con riguardo al tracciamento degli accessi all'applicativo, si era posto pertanto in contrasto anche con i principi della "protezione dei dati fin dalla progettazione" e della "protezione dei dati per impostazione predefinita" di cui all'art. 25 del Regolamento.

[85] Cfr. GPDP, Parere del 22 dicembre 2021, doc. *web* n. 9732234*,* sullo schema di provvedimento del Direttore dell'Agenzia delle Entrate relativo alle nuove regole tecniche per la memorizzazione delle fatture elettroniche, da utilizzare per l'analisi del rischio e controllo a fini fiscali e per le funzioni di polizia economica e finanziaria.

In vari provvedimenti del Garante viene, poi, affrontata la tematica relativa alla diffusione da parte di una p.a. dei dati di soggetti privati. Ad esempio, il Garante ha rilevato l'illiceità del trattamento di dati personali effettuato da un Comune, per aver diffuso dati e informazioni personali del reclamante, contenuti in un'ordinanza pubblicata *online*[86], con violazione dell'obbligo di adottare *by design*, fin dall'inizio del trattamento, idonee misure tecniche e organizzative volte a minimizzare i dati pubblicati. Nell'ordinanza pubblicata *online* dal Comune, infatti, era rimasta l'indicazione in chiaro della data e del luogo di nascita, nonché del domicilio del reclamante. Nell'occasione è stata rilevata la non conformità al principio di «minimizzazione» dei dati, considerando che gli stessi non risultavano essere stati «limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Analoga problematica è stata decisa dal Garante Privacy nei confronti di altro Comune[87], sul cui sito *web* istituzionale era possibile visualizzare e scaricare liberamente la Determinazione che riportava in chiaro, nel testo e nell'oggetto, dati e informazioni personali, quali il nominativo del dipendente e l'indicazione della relativa condizione assoluta di inabilità al lavoro, nonché altre informazioni inerenti all'attività lavorativa, all'effettuazione della visita medica, all'«acquisizione al diritto alla pensione di inabilità per infermità non dipendente da cause di servizio»; alla risoluzione del rapporto di lavoro. Si è

[86] Cfr. GPDP, Ordinanza-ingiunzione resa nei confronti di Comune di Fisciano in data 24 giugno 2021, doc. *web* n. 9689586. In senso analogo, vedi GPDP, Provv. del 16 settembre 2021, doc. *web* n. 9714622, nei confronti del Comune di Ladispoli. In esso è stato censurata la diffusione *online* dei dati personali del reclamante (data e luogo di nascita, indirizzo di residenza, codice fiscale, codice iban personale su cui accreditare le somme dovute dal Comune) contenuti nelle determinazioni dirigenziali. Anche in questo caso è stata invocata la violazione del Regolamento, che prevede che il titolare del trattamento debba mettere «in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento» («*data protection by default*») e debba essere «in grado di dimostrare» – alla luce del principio di «responsabilizzazione» («*accountability*») – di averlo fatto (artt. 5, par. 2; 24 e 25, par. 2, GDPR). Pertanto, la diffusione dei dati e delle informazioni del reclamante è risultata non conforme al principio di «minimizzazione» [art. 5, par. 1, lett. *c)*, del GDPR], in quanto i predetti dati non erano «limitati a quanto necessario rispetto alle finalità» di pubblicità legale sull'albo pretorio online. Anche nell'Ordinanza ingiunzione 22 luglio 2021 nei confronti della Università degli studi di Milano Bicocca (doc. *web* n. 9697781), il Garante si è occupato della diffusione di dati e informazioni personali del reclamante (data e luogo di nascita, codice fiscale) contenuti in documenti pubblicati online sul sito *web* istituzionale della suddetta Università, unitamente alla copia fronte-retro della relativa carta d'identità. L' Autorità, nell'invocare la violazione dei medesimi suindicati articoli del Regolamento, ha ricordato che la presenza di uno specifico regime di pubblicità non può comportare alcun automatismo rispetto alla diffusione online dai dati e informazioni personali, né una deroga ai principi in materia di protezione dei dati personali di provenienza europea.

[87] Cfr. GPDP, Provv. dell'8 luglio 2021, doc. *web* n. 9703112, nei confronti del Comune di Salò; analoga fattispecie si è verificata con riferimento al provvedimento in data 1 dicembre 2022 nei confronti dell'Azienda Ospedaliera A.r.n.a.s. Civico di Cristina Benfratelli (doc. *web* n. 9842783), in cui è stata lamentata la pubblicazione sul sito *web* istituzionale dell'Azienda di due provvedimenti, contenenti dati personali dell'interessato, anche relativi alla salute (con l'espresso riferimento al «verbale di riconoscimento dell'invalidità civile» del reclamante, oltre a informazioni di dettaglio relative a vicende connesse al rapporto di lavoro – es. la richiesta di collocamento a riposo dell'interessato). Nell'occasione si è ribadito che il titolare del trattamento deve mettere «in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento».

rilevata quindi l'illiceità del trattamento di dati personali effettuato da tale Comune, per la diffusione sul sito *web* istituzionale dei dati sulla salute del soggetto interessato (avvenuta in violazione del divieto previsto dall'art. 2-*septies*, co. 8, del Codice e dell'art. 9, parr. 1, 2 e 4, del Regolamento) e di ulteriori dati personali del medesimo – come le informazioni inerenti all'attività lavorativa e alla risoluzione del rapporto di lavoro. In tale quadro, si è reputato necessario ingiungere, ai sensi dell'art. 58, par. 2, lett. *d)*, del GDPR, al suddetto Comune di mettere in atto, fin dalla progettazione, le misure tecniche e organizzative adeguate, con particolare riferimento al «servizio di pubblicazioni all'Albo pretorio, e al successivo passaggio nella sezione storica dell'albo», in modo da evitare automatismi nella pubblicazione di atti sul sito *web* istituzionale che possano portare a illecite diffusioni di dati personali, integrando «nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati» (art. 25, parr. 1 e 2, GDPR), quali la minimizzazione, tenendo conto, fra l'altro, dei rischi, del contesto e dell'ambito di applicazione del trattamento, garantendo «che siano trattati, per impostazione predefinita» (*data protection by default*) «solo i dati personali necessari per ogni specifica finalità del trattamento» (art. 25, parr. 1 e 2, GDPR)[88].

[88] Analoghe violazioni dei principi più volte richiamati, ma relative a fattispecie del tutto diversa sono state trattate dall'ordinanza ingiunzione del Garante nei confronti di Università Commerciale "Luigi Bocconi" di Milano (GPDP, Provv. del 16 settembre 2021, doc. *web* n. 9703988*)*. Nel caso in esame, a seguito del reclamo di uno studente, il Garante ha rilevato l'illiceità del trattamento dei dati personali degli studenti effettuato dall'Ateneo. In particolare, è emerso che l'Ateneo, nel contesto dell'emergenza epidemiologica da SARS-CoV-2, aveva adottato una modalità alternativa di svolgimento degli esami universitari a distanza, avvalendosi di un sistema di supervisione a distanza delle prove d'esame scritte (*proctoring*), avente la duplice finalità di identificare gli studenti e di verificare il corretto comportamento degli stessi durante lo svolgimento della prova d'esame. Il sistema sopradescritto comportava il trattamento di categorie particolari di dati, come i dati biometrici. Il *software*, infatti, catturava le immagini video e lo schermo dello studente identificando i momenti in cui erano rilevati comportamenti insoliti e/o sospetti, mediante registrazione video e istantanee scattate a intervalli casuali per tenere traccia di tali comportamenti anomali (quali, ad esempio, sguardo non rivolto verso il *monitor*, volto mancante e così via). Al termine della prova d'esame, il sistema elaborava il video, inserendo segnali d'allerta in merito a possibili indici di comportamenti scorretti (c.d. *flag*) e attribuendo una c.d. "*review priority*", affinché il docente potesse poi valutare se effettivamente fosse stata commessa un'azione non consentita. Con riguardo ai rischi per gli interessati derivanti, sotto il profilo della protezione dei dati, dall'impiego di sistemi di supervisione del comportamento degli studenti durante le prove d'esame a distanza, il Garante ha evidenziato che tali sistemi «non devono essere indebitamente invasivi e comportare un monitoraggio dello studente eccedente le effettive necessità». Il trattamento dei dati personali degli studenti è risultato effettuato in maniera non conforme ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, minimizzazione e limitazione della conservazione, in violazione degli artt. 5, par. 1, lett. *c)* ed *e)*, e 25 del Regolamento. È emerso, inoltre, che il sistema di supervisione non si fosse limitato a inibire specifiche funzionalità dei dispositivi in uso agli studenti nel corso dello svolgimento dell'esame, ma teneva anche traccia del comportamento dello studente durante la prova (disconnessioni dalla rete Internet; tentativi di utilizzare il mouse o il trackpad per passare da un'applicazione all'altra o per uscire dal sistema; applicazioni in uso; posizione del viso dello studente), generando una pluralità di informazioni e dati personali relativi allo studente e alla sua condotta, il cui trattamento non risultava strettamente necessario per assicurare il regolare svolgimento e la validità della prova. Il titolare del trattamento, anche avvalendosi del supporto del responsabile della protezione dei dati, deve invece «fin dalla progettazione» e «per impostazione predefinita» (art. 25 del Regolamento)

Un altro tipo di diffusione illecita di dati personali, stigmatizzata dai provvedimenti dell'Autorità, concerne la materia delle sovvenzioni pubbliche. Va premesso che il Garante, fin dal 2014, ha fornito a riguardo specifiche indicazioni alle amministrazioni sulle cautele da adottare in ordine alla diffusione di dati personali[89]. In contrasto con tali indicazioni, un Comune ha pubblicato sull'albo pretorio *online* una «graduatoria definitiva degli aventi diritto» al sostegno economico per il fitto delle abitazioni principali per situazioni di emergenza socio-economica, «contenente dati personali sensibili e riservati (nome, cognome, codice fiscale, indirizzo, importo canone fitto, indicazione importo erogabile e posizione in graduatoria)». In qualità di titolare del trattamento dei dati personali, il Comune era però tenuto a mettere in atto «fin dalla progettazione», ossia al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, «misure tecniche e organizzative adeguate, (…) volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati», garantendo «che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento» (art. 25, parr. 1 e 2, GDPR)[90]. Il caso in esame riguarda, in primo luogo, il trattamento di dati personali effettuato tramite un'apposita maschera di ricerca, presente sul sito *web* istituzionale del suddetto Comune, che consentiva di

adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento), quali i principi di minimizzazione e di limitazione della conservazione di cui agli artt. 5, par. 1, lett. *c)* e *e)*, del Regolamento e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati. Nella specie, con riguardo ai tempi di conservazione delle registrazioni audio-video delle prove d'esame (ovvero cinque anni dalla data della prova, poi riformulati dall'Ateneo in dodici mesi successivamente alla contestazione amministrativa), il titolare non ha fornito le specifiche motivazioni sulla cui base si renderebbe necessaria per un così esteso lasso temporale. Il Garante, sul punto, ha sottolineato che, in ogni caso, tale periodo di conservazione non risultava proporzionato rispetto alla finalità di assicurare la regolarità delle prove d'esame, né tale ampio arco temporale poteva essere giustificato per l'ulteriore finalità legata all'utilizzo dei medesimi dati in caso di eventuali contestazioni da parte degli interessati, considerati i termini previsti dalla legge per impugnare l'esito della prova (reclamo alla commissione esaminatrice ovvero ricorso al TAR).

[89] Cfr. il provvedimento denominato «Obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici e dell'elenco dei soggetti beneficiari (artt. 26 e 27 del d. lgs. n. 33/2013)», nella parte prima, par. 9.e, del provvedimento generale n. 243 del 15 maggio 2014, recante le «Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati», in G.U. n. 134 del 12 giugno 2014.

[90] Cfr. GPDP, Provv. del 22 luglio 2021, doc. *web* n. 9696764, nei confronti del Comune di Napoli. Sempre in riferimento alla diffusione di dati personali sul sito *web* istituzionale, si può annoverare un altro provvedimento del Garante Privacy nei confronti della Regione Lombardia (GPDP, Provv. del 22 luglio 2021, doc. *web* n. 9697724). Si trattava di elenchi relativi alla selezione per l'erogazione di contributi economici per l'acquisto di libri di testo, dotazioni tecnologiche e strumenti per la didattica, oppure per l'erogazione di borse di studio, da parte dello Stato, a favore di studenti residenti in Lombardia, iscritti e frequentanti corsi presso le scuole, statali e paritarie, a condizione del rientro quotidiano dello studente alla propria residenza. È stata riconosciuta, nel caso, una diffusione di dati personali online in assenza di una idonea base normativa e in violazione del principio di minimizzazione dei dati [art. 5, par. 1, lett. *c)*, GDPR].

visualizzare – attraverso l'inserimento del solo codice fiscale, senza richiedere alcuna identificazione dell'utente – sia i dati personali dei soggetti ammessi (nominativo, posizione in graduatoria, codice fiscale, indirizzo, importo del canone, importo erogabile) che dei non ammessi al contributo per il sostegno economico relativo al fitto delle abitazioni principali per situazioni di emergenza socio-economica, con la relativa motivazione. Tale diffusione di dati personali è avvenuta: in assenza di idonei presupposti normativi, in violazione dell'art. 2-*ter*, co. 1 e 3, del Codice e dell'art. 6, par. 1, lett. *c)* ed *e)*, par. 2 e par. 3, lett. *b)*, del GDPR; nonché in contrasto con la disciplina statale in materia di trasparenza, laddove è previsto che non possano essere pubblicati i dati identificativi delle persone fisiche destinatarie di benefici economici «qualora da tali dati sia possibile ricavare informazioni relative (…) alla situazione di disagio economico-sociale degli interessati» (art. 26, co. 4, d.lgs. n. 33/2013); in violazione del principio di «minimizzazione dei dati», di cui all'art. 5, par. 1, lett. *c)*, del GDPR, in quanto i dati non sono risultati «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Non erano quindi state adottate, nel caso, secondo il Garante, «misure tecniche e organizzative» adeguate per «attuare in modo efficace i principi di protezione dei dati» fin dalla progettazione e per garantire che fossero trattati per «impostazione predefinita» solo «i dati personali necessari per ogni specifica finalità del trattamento», in violazione dell'art. 25, parr. 1 e 2, del GDPR.

Infine, un'altra fattispecie, per certo rilevante, ha riguardato gli illegittimi ripetuti accessi al dossier sanitario aziendale da parte di un operatore sanitario operante presso una struttura di riabilitazione dell'Azienda Usl della Valle d'Aosta[91], ove la reclamante non aveva mai ricevuto assistenza sanitaria, negando peraltro il consenso al trattamento dei suoi dati personali attraverso il dossier sanitario aziendale[92].

[91] Cfr. Ordinanza-ingiunzione nei confronti di Azienda Usl Valle d'Aosta (GPDP, Provv. n. 371 del 10 novembre 2022, doc *web* n. 9819792.

[92] Nelle linee guida del 2015, il Garante ha specificato che il dossier sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo. All'interessato, infatti, deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale strumento. Ciò significa che qualora l'interessato non manifesti il suo consenso al trattamento dei dati personali mediante il dossier sanitario il professionista che lo prende in cura avrà a disposizioni solo le informazioni rese in quel momento dallo stesso interessato (es. raccolta dell'anamnesi, delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista. Analogamente, in tale circostanza, il personale sanitario di reparto/ambulatorio avrà accesso solo alle informazioni relative all'episodio per il quale si è rivolto presso quella struttura l'interessato e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio (c.d. accesso agli applicativi verticali dipartimentali). Con provvedimento del 7 marzo 2019, il Garante ha individuato – a titolo esemplificativo – alcuni trattamenti in ambito sanitario per i quali è ancora necessario richiedere il consenso esplicito dell'interessato (art. 9, par. 2, lett. a) del Regolamento), tra i quali sono stati annoverati anche quelli effettuati attraverso il dossier sanitario (doc. *web* n. 9091942). Analoghe

Nell'occasione, il Garante ha stabilito che il titolare del trattamento deve mettere in opera sistemi per il controllo degli accessi anche al database per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, attraverso l'utilizzo di indicatori di anomalie (c.d. *alert*), utili per orientare successivi interventi di audit. Il titolare doveva prefigurare, quindi, l'attivazione di specifici *alert* che individuassero comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati del trattamento (es. relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi). Nel caso *de quo*, l'Azienda aveva scelto di adottare un atto amministrativo con il quale disporre la "rimozione dei filtri privacy" nel sistema informativo che gestisce il dossier sanitario aziendale, nella convinzione che tale misura avrebbe semplificato la gestione dei pazienti durante la pandemia. La rimozione dei predetti filtri aveva determinato: l'attivazione del dossier sanitario per tutti gli assistiti della Azienda, che coincidono con quelli della Regione, anche nel caso gli stessi avessero espressamente negato il consenso all'uso del dossier o non lo avessero mai prestato; la possibilità che il dossier fosse consultato, sebbene con diverse profondità di accesso, da parte di tutti gli operatori sanitari aziendali, a prescindere dal loro coinvolgimento nel percorso di cura dell'interessato. La predetta scelta aziendale, effettuata in relazione all'emergenza da Covid-19, non ha riguardato solo i pazienti affetti da tale ultima patologia, ma tutti quelli afferenti all'Azienda e alle sue articolazioni (come la struttura ove è stato effettuato l'accesso in esame) e non è stata limitata alle sole prestazioni sanitarie rese in emergenza, bensì a tutte quelle erogate dall'Azienda dal marzo del 2020 al maggio del 2022. Le predette modifiche alla configurazione del dossier aziendale hanno reso quindi possibile ad un professionista sanitario operante presso l'Azienda di accedere al dossier sanitario anche di interessati che non erano in quel momento in cura presso l'Azienda o comunque presso il titolare dell'utenza e che non avevano mai prestato il consenso al dossier (ovvero, come nel caso di specie, il consenso al dossier era stato addirittura espressamente negato) in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e f) e 9 del Regolamento, nonché del principio di protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*) (art. 25 del Regolamento).

---

violazioni sono state riscontrate per ripetuti accessi al dossier da parte di personale sanitario che, sebbene autorizzato al trattamento, non era coinvolto nel processo di cura dei soggetti a cui i dossier sanitari si riferivano. Nell'ambito delle istruttorie avviate a seguito delle notifiche di violazione e dei reclami nei confronti di alcune aziende sanitarie della Regione Friuli Venezia Giulia è emerso che tutte le aziende sanitarie appartenenti a quel servizio sanitario regionale (SSR) hanno istituito il dossier sanitario aziendale mediante l'applicativo denominato "visore referti", messo a disposizione da Insiel S.p.A. (cfr. GPDP, Provv. n. 210 del 26 maggio 2022 doc. *web* n. 9777974). Nei casi esaminati dal Garante la configurazione del dossier ha reso possibile che personale sanitario operante presso alcune aziende sanitarie regionali potesse accedere senza restrizioni al dossier sanitario di colleghi ovvero di interessati che non erano – all'atto dell'accesso – in cura presso gli stessi, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. *a)* e *f)* e 9 del Regolamento, nonché dei principi di protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*) contemplati all'art. 25 del Regolamento.

Capitolo XIII

Il principio di responsabilizzazione (*accountability*)

*Fiorella Albanese - Isabella Cardinali**

SOMMARIO: 1. Inquadramento normativo. – 2. Portata del principio. – 2.1. Il concetto di *accountability*. – 2.2. Codici etici e certificazioni. – 2.3. Ricadute applicative nel diritto positivo. – 2.4. Gli strumenti documentali e probatori espressione del principio di *accountability*. – 2.5. Le misure di "secondo livello": modelli organizzativi e nomina volontaria del DPO. – 2.6. Dalla responsabilità *ex ante* a quella *ex post*: i riflessi del principio di *accountability* sulla responsabilità civile (legittimazione passiva e prova liberatoria). – 2.7. Brevi cenni al rapporto fra *accountability* e responsabilità amministrativa. – 3. Applicazione del principio nella casistica. – 3.1. Breve premessa. – 3.2. *Accountability* e trattamento dati per finalità di *marketing*: i casi Tim S.p.a e Wind Tre S.p.a. nei provvedimenti del Garante. – 3.3. (*segue*): i casi Fastweb S.p.a. ed Edison Energia Sp.a. – 3.4. L'*accountability* al suo esordio: le prime sanzioni delle autorità di controllo degli altri Paesi dell'EU. – 4. Riflessioni conclusive.

1. Inquadramento normativo

Il principio di "*accountability*" (in italiano reso dal termine "responsabilizzazione" o "responsabilità") permea l'intero impianto normativo concepito dal Reg. UE 679/2016 del Parlamento europeo e della Commissione europea relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, noto come *General Data Protection Regulation* (nel prosieguo, per brevità, "GDPR" o "Regolamento")[1].

---

* Pur essendo lo scritto frutto di riflessione comune, i parr. 1 e 2 sono da attribuire a Fiorella Albanese, i parr. 3 e 4 sono da attribuire a Isabella Cardinali.

[1] Sul principio di *accountability* si vedano i preziosi contributi di G. MALGIERI, *Principi applicabili al trattamento dei dati personali*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* Privacy *e* Data Protection, Milano, 2021, pp. 189 ss., G. FINOCCHIARO, *GDPR tra novità e discontinuità. Il principio di* accountability, in *Giur. it.*, 2019, 12, pp. 2777 ss.; EAD., *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, pp. 1 ss.; EAD., *Il quadro d'insieme sul Regolamento Europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 1 ss.; EAD., *Approfondimento sub Commento all'articolo 24*, in A. BARBA-S. PAGLIANTINI (a cura di), *Commentario del Codice Civile, Delle Persone*, diretto da E. GABRIELLI, Milano 2019, pp. 513 ss.; F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 775 ss.; F. MOLLO, *Gli Obblighi Previsti In Funzione Di Protezione Dei Dati Personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 255 ss., D. ACHILLE, *Comm. art. 5*, in A. BARBA-S. PAGLIANTINI (a cura di), *Com-*

La ricostruzione normativa del principio muove anzitutto dall'art. 5, par. 2, ove il legislatore statuisce che «Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")»[2].

Ulteriore manifesta espressione del principio si riscontra all'art. 24 del GDPR, rubricato «*Responsabilità del titolare del trattamento*», ove si prevede innanzitutto, al par. 1, che «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario».

Nel medesimo articolo viene altresì previsto, al par. 2, che, «Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento».

Il terzo ed ultimo paragrafo dell'art. 24 stabilisce infine che «L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento».

In *pendant* con l'art. 24, da ultimo, al *considerando* 74, si prevede che «*È opportuno* stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura,

mentario del Codice Civile, cit., pp. 103 e ss.; F. CAPPARELLI, *Comm. art. 24*, in L. BOLOGNINI-E. PELINO (a cura di), *Codice della disciplina Privacy*, Milano 2019, p. 201 ss.; F. RESTA, *Comm. Art. 5*, in G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e Normativa Privacy Commentario*, Milano, 2018, pp. 49 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori,* in *Contratto e Impresa*, 2018, I, pp. 106 ss.; ID., *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale, Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 82 ss.; D. POLETTI-C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in *Ibidem*, pp. 377 ss.; E. TOSI, *La responsabilità civile per trattamento illecito dei dati personali*, in *Ibidem*, pp. 639 ss.

In generale, sul Regolamento, V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit.; G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit.

Nella letteratura straniera, C. KUNER-L.A. BYGRAVE-C. DOCKSEY, *The EU general data protection regulation (GDPR): a commentary*, Oxford, 2020; MARIUSZ KRZYSZTOFEK, *GDPR: general data protection regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union*, Alphen aan den Rijn, 2018.

[2] Nel richiamato par. 1 vengono affermati i principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche».

Non si ravvisa un precedente del principio di responsabilizzazione nella previgente disciplina europea in materia di protezione dei dati personali: l'*accountability* rappresenta infatti una novità introdotta nel diritto positivo dal GDPR[3]. Tuttavia, la Dir. 95/46/CE aveva previsto una, sia pur embrionale (e monca della componente della "responsività")[4], forma di responsabilizzazione del titolare, laddove disponeva che «*Il responsabile del trattamento*[5] è tenuto a garantire il rispetto delle disposizioni del paragrafo 1»[6] (art. 6, par. 2).

Questa previsione normativa non ha però avuto alcuna ricaduta sulle disposizioni interne di recepimento della direttiva, vale a dire la l. 31 dicembre 1996, n. 675 e, successivamente, il d.lgs. 30 giugno 2003, n. 196 e ss.mm.ii., all'interno delle quali non si trovano cenni che in alcun modo rimandino alla responsabilizzazione del titolare del trattamento per la predisposizione e implementazione di misure appropriate per garantire il rispetto dei «principi relativi alla qualità dei dati» ed, in generale, della disciplina applicabile in materia di protezione dei dati personali[7].

Sebbene il principio non abbia il suo omologo nella direttiva 95/45/CE (se non nei limiti summenzionati, peraltro neutralizzati dal mancato recepimento nelle disposizioni interne su questo spunto), tracce dell'*accountability* applicata alla *privacy*

---

[3] Si rinvia, in proposito, al documento del Gruppo di Lavoro ex Art. 29, *The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (WP- 168), 1 dicembre 2009, da cui emerge come il vecchio quadro giuridico non fosse riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducessero in meccanismi efficaci atti a fornire una protezione reale.

[4] Per "*responsività*" (traduzione letterale di *responsiveness*, capacità di dare risposte), concetto di derivazione pubblicistica, si intende la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli *stakeholder* e dalle autorità del settore.

[5] Leggasi il «titolare del trattamento». La traduzione della direttiva summenzionata utilizza un registro lessicale poi rivoluzionato con la versione italiana del GDPR. In quel contesto, difatti, il termine «*Data Controller*», oggi pacificamente traslato con la locuzione «Titolare del trattamento», veniva reso con il termine «Responsabile del trattamento», adesso invece utilizzato per rendere il concetto di «*Data Processor*».

[6] L'art. 6, par. 1, della direttiva cit. prevedeva che «1. Gli Stati membri dispongono che i dati personali devono essere:
a) trattati lealmente e lecitamente;
b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;
d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati;
e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici».

[7] Cfr., *amplius*, nota 9.

si riscontrano precedentemente all'entrata in vigore del Regolamento ed in particolare in due pareri del Gruppo di Lavoro *ex* articolo 29: (i) il parere n. 168/2009, «*Il Futuro della Privacy. Contributo congiunto alla consultazione della Commissione europea sul quadro giuridico per il diritto fondamentale alla protezione dei dati personali*», adottato l'1 dicembre 2009; (ii) il parere n. 3/2010, «*Sul Principio di responsabilità*», adottato il 13 luglio 2010[8].

L'elaborazione del Gruppo di lavoro *ex* articolo 29, espressa nei summenzionati pareri[9], ha posto delle solide basi per la concettualizzazione del principio di responsabilità nella sua accezione ancipite attuale, poi confluita nel GDPR, in virtù della quale (citando testualmente il Parere sul futuro della *privacy*), se da una parte: «(…) i titolari del trattamento dei dati sarebbero tenuti ad attuare le misure necessarie per garantire il rispetto dei principi e degli obblighi sostanziali della direttiva attuale durante il trattamento dei dati personali», anche allo scopo di « rafforzare la necessità di adottare misure efficaci che si traducano in un'efficace attuazione interna degli obblighi e dei principi sostanziali attualmente incorporati nella direttiva», dall'altra parte «il principio di responsabilità richiederebbe [altresì] ai titolari del trattamento dei dati di disporre dei meccanismi interni necessari per dimostrare la conformità alle parti interessate esterne, comprese le DPA [*Data Protection Authority*] nazionali. La conseguente necessità di fornire la prova delle misure adeguate prese per garantire la conformità faciliterà notevolmente l'applicazione delle norme applicabili»[10].

Sul versante internazionale, il primo documento a introdurre il concetto di *accountability,* sono le Linee Guida OCSE del 1980, che già all'epoca affermavano

---

[8] Nel documento si dà evidenza dei precedenti del principio di responsabilizzazione. In particolare vengono annoverate: *a)* le Linee Guida per la protezione della vita privata dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) del 1980; *b)* lo *standard* ISO/IEC 27001:2005 «Tecnologia delle informazioni – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni (SGSI o ISMS, *Information Security Management System*)», sostituito poi da ISO IEC 27001:2013 e da ultimo da ISO/IEC 27001:2017; *c)* la 31a Conferenza internazionale delle Autorità di protezione dei dati e la *privacy*, tenutasi a Madrid dal 4 al 6 novembre 2009, che ha elaborato gli *Standard* Internazionali sulla protezione dei dati e la *privacy*; *d)* la 32a Conferenza internazionale delle Autorità di protezione dati tenutasi a Gerusalemme dal 27 al 29 ottobre 2010.

[9] Nei suoi elaborati, il Gruppo di lavoro articolo 29 conferma come il principio debba considerarsi inedito; si legge infatti nel parere 3/2010 che «il Gruppo di lavoro articolo 29 ha ritenuto che l'attuale quadro giuridico non sia riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducano in meccanismi efficaci atti a fornire una protezione reale» e per tale ragione ritiene necessario introdurre la nuova disposizione sull'*accountability*. Analogamente, nel parere sul Futuro della *privacy* (parr. 78-79) viene rappresentato che «L'articolo 17, paragrafo 1, della direttiva 95/46 / CE, in una certa misura, richiede già ai titolari del trattamento l'attuazione di misure, sia di natura tecnica che organizzativa (il titolare del trattamento deve "attuare misure tecniche e organizzative adeguate per proteggere i dati personali da (...) forme di trattamento illecite"). Queste misure possono includere alcune delle misure di cui sopra. Tuttavia, in pratica l'articolo 17, paragrafo 1, non ha avuto successo nel rendere la protezione dei dati sufficientemente efficace anche nell'organizzazione, a causa dei diversi approcci adottati nelle misure nazionali di attuazione (…). Per affrontare questo problema, sarebbe opportuno introdurre nel quadro globale un principio di responsabilità».

[10] Il testo del parere sul futuro della *privacy* è disponibile solo in lingua inglese, tedesca e francese. L'estratto proposto nel testo è stato liberamente tradotto dall'a.

che «*A data controller should be accountable for complying with measures which give effect to the principles stated above*»[11].

Nessuna menzione, invece, del principio o più in generale della responsabilità del titolare del trattamento si riscontra nella prima versione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (c.d. Convenzione 108), del Consiglio d'Europa, firmata a Strasburgo, il 28 gennaio 1981.

Nel 2018, con il Protocollo emendativo[12] della predetta Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, c.d. Convenzione 108+[13], il principio di responsabilità (*accountability*) ha fatto il suo effettivo debutto anche nel diritto internazionale[14]. In particolare, all'art.

---

[11] Cfr. OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 settembre 1980, nella versione originaria, disponibile all'url https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (verificato da ultimo in data 9 aprile 2023). Il documento è stato successivamente emendato nel 2013.

[12] «*Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*», 128th Session of the Committee of Ministers, in Elsinore, Denmark, on 17-18 May 2018.

[13] Hanno firmato la Convenzione 108+, nell'ambito del Consiglio d'Europa, i seguenti paesi: Andorra; Armenia; Austria; Belgium; Bosnia and Herzegovina; Bulgaria; Croatia; Cyprus; Czech Republic; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Italy; Latvia; Liechtenstein; Lithuania; Luxembourg; Malta; Monaco; Netherlands; North Macedonia; Norway; Poland; Portugal; Romania; Russian Federation; San Marino; Serbia; Slovak Republic; Slovenia; Spain; Sweden; Switzerland; United Kingdom.
Dei paesi menzionati, hanno già provveduto alla ratifica soltanto: Bulgaria; Croatia; Cyprus; Estonia; Lithuania; Malta; Poland; Serbia. Per ora, fra i paesi del Consiglio d'Europa che non hanno sottoscritto la Convenzione 108+ figurano: Albania; Azerbaijan; Denmark; Georgia, Liechtenstein; Montenegro; Republic of Moldavia; Turkey; Uckraine. Fra i paesi estranei al Consiglio d'Europa, hanno sottoscritto il protocollo: Argentina; Mauritius (l'unico stato ad avere già ratificato); Tunisia; Uruguay. La lista aggiornata è disponibile all'indirizzo: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (consultato da ultimo in data 18 dicembre 2020).

[14] Invero, oltre alle linee guida OCSE, almeno altri quattro documenti (tre dei quali citati alla nota 8) di tenore internazionale, precedenti al Protocollo emendativo, menzionano l'*accountability* in materia di trattamento dei dati. Ci si riferisce:
(i) agli *standard* ISO IEC 27001:2005;
(ii) alla Conferenza Internazionale di Madrid del 2009, che, *sub* par. 11 (rubricato "Principio di responsabilità [*accountability*]") rileva come «Il titolare
a. Adotta tutte le misure necessarie all'osservanza dei principi e degli obblighi fissati nel presente documento e nelle norme nazionali applicabili, e
b. Implementa tutti i meccanismi interni necessari a dimostrare tale osservanza sia agli interessati sia alle autorità di controllo nell'esercizio dei rispettivi poteri, secondo quanto stabilito dall'articolo 23»
(iii) alla Conferenza Internazionale di Gerusalemme del 2010;
(iv) al *Privacy Framework* dell'APEC (Cooperazione Economica Asiatico-Pacifica), pubblicato nel 2015, ai sensi del quale (par. 32, rubricato «*Responsabilità*») «Un titolare del trattamento dei dati personali dovrebbe essere responsabile del rispetto delle misure che danno effetto ai Principi sopra indicati. Quando le informazioni personali devono essere trasferite a un'altra persona o organizzazione, a livello nazionale o internazionale, il titolare del trattamento delle informazioni personali deve ottenere il consenso dell'individuo o esercitare la dovuta diligenza e adottare misure ragionevoli per garantire che la persona o l'organizzazione ricevente protegga le informazioni in modo coerente con questi principi». Nel commento al par. 32 si aggiunge che «Modelli di *business* efficienti ed

10, rubricato «*Obblighi aggiuntivi*», la Convenzione prevede che: «1. Ciascuna Parte provvede affinché i titolari del trattamento e ove applicabile, i responsabili del trattamento, adottino tutte le misure appropriate per adempiere agli obblighi della presente Convenzione ed essere in grado di dimostrare, fatta salva la legislazione nazionale adottata ai sensi dell'articolo 11, paragrafo 3, in particolare all'autorità di controllo competente di cui all'articolo 15 , che il trattamento dei dati sotto il loro controllo è conforme alle disposizioni della presente Convenzione.

2. Ciascuna Parte provvede affinché i titolari del trattamento e, ove applicabile, i responsabili, esaminino il probabile impatto del previsto trattamento dei dati sui diritti e sulle libertà fondamentali degli interessati prima dell'inizio di tale trattamento e concepisca in origine il trattamento dei dati in modo da prevenire o ridurre al minimo il rischio di interferenza con tali diritti e libertà fondamentali.

3. Ciascuna Parte provvede affinché i titolari del trattamento e, ove applicabile, i responsabili del trattamento mettano in atto misure tecniche e organizzative che tengano conto delle implicazioni del diritto alla protezione dei dati personali in tutte le fasi del trattamento dei dati.

4. Ciascuna Parte, tenendo conto dei rischi derivanti per gli interessi, dei diritti e delle libertà fondamentali degli interessati, può adattare l'applicazione delle disposizioni dei paragrafi 1, 2 e 3 nella legge che dà effetto alle disposizioni della presente Convenzione, in base alla natura e al volume dei dati, alla natura, alla portata e allo scopo del trattamento e, se del caso, alle dimensioni del titolare del trattamento o del responsabile del trattamento»[15].

---

economici spesso richiedono trasferimenti di informazioni tra diversi tipi di organizzazioni in luoghi diversi con rapporti diversi. Durante il trasferimento delle informazioni, i titolari del trattamento delle informazioni personali dovrebbero essere responsabili nel garantire che il destinatario proteggerà le informazioni in modo coerente con questi Principi quando non ottiene il consenso. Pertanto, i titolari del trattamento delle informazioni dovrebbero adottare misure ragionevoli per garantire che le informazioni siano protette, in conformità con questi principi, dopo il trasferimento. Ci sono alcune situazioni in cui tale *due diligence* può essere impraticabile o impossibile, ad esempio, quando non esiste una relazione in corso tra il titolare del trattamento delle informazioni personali e la terza parte a cui vengono divulgate le informazioni. In questi tipi di circostanze, i titolari del trattamento delle informazioni personali possono scegliere di utilizzare altri mezzi, come ottenere il consenso, per garantire che le informazioni siano protette in modo coerente con questi principi.

Tuttavia, nei casi in cui la divulgazione sia richiesta dalla legge nazionale, il titolare del trattamento dei dati personali sarebbe esonerato da qualsiasi obbligo di dovuta diligenza o consenso. Un mezzo utile per un titolare del trattamento delle informazioni personali per contribuire a garantire la responsabilità per le informazioni personali che detiene è disporre un programma di gestione della *privacy*».

Rispetto ai summenzionati documenti, la Convenzione 108+ si caratterizza non soltanto per l'accuratezza e il dettaglio con cui è tracciato il principio di responsabilità (che ad esempio nelle linee guida OCSE ha la stessa limitatezza che si riscontra nella direttiva 95/45/CE), ma altresì per l'estensione della platea dei sottoscrittori (va ricordato che gli Standard ISO IEC non sono vincolanti e che le risoluzioni di Madrid e di Gerusalemme riguardano principalmente stati membri e solo pochissimi stati extra UE).

[15] Il testo del Protocollo emendativo è disponibile, in versione integrale, all'indirizzo Internet seguente: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (verificato da ultimo in data 9 aprile 2023), in lingua inglese e francese; l'estratto è una traduzione, non ufficiale, proposta dall'a.

Tra le novità delineate dalla Convenzione 108+, rispetto al regolamento europeo, si nota l'estensione del principio di responsabilizzazione anche ai responsabili del trattamento, mentre il GDPR rivolge l'art. 24 al solo titolare del trattamento.

2. Portata del principio

2.1. Il concetto di *accountability*

Come già rilevato, l'*accoutability* ha una natura ancipite, sostanziandosi di due fondamentali componenti: assicurare l'efficace attuazione dei principi posti a presidio del trattamento dei dati personali (e prospettati al par. 1 dell'art. 5), oltre che dell'intero regolamento (v. art. 24, par. 1), da una parte, e comprovare tale adempimento, dall'altra.

La precedente disciplina normativa nazionale in materia di tutela dei dati personali adottava un approccio incardinato su adempimenti specifici, scolpiti all'interno di prescrizioni dettagliate (*ex multis*, le misure minime di sicurezza elencate nell'All. B al d.lgs. 196/2003, «*Disciplinare tecnico in materia di misure minime di sicurezza*», poi abrogato). Il radicale cambio di paradigma eletto dal GDPR abbandona il sicuro tracciato degli adempimenti tipizzati e sposta sul titolare "l'onore e l'onere" di scegliere soluzioni adeguate al caso di specie, capaci di realizzare l'efficace concretizzazione dei presidi di *data protection*.

Nella scelta degli strumenti (*rectius*: misure, organizzative e di sicurezza) atti a erigere un assetto *compliant* con i principi e gli obblighi sanciti dal Regolamento, il titolare deve tenere conto: i) della natura, ii) dell'ambito di applicazione, iii) del contesto e iv) delle finalità del trattamento, v) nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

La valutazione prodromica alla scelta delle misure organizzative e di sicurezza adeguate, richiesta dal GDPR al titolare, muove da un'accurata mappatura dei flussi dei dati raccolti e trattati[16] e, loro tramite, approda all'identificazione ed elencazione delle fonti di rischio per i diritti e le libertà degli interessati (c.d. analisi del rischio).

Sulla base di queste premesse, il titolare individua le misure "adeguate" a contenere i rischi derivanti dai trattamenti effettuati e dunque a neutralizzarne le fonti.

L'adeguatezza è da parametrarsi, oltre che sul contesto desumibile dall'analisi del rischio summenzionata, anche sullo stato dell'arte e della conoscenza tecnica vigente.

Il procedimento che porta all'individuazione e poi all'implementazione delle misure organizzative e di sicurezza deve essere documentato, al duplice scopo di attestare l'attenta ponderazione che si sostanzia nell'analisi degli elementi oggettivi

[16] Natura, ambito di applicazione, contesto e finalità del trattamento presuppongono, a monte, una classificazione dei dati: per tipologia e finalità di trattamento, per categorie di dati trattati, per categorie di interessati, per categoria di soggetti esterni all'organizzazione del titolare a cui i dati vengono trasmessi.

presi in considerazione nel procedimento valutativo preliminare effettuato e di rendere tale attività conoscibile e verificabile in caso di controllo[17]; la procedimentalizzazione consente al titolare di essere in grado di dimostrare di avere posto in essere gli adempimenti necessari per l'attuazione dei principi elencati al par. 1 dell'art. 5 GDPR.

Se questa nuova prospettiva introdotta dal legislatore europeo ha il pregio di valorizzare la libertà di scelta del titolare (e, ove applicabile, del responsabile, in base alla Convenzione 108+), che può attingere oggi a una moltitudine di soluzioni e declinarle, a suo piacimento, all'interno della propria realtà aziendale/professionale, essa al contempo lo disorienta, ponendolo innanzi a delle scelte che, per quanto caute e ponderate, mantengono un'alea ineliminabile di incertezza, attesa l'assenza di parametri tipizzati e soprattutto di un contesto normativo ordinato e chiaro[18].

2.2. Codici etici e certificazioni

L'imbarazzo delle scelte addossate sul titolare può essere, in qualche misura, attenuato dall'eventuale adesione del medesimo a codici di condotta (art. 40 GDPR) o a meccanismi di certificazione (art. 42 GDPR)[19]. Questi strumenti regolamentari non sono stati ancora completamente implementati.

Nel 2019 sono stati approvati i primi codici di condotta (si trattava del codice in materia di «informazioni commerciali»[20] e di quello riguardante i «sistemi infor-

[17] Riferisce della componente procedimentale del principio di *accountability*, G. ARCELLA, *GDPR: il registro delle attività di trattamento e le misure di accountability*, in *Notariato*, 2018, 4, p. 393.
Questa faccia del principio rimanda all'alveo originario in cui si è sviluppato in concetto di *accountability*: il diritto pubblico amministrativo; nella sua accezione di "rendere conto" delle scelte operate, il principio rivela un intenso legame con quello della trasparenza amministrativa.

[18] La materia della protezione dei dati è frammentata, stratificata e multidisciplinare. Convivono fonti del diritto propriamente dette (es.: il regolamento europeo, il codice in materia di protezione dei dati personali adottato con decreto legislativo) ed un profluvio di documenti di prassi (es.: linee guida, pareri), molti dei quali non disponibili in lingua italiana, riconducibili ad autorità diverse, nazionali e sovranazionali (Gruppo di lavoro *ex* Art. 29, EDPB, autorità di controllo nazionale) e materie poliedriche alle volte molto tecniche (si pensi, ad esempio, alla disciplina dell'amministratore di sistema), la cui approfondita conoscenza è da considerarsi ardua anche per un operatore qualificato del diritto. Il tema è tanto più accentuato per le realtà medio piccole (c.d. PMI), attesa l'evidente non intellegibilità della materia, le quali non godono delle medesime risorse delle grandi realtà economiche da destinare alla creazione di competenze qualificate e specifiche in materia di protezione dei dati personali.

[19] Per un approfondimento del tema si rinvia ai contributi di A.R. PEPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati*, cit., pp. 367 ss.; S. SILEONI, *I codici di condotta e le funzioni di certificazione*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 917; R. D'ORAZIO, *Comm. art. 40*, in A. BARBA-S. PAGLIANTINI (a cura di) *Commentario del Codice Civile, Delle Persone*, cit., p. 807; R. TUCCILLO, *Comm. art. 41*, in *Ibidem*, p. 827; F. BIANCA, *Comm art. 42*, in *Ibidem*, p. 837.
I codici di condotta non vanno confusi con le cinque regole deontologiche ad oggi vigenti, soggette alla diversa disciplina di cui agli artt. 2-*quater* del Codice *privacy* e 20 del d.lgs. 10 agosto 2018 n. 101.

[20] Che sostituisce il precedente Codice di deontologia e buona condotta per il trattamento dei dati personali effettuato ai fini di informazioni commerciali (Allegato 7 del Codice *Privacy*), in vigore dal 1° ottobre 2016.

mativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti»[21]). Il Garante ha subordinato l'efficacia di codici di condotta approvati al completamento della fase di accreditamento del relativo organismo di monitoraggio. Oltre un anno dopo, con il provvedimento n. 98 del 10 giugno 2020, sono stati definiti dapprima i «Requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta» e, successivamente, con il provvedimento n. 148 del 29 luglio 2020, i «Requisiti di accreditamento aggiuntivi».

Ad oggi sul sito del Garante sono stati predisposti due registri, uno dedicato ai codici di condotta approvati dal Garante e l'altro dedicato ai codici di condotta del Comitato Europeo per la Protezione dei Dati Personali[22].

Sul versante invece dei meccanismi di certificazione, dopo aver stipulato, in data 20 marzo 2019, con Accredia, l'Ente nazionale di accreditamento, una convenzione tesa a favorire lo scambio di informazioni, nonché a valorizzare le reciproche competenze, in rapporto alle attività di accreditamento e certificazione, il Garante per la protezione dei dati personali, con provvedimento n. 148, del 29 luglio 2020, ha approvato i requisiti aggiuntivi di accreditamento degli organismi di certificazione[23]. Allo stato, non risulta ancora l'accreditamento ufficiale di alcun ente in materia di trattamento dei dati personali: il percorso, quindi, che porterà all'elaborazione degli *standard* di certificazione[24] dei processi o dei servizi di trattamento dei dai personali non può considerarsi a tutti gli effetti completato[25].

---

[21] Che ha solo leggermente modificato il previgente Codice di deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (Allegato 5 del Codice *Privacy*), in vigore dal 1° gennaio 2005.

[22] Disponibili all'url: https://www.gpdp.it/codici-di-condotta (verificata da ultimo in data 9 aprile 2023).

[23] I requisiti si intendono aggiuntivi rispetto alla norma EN-ISO/IEC 17065:2012, «*Valutazione della conformità. Requisiti per organismi che certificano prodotti, processi e servizi*».

[24] Gli schemi di certificazione che verranno approvati saranno disponibili sul registro europeo dei meccanismi di certificazione, sigilli e marchi accessibile alla seguente URL (verificato da ultimo in data 9 aprile 2023): https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en (Accredia, Circolare Informativa DC N° 18/2020 – Accreditamento ai sensi dell'art. 43 par. 1, del Reg. UE n. 2016/679 e dell'art. 2-*septiesdecies* del d. lgs. n. 196/2003, del 16 ottobre 2020).

[25] Lo *standard* internazionale (ma non ufficiale in quanto privo del sugello dell'autorità garante in materia di protezione dei dati personali) comunque ad oggi utilizzato in materia di trattamento dei dati personali, è il menzionato UNI CEI EN ISO/IEC 27001:2017 «*Tecnologie Informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazione – Requisiti*».
Ulteriore strumento per guidare il processo di *compliance* di titolari e responsabili, è stato proposto dall'ente. Invero, che ha elaborato lo schema ISDP 10003:2018, «*Requisiti e regole di controllo per la certificazione dei processi di trattamenti con riguardo alla valutazione del rispetto dei diritti fondamentali delle persone fisiche e della libera circolazione dei dati*». In particolare l'ambito di applicazione di quest'ultimo schema può essere generale, vale a dire volto ad attestare la conformità, a tutto tondo, del titolare e/o del responsabile ai principi e alle norme in materia di protezione dei dati, ma può (alternativamente o in aggiunta) riguardare la conformità di uno o più specifici processi, prodotti e/o servizi del titolare/responsabile al regolamento in materia di trattamento dei dati personali. Sul sito di Accredia, all'URL https://www.accredia.it/certificazioni-oggi/ (da ultimo verificato in data 9 aprile 2023) si legge: «Le certificazioni rilasciate dagli organismi accreditati non sono ancora riconosciute dal Garante per la Protezione dei Dati Personali (GPDP) ai sensi del GDPR,

Attraverso regole comuni di condotta e *standard* oggettivi, in futuro, quando l'attuazione del capo IV sezione 5 del GDPR sarà esaustiva, le decisioni di titolari potrebbero essere semplificate in quanto orientate da istruzioni pragmatiche che daranno contenuto e concretezza ai concetti duttili e astratti entro cui orbita il principio di *accountability*[26]. In generale, l'adesione a questi strumenti costituisce elemento valevole a dimostrare – anche se solamente in via presuntiva – il rispetto degli obblighi da parte di titolare e/o responsabile del trattamento (art. 24, par. 3), ovvero la sussistenza di misure tecniche e organizzative adeguate a garantire la sicurezza (art. 32, par. 3). Ancora: costituisce una "garanzia adeguata" nell'ipotesi di trasferimento dei dati verso paesi terzi (art. 46, par. 2); nell'ambito della valutazione d'impatto è un elemento da tenere in debita considerazione (art. 35, par. 8)[27]; nel contesto della responsabilità amministrativa, costituisce circostanza "attenuante" della sanzione eventualmente comminata [art. 83, par. 2 lett. *j)*].

In attesa dell'elaborazione ed implementazione di questi codici e *standard*, le autorità di controllo, anche attraverso lo specifico ufficio di coordinamento del Comitato europeo per la protezione dei dati, suppliscono attraverso la pubblicazione di linee guida, orientamenti generali e di decisioni puntuali sui modelli applicati dai soggetti del trattamento.

In particolare, merita menzione l'*Accountability Framework* predisposto dall'autorità di controllo del Regno Unito (ICO), che mette a disposizione dell'operatore una sorta di "guida" per il corretto adempimento dei principi a presidio del trattamento dei dati[28].

2.3. Ricadute applicative nel diritto positivo

Le norme analizzate nel par. 1 (artt. 5 e 24 GDPR) non esauriscono la trattazione del principio di *accountability*; esso innerva l'intero *corpus* normativo del GDPR[29], giacché lo si riscontra in tutte le disposizioni che, lasciando margini di di-

---

ma sono riconosciute dal mercato come una garanzia e un atto di diligenza dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme del Regolamento. Non esiste pertanto alcuna "esimenza" giuridica rispetto alle possibili sanzioni e imputazioni di colpevolezza che possono derivare da illeciti come, per esempio, un Data Breach o la mancata liceità di un trattamento».

[26] Cfr. par. 2.3.

[27] Vale solo per l'adesione ai codici di condotta.

[28] L'*Accountability Framework* dell'autorità di controllo britannica (ICO) è consultabile *online* all'indirizzo seguente: https://ico.org.uk/for-organisations/accountability-framework/ (verificato da ultimo in data 9 aprile 2023).
Seppure riferiti ad aspetti più specifici, è utile richiamare altresì il *tool* per la DPIA predisposto dal CNIL, alla cui realizzazione ha partecipato anche il nostro Garante per la protezione dei dati personali.

[29] Il concetto è reso in modo elegante da SIANO, *Comm all'art. 24*, cit.: «Senza dubbio si è innanzi a una norma dal contenuto assai ampio (nei *fora* internazionali di *data protection* si parla di "*overarching concept of accountability*", dove *overarching* sta proprio a indicare la portata globale dell'obbligo di responsabilità) che in sé contempla: l'obbligo di mettere in atto misure che rendano ogni trattamento effettuato come conforme (*compliant*) alle previsioni del GDPR; l'obbligo che le misure adottate forniscano la garanzia di detta conformità; l'obbligo di fondare la scelta delle misure adottate su preventive analisi dei rischi; l'obbligo che la conformità così garantita sia anche facilmente

screzionalità – generalmente espressi da concetti fumosi come quello di adeguatezza, sufficienza, appropriatezza –, rimettono al titolare (e/o al responsabile, che opera per conto del titolare) delle scelte, di cui costui dovrà poi rispondere nei confronti degli interessati e delle autorità di controllo. Di seguito si tenterà di compendiare le norme nelle quali il principio di responsabilizzazione si sostanzia.

Rientra nell'alveo delle disposizioni in cui si manifesta il principio di responsabilizzazione anzitutto l'art. 25[30], che pone in capo al titolare doveri di protezione dei dati personali sin dalla progettazione di un trattamento (c.d. *privacy by design*)[31] e per impostazione predefinita (c.d. *privacy by default*)[32].

---

dimostrabile (*in primis* alle Autorità di protezione dati europee), di fatto imponendo un obbligo di rendicontazione».

[30] Sul rapporto fra *accountability* e art. 25, si vedano G. Finocchiaro, *GDPR tra novità e discontinuità*, cit., p. 2777; E. Faccioli-M. Cassaro, *Il "Gdpr" e la normativa di armonizzazione nazionale alla luce dei principi:* Accountability *e* Privacy By Design, in *Dir. ind.*, 2018, 6, p. 561.
Il rapporto intercorrente fra i due principi è evidenziato altresì dall'art. 10.3 della Convenzione 108+ di cui, di seguito, si propone stralcio del Commento: «89. Il paragrafo 3 specifica che, al fine di garantire un livello di protezione efficace, i titolari del trattamento e, ove applicabile, i responsabili del trattamento, dovrebbero garantire che i requisiti di protezione dei dati siano integrati il prima possibile, vale a dire idealmente nella fase dell'architettura e del sistema design, nelle operazioni di trattamento dei dati attraverso misure tecniche e organizzative (*Data Protection by design*). Questa attuazione dei requisiti di protezione dei dati dovrebbe essere raggiunta non solo per quanto riguarda la tecnologia utilizzata per il trattamento dei dati, ma anche i relativi processi di lavoro e di gestione. Dovrebbero essere messe in atto funzionalità di semplice utilizzo che facilitano la conformità alla legge applicabile. Ad esempio, l'accesso online sicuro ai propri dati dovrebbe essere offerto agli interessati ove possibile e pertinente. Dovrebbero esserci anche strumenti di agevole utilizzo per consentire agli interessati di portare i propri dati a un altro fornitore, di loro scelta, o di conservare i dati stessi (strumenti di portabilità dei dati)».

[31] L'art. 25, par., 1, GDPR stabilisce che, «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».
La norma richiama, nel testo, un contenuto similare a quello di cui all'art. 24, precisando che le valutazioni che riguardano la scelta delle misure organizzative e di sicurezza da apprestare vanno effettuate sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso. Sono invece del tutto peculiari, in quanto non presenti nel testo di cui all'art. 24: il richiamo allo «stato dell'arte» e ai «costi di attuazione», nonché il cenno esemplificativo alla «pseudonimizzazione» (come misura tecnica e organizzativa) e alla «minimizzazione» (quale principio da attuare).
Altro elemento di diversificazione rispetto all'art. 24, si ravvisa nel richiamo fatto dall'art. 25, ai soli meccanismi di certificazione *ex* art. 42, quali elementi per dimostrare la conformità ai requisiti di cui ai parr. 1 e 2 dell'art. 25.

[32] L'art. 25, par. 2, GDPR stabilisce che «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

Analogamente, l'art. 32[33] stabilisce che, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: *a)* la pseudonimizzazione e la cifratura dei dati personali; *b)* la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; *c)* la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (c.d. *business continuity* e *disaster recovery*); *d)* una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (c.d. *vulnerability assessment* e *penetration test*)[34].

La norma disciplina un ulteriore obbligo per il titolare e il responsabile del trattamento, prevedendo che chiunque agisca sotto la loro autorità, e abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso dal titolare del trattamento (par. 4), in questo modo stabilendo l'obbligo di predisporre idonei piani formativi e *policy* interne in grado di assicurare un adeguato livello di consapevolezza dei dipendenti e dei collaboratori interni[35].

Un'espressione del principio di responsabilità è ravvisabile nell'art. 28, non soltanto per quanto attiene agli espetti che riguardano la contrattualizzazione del rapporto con i fornitori[36], ma altresì con riguardo alla fase prodromica, allorquando stabilisce che il titolare «ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato» (par. 1), in questo modo configurando, per la fase che precede la nomina (in un'ottica *by design*), una responsabilità per *culpa in eligendo* a carico del titolare che non abbia selezionato con accortezza i fornitori

---

Il rapporto intercorrente fra *accountability* e *protection by default* è evidenziato dall'art. 10.3 della Convenzione 108+ di cui, di seguito, si propone stralcio del Commento: «Quando si stabiliscono i requisiti tecnici delle impostazioni predefinite, i titolari del trattamento e i responsabili del trattamento dovrebbero scegliere configurazioni standard rispettose della *privacy* in modo che l'utilizzo di applicazioni e *software* non violi i diritti degli interessati (protezione dei dati per impostazione predefinita), in particolare per evitare di elaborare più dati del necessario per il raggiungimento dello scopo legittimo. Ad esempio, i *social network* dovrebbero essere configurati di *default* in modo da condividere post o immagini solo con cerchie ristrette e scelte e non in tutta internet. (…) Il paragrafo 4 consente alle Parti di adattare gli obblighi aggiuntivi elencati nei paragrafi da 1 a 3 tenendo conto dei rischi in gioco per gli interessi, i diritti e le libertà fondamentali degli interessati».

[33] Sul tema si veda il contributo di F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., pp. 804 ss.

[34] La norma prosegue (par. 2) rilevando come la valutazione dell'adeguato livello di sicurezza debba tenere conto, in special modo, dei rischi presentati dal trattamento che derivino dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

[35] Il dovere di istruzione dei soggetti che agiscano sotto l'autorità del titolare e del responsabile del trattamento lo si riscontra altresì *sub* art. 29.

[36] Aspetto per cui si rinvia al par. successivo.

cui affidare in *outsourcing* servizi che comportino il trattamento di dati personali; responsabilità che si protrae per tutta la durata del rapporto con il fornitore/responsabile del trattamento, assumendo i connotati della *culpa in vigilando*, mediante la previsione di un obbligo di controllo cui lo stesso responsabile è tenuto a soggiacere mettendo «a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consent[endo] e contribu[endo] alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato» [art. 28, par. 3, lett. *h)*].

Il principio di *accountability* affiora anche in altra disposizione del GDPR. All'art. 13, par. 1, lett. *f)*, è previsto che, ove i dati personali vengano trasferiti fuori dall'Unione Europea, il titolare deve informare l'interessato, «indicando l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili». Se poi il paese terzo non sia coperto da una decisione di adeguatezza, «il titolare del trattamento o il responsabile del trattamento dovrebbe[ro] provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate da un'autorità di controllo o clausole contrattuali autorizzate da un'autorità di controllo»[37]. L'adempimento alle disposizioni testé menzionate risulta tutt'altro che agevole, atteso che gli strumenti di cui il titolare, il responsabile e i sub-responsabili si avvalgano (*tool*, applicazioni, *software* finalizzati a fornire sistemi di archiviazione *clouds*, piattaforme di trasferimento di documenti, servizi di *hosting*, caselle di posta, etc.) sempre più spesso utilizzano *server* ubicati fuori dall'Unione Europea e in alcuni casi addirittura "in tutto il mondo" (cfr., *ex multis*, le *policy privacy* di Microsoft e Google), in questo modo rendendo praticamente impossibile, oltre che l'ossequio,

[37] *Sic, considerando* n. 108 GDPR.

da parte del titolare, alla chiarezza dell'informativa sul punto di cui all'art. 13, par. 1 lett. *f)*[38], anche quello al disposto di cui agli artt. 28, 30[39] e 46 e ss.[40].

Altra disposizione normativa in cui emerge il principio di *accountability* è di carattere generale ed è contenuta nell'art. 12 GDPR, ove è stabilito che il titolare adotta «le misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 e le comunicazioni di cui agli artt. da 15 a 22», in questo modo rimettendo al titolare la concreta individuazione delle modalità attraverso cui portare a conoscenza degli interessati i contenuti summenzionati (informativa e diritti dell'interessato).

Si tratta di disposizione che si ricollega anche al principio di *accountability* nell'ambito della valutazione del legittimo interesse quale condizione di liceità del trattamento dei dati personali, alternativa al consenso dell'interessato per il trattamento di dati personali non appartenenti a categorie particolari[41].

A tal riguardo va rimarcato, infatti, che il titolare deve individuare le basi giuridiche a copertura dei trattamenti effettuati, dandone atto nell'informativa [art. 13, par. 1, lett. *c)*]; se il trattamento tuttavia si basa su un legittimo interesse del titolare

[38] Giacché ovviamente il trasferimento a un paese terzo operato da un fornitore si riflette sul titolare per conto del quale tratta i dati, difatti «Il titolare del trattamento (…) nell'utilizzo di soluzioni di *cloud computing*, deve essere particolarmente vigile con riguardo all'effettiva localizzazione dei servizi richiesti, adottando nel caso gli opportuni strumenti giuridici posti a legittimazione di un trattamento extra europeo di dati personali. Ciò soprattutto in considerazione del fatto che, con il nuovo regolamento, il principio di *accountability* pone in capo ai titolari un regime di responsabilità rafforzato nei confronti non solo dei trasferimenti di dati per così dire diretti, ma anche di quelli che potrebbero successivamente essere posti in essere dal soggetto terzo verso altri Paesi terzi od organizzazioni internazionali». Così M.C. MENEGHETTI, *Trasferimenti di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 438.

[39] Nella compilazione del registro dei trattamenti, sia il titolare che il responsabile – ai sensi dell'art. 30, par. 1, lett. *e)* e dell'art. 30, par. 2, lett. *c)* – devono dare conto dei «trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate». Cfr., *amplius*, par. successivo.

[40] Si osserva che le norme vincolanti d'impresa, le clausole tipo adottate dalla Commissione o da un'autorità di controllo e le clausole contrattuali autorizzate da un'autorità di controllo vanno applicate al rapporto fra il soggetto che trasferisce i dati extra UE e quello che li riceve e pertanto riguardano, nelle ipotesi di più frequente verificazione, il fornitore di servizi per l'archiviazione e/o il trasferimento di dati. Ciò comporta la tendenziale carenza di controllo, da parte del soggetto fruitore del servizio (titolare e/o responsabile/subresponsabile), cui non resta altra scelta che rinunciare alla *compliance* oppure cambiare fornitore, con la conseguenza che nei casi meno gravi tali soggetti subiranno i disagi e le spese connesse alla sostituzione degli strumenti e alla riorganizzare della propria struttura e, nei casi più gravi dovranno fare a meno servizio (erogato dal solo fornitore "inaffidabile"), ingessando la propria organizzazione.
Un'applicazione diffusa del GDPR dovrebbe portare alla neutralizzazione del problema, tuttavia non si può non rilevare come a ben cinque anni dalla vincolatività del Regolamento non si ravvisi una sensibilizzazione diffusa, anche da parte dei colossi dei servizi di *hosting*, di *files-sharing*, di archiviazione, di *webinair*, di posta elettronica, etc.

[41] Si veda, in materia, F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 110 ss.

o di terzi, nell'informativa occorre rappresentare di quali legittimi interessi si tratti [art. 13, par. 1, lett. *d)*]. In particolare, il ricorso all'interesse legittimo del titolare del trattamento o di terzi costituisce una valida base giuridica del trattamento solo «a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore» [art. 6, par. 1, lett. *f)*]. Questo bilanciamento fra interessi spetta al titolare e muove dal fondamentale postulato, di cui al *considerando* 4, secondo cui «Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[42]. Il legislatore europeo, volendo favorire l'applicazione del principio di proporzionalità in tale contesto, individua alcune fattispecie di interesse legittimo del titolare che giustifica il trattamento dei dati dell'interessato, ad esempio nelle ipotesi: i) di *marketing* diretto (*considerando* 47); ii) di prevenzione delle frodi (*considerando* 47); iii) di trasmissione dei dati all'interno del gruppo imprenditoriale a fini amministrativi interni (*considerando* 48); iv) di trattamenti di dati personali relativi al traffico di rete, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza (*considerando* 49).

Nella prassi, emergente dai provvedimenti del Garante[43], ricorrono poi le ipotesi v) della videosorveglianza; vi) della localizzazione dei lavoratori (*smartphone*, GPS); vii) dei sistemi di autenticazione che prevedano l'utilizzo di dati biometrici di collaboratori e dipendenti.

Anche nelle ipotesi in cui ricorrano le casistiche delineate dal legislatore europeo ovvero avallate da provvedimenti delle autorità di controllo, il titolare è tenuto

[42] *Considerando* 4. Cfr. altresì Gruppo di lavoro ex Art. 29, Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'art. 7 della direttiva 95/46/CE (WP217). Il bilanciamento degli interessi di norma si svolge prima che il trattamento venga effettuato (nella fase di progettazione/*by design* dell'organizzazione *privacy*), v'è tuttavia un'ipotesi in cui siffatto bilanciamento è richiesto anche in un momento successivo. Si tratta del caso di esercizio del diritto di opposizione al trattamento dei dati, da parte dell'interessato, ai sensi dell'art. 21 par 1. Nelle more di questo bilanciamento, all'interessato è consentito esercitare il diritto di limitazione dei trattamenti oggetto di opposizione, ai sensi dell'art. 20.

[43] Numerosi provvedimenti sono stati emessi dal Garante e dal Gruppo di lavoro ex Art. 29 in materia di videosorveglianza e geolocalizzazione, sia con riguardo al profilo delle finalità per cui i trattamenti vengono effettuati sia con riguardo alla durata della conservazione dei dati personali raccolti. Cfr. *ex multis* Gruppo di lavoro ex Art. 29, Parere 6/2014, cit.; GPDP, Provv. 4.10.2011, n. 370, nel quale viene rilevata l'importanza: «nel rispetto del principio di necessità, che la posizione del veicolo non sia di regola monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite».

a rispettare i principi di proporzionalità e di minimizzazione, che sovente hanno portato all'esclusione, ovvero alla limitazione (circondandoli di cautele) di questi trattamenti[44].

Al titolare e al responsabile del trattamento spetta poi verificare la ricorrenza delle circostanze che rendono obbligatoria la nomina di un Responsabile della Protezione dei dati (DPO) ai sensi dell'art. 37[45] e/o procedere a una valutazione di impatto (DPIA) ai sensi dell'art. 35[46]; verifica, questa, tutt'altro che banale, atteso l'impiego di concetti sdrucciolevoli quali «larga scala», «monitoraggio regolare e sistematico», possibilità di un «rischio elevato» per i diritti e le libertà degli interessati.

Ulteriori valutazioni[47] vengono poi richieste nel caso in cui si verifichi una violazione di dati personali, ai sensi degli art. 33 e 34 GDPR, giacché solo ove «sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche» (art. 33) il titolare/responsabile sarà esentato dal notifi-

---

[44] Cfr. nota precedente.

[45] Vale a dire, ai sensi dell'art. 37, ove:
– il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
– le attività principali del titolare/responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
– le attività principali del titolare/responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali *ex* art. 9 o di dati relativi a condanne penali e a reati *ex* art. 10.

[46] Ai sensi dell'art. 35, in particolare quando:
– un tipo di trattamento prevede in particolare l'uso di nuove tecnologie e considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
– il trattamento si sostanzia in una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
– il trattamento è effettuato su larga scala ed ha ad oggetto categorie particolari di dati personali *ex* art. 9, par. 1, o di dati relativi a condanne penali e a reati *ex* art. 10; o
– il titolare proceda alla sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Preme richiamare un interessante passo del documento del GRUPPO DI LAVORO EX ART. 29, Linee guida sui responsabili della protezione dei dati, del 13 dicembre 2016 (emendate il 5 aprile 2017): «Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il Gruppo di lavoro raccomanda a titolari del trattamento e responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti. Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i titolari del trattamento o i responsabili del trattamento intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'articolo 37, paragrafo 1».

[47] Cfr. sul tema, A. SPANGARO, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, in *Dir. mercato tec.*, 2018. Nella prassi, si veda anche GRUPPO DI LAVORO EX ART. 29, *Linee guida in materia di notifica del* data breach, adottate il 3 ottobre 2017 – WP 250.
Il Garante in materia di trattamento dei dati personali ha di recente predisposto un *tool* per il *self assessment* del *data breach*, disponibile *online* all'indirizzo seguente: https://servizi.gpdp.it/databreach/s/self-assessment (verificato da ultimo in data 9 aprile 2023).

care all'autorità di controllo il *data breach*, notifica che invece dovrà essere disposta tempestivamente ed entro 72 ore in tutti gli altri casi. Se peraltro la violazione sia «suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo» (art. 34).

Pertanto una volta che il titolare e/o il responsabile abbiano stabilito che non è improbabile che la violazione presenti un rischio per i diritti e le libertà dell'interessato, occorre verificare altresì se tale rischio (non improbabile) sia o meno elevato e, in caso affermativo, procedere alla notificazione all'autorità di controllo e alla comunicazione agli interessati[48].

2.4. Gli strumenti documentali e probatori espressione del principio di *accountability*

Il Regolamento introduce diversi specifici vincoli documentali che possono considerarsi espressione dell'accezione probatoria o di rendicontazione del principio di responsabilizzazione[49].

Anzitutto al *considerando* 82 si precisa che per dimostrare la conformità al GDPR «il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti»[50].

---

[48] Cfr. *considerando* 85, che espressamente richiama il principio di responsabilizzazione e l'onere di documentazione/dimostrazione della valutazione volta a determinare la improbabilità di verificazione del rischio: «Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al *principio di responsabilizzazione*, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche».

[49] A sottolineare la vocazione probatoria del principio di responsabilità già Gruppo di lavoro ex Art. 29, Parere 3/2010: «una nuova disposizione che obblighi i responsabili del trattamento ad attuare misure appropriate ed efficaci per garantire che i principi e gli obblighi della direttiva sulla protezione dei dati siano rispettati e di dimostrarlo su richiesta delle autorità. Tali misure dovrebbero favorire il rispetto dei principi e degli obblighi di protezione dei dati, riducendo al minimo i rischi di accesso non autorizzato, uso improprio, perdita etc. L'obbligo di dimostrare su richiesta la predisposizione delle misure necessarie dovrebbe diventare uno strumento utile alle autorità di protezione dei dati nello svolgimento dei loro compiti di verifica dell'applicazione».
Per una semplificata panoramica degli obblighi e delle misure riconducibili all'*accountability*, si rinvia all'URL seguente: https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili (verificato da ultimo in data 9 aprile 2023).

[50] Si soffermano sul ruolo rivestito dal registro dei trattamenti nell'ottica dell'*accoutability,* in particolare: G. Finocchiaro, *GDPR tra novità e discontinuità*, cit., p. 2777; G. Arcella, *op. cit*., p. 393.
Nella prassi si segnala Gruppo di lavoro ex Art. 29, *Parere 3/2010*, sul principio di responsabilità che fra le misure comuni in cui si sostanzia l'applicazione del principio annovera la «mappatura

Il registro dei trattamenti – che, si rammenta, rappresenta un obbligo per tutti quei titolari e/o responsabili che trattino dati in modo stabile[51] – rappresenta il principale documento di rendicontazione del titolare e del responsabile, giacché la compilazione del medesimo comporta una completa mappatura dei trattamenti effettuati, dei soggetti coinvolti nei trattamenti e delle misure organizzative e di sicurezza predisposte.

Il legislatore europeo, identificando un contenuto necessario dei registri (del titolare e del responsabile), ha di fatto introdotto un onere documentale (anche a supporto probatorio) che si estende a tutti gli aspetti che nei registri devono essere inclusi ai sensi dell'art. 30. Per quanto attiene al titolare, il registro deve indicare: «*a)* il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; *b)* le finalità del trattamento; *c)* una descrizione delle categorie di interessati e delle categorie di dati personali; *d)* le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; *e)* ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; *f)* ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; *g)* ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1»[52].

Il registro del responsabile deve indicare: «*a)* il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; *b)* le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; *c)* ove applicabile, i trasferimenti di dati personali verso un

delle procedure per garantire la corretta identificazione di tutte le operazioni di trattamento dei dati e gestione di un inventario di dette operazioni.».

[51] La conclusione è desumibile dal testo dell'art. 30, che tuttavia non brilla per la chiarezza espositiva, di talché è stato necessario un intervento esplicativo del Gruppo di lavoro *ex* art. 29, che nel documento «*Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*)» precisa che è sufficiente che occorra una sola delle condizioni previste dall'art. 30 per far scattare l'obbligo di tenuta del registro: ne discende che difficilmente un operatore professionale potrà considerarsi esente dall'obbligo di tenere un registro. Nel summenzionato documento il WP29 esorta le Autorità nazionali a proporre sui propri siti un modello di registro semplificato per le piccole e medie imprese. Il Garante italiano ha provveduto con la pubblicazione di uno *standard* (in formato pdf ed *excel*), consultabile al link seguente: https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento (verificato da ultimo in data 9 aprile 2023).

[52] I contenuti del registro del titolare, ad eccezione di quello di cui alla lett. *g)* summenzionata, si ritrovano altresì all'interno delle informativa sul trattamento dei dati personali (artt. 13 e 14), che aggiunge: le basi giuridiche individuate dal titolare a copertura dei trattamenti [art. 13, par. 1, lett. *c)*]; l'esistenza di diritti dell'interessato ai sensi degli artt. 15 a 21 [art. 13, par. 2, lett. *b)*]; la natura del conferimento dei dati e le conseguenze in caso di mancata comunicazione [art. 13, par. 2, lett. *e)*]; l'esistenza di processi decisionali automatizzati [art. 13, par. 2, lett. *f)*].

paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; *d)* ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1».

Un ulteriore registro deve essere predisposto in caso di *data breach* per «documenta[re] qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio» (art. 33, par. 5) e ciò in quanto «tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo». Le stesse scelte lessicali usate in tale disposizione normativa mettono in evidenza la funzione di tale adempimento in relazione al principio di *accountability*.

Sotto altro profilo, all'art. 7 il Regolamento stabilisce che «qualora il trattamento sia basato sul consenso, il titolare deve essere in grado di dimostrare che il titolare ha prestato il proprio consenso al trattamento dei propri dati personali»[53], rimettendo in questo modo al titolare la scelta del mezzo attraverso cui documentare e provare il consenso dell'interessato. Anche qui si ravvisa una concreta applicazione del principio di *accountability*, nella parte in cui si richiede al titolare del trattamento non solo di garantire, ma anche di essere in grado di dimostrare, mediante l'adozione di apposite misure tecniche e organizzative, che il trattamento è conforme a quanto previsto dal Regolamento, giusto quanto previsto dall'art. 24, par. 1, GDPR. La documentazione richiesta espressamente dall'art. 7 costituisce dunque una misura *ad hoc*, prevista direttamente *ex lege* in funzione dell'esigenza di documentare l'intervenuta acquisizione del consenso, quale condizione di liceità del trattamento.

Un'ulteriore attività di documentazione – sempre quale espressione del principio di responsabilizzazione di cui all'art. 24 – è prevista, in modo implicito, per la regolamentazione dell'accordo con eventuali contitolari[54], per la nomina dei responsabili del trattamento[55], per vincolare alla riservatezza i collaboratori del responsabile[56]; in modo esplicito, per la nomina dei rappresentanti[57] e per istruire i responsabili eventualmente nominati[58].

---

[53] Sul tema cfr. F. Bravo, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, pp. 188 ss.

[54] Art. 26, par. 1.

[55] Si è già avuto modo di rilevare che il titolare deve indicare, all'interno del registro, i "destinatari" dei dati.
Sul rapporto fra responsabilizzazione e la contrattualizzazione del rapporto con il responsabile del trattamento cfr. Commento all'art. 10 della Convenzione 108 + che espressamente riferisce dell'opportunità di «stabilire specifiche disposizioni contrattuali in caso di delega del trattamento per dare efficacia alla Convenzione».

[56] Art. 28, par. 3, lett. *b)*.

[57] Art. 27 par. 1 «Ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione».

[58] Art. 28, par. 3, lett. *a)*, ai sensi del quale il responsabile tratta «i dati personali soltanto su istruzione documentata del titolare del trattamento».

Un cenno conclusivo di questa carrellata normativa deve poi farsi al contenuto documentale della valutazione di impatto[59], che, ove effettuata, include almeno «*a)* una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; *b)* una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; *c)* una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e *d)* le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione»[60].

2.5. Le misure di "secondo livello": modelli organizzativi e nomina volontaria del DPO

Il principio di *accountability* ha profondamente accentuato l'importanza del profilo organizzativo, conducendo la materia della protezione dei dati nell'alveo del c.d. *risk management* ed incentivando l'allestimento di modelli[61] che diano veste procedurale alle varie e complesse attività richieste per porre in essere gli adempimenti, tutti fra loro concatenati, previsti dal Regolamento.

L'insieme dei processi decisionali che il titolare deve effettuare e che necessariamente muove da una globale valutazione della situazione esistente – che si sostanzia, tra l'altro, anche nell'esame della natura e del volume dei dati e delle tipologie di trattamento, prosegue nella ponderazione dei rischi e si conclude con l'adozione di una decisione sulle misure di sicurezza da predisporre – non soltanto deve essere documentato dal titolare, ma è consigliabile che venga, a monte, dal medesimo "regolamentato" in modo sistematico, attraverso la predisposizione di un modello organizzativo (sulla falsariga di quanto avviene, ad esempio, nell'applicazione del d.lgs. n. 231/2001 ed in generale per tutte quelle materie che in qualche modo si collocano nell'alveo del c.d. *risk management*), costituito da un insieme di procedure definite in anticipo, in un'ottica *by design* e *by default*.

---

[59] Menzionata al par. precedente, con particolare riguardo però all'aspetto discrezionale riguardante la verifica della ricorrenza o meno delle condizioni che ne rendono obbligatoria l'espletazione.

[60] *Sic* art. 35, par. 7. In questo senso, cfr: art. 10, par. 2 della Convenzione 108+ summenzionata, si riporta di seguito il commento corrispondente «88. Il paragrafo 2 chiarisce che prima di svolgere un'attività di trattamento dei dati, il titolare del trattamento dovrà esaminarne il potenziale impatto sui diritti e sulle libertà fondamentali degli interessati. Questo esame può essere svolto senza formalità eccessive. Dovrà inoltre considerare il rispetto del principio di proporzionalità sulla base di una panoramica completa del trattamento previsto. In alcune circostanze, se oltre al titolare del trattamento è coinvolto un responsabile del trattamento, anche il responsabile del trattamento dovrà esaminare i rischi. Gli sviluppatori di sistemi IT, compresi i professionisti della sicurezza o i progettisti, insieme agli utenti e agli esperti legali potrebbero fornire assistenza nell'esame dei rischi».

[61] G. FINOCCHIARO, *GDPR tra novità e discontinuità*, cit., p. 2777; G. FONDERICO, *La regolazione amministrativa del trattamento dei dati personali*, in *Giorn. dir. amm*., 2018, 4, p. 415; A. MONEA, *Regolamento n. 2016/679: la necessità di uno specifico "modello organizzativo" per la protezione dei dati personali*, in *Azienditalia*, 2018, 8-9, p. 1114; M. IRRERA (a cura di), *Assetti adeguati e modelli organizzativi*, Bologna, 2016.

L'adozione di un modello organizzativo, procedurale e di gestione consente di rispondere all'esigenza di creare un'organizzazione *risk-based* adeguata a gestire la complessità degli adempimenti vigenti in materia di trattamento dei dati, mediante un approccio precauzionale, mirato a prevenire trattamenti non conformi alla disciplina e ad evitare che si verifichino violazioni dei dati personali.

Come un *manager* della protezione dei dati, il titolare progetta e adotta un insieme di linee strategiche che disegnino un'organizzazione che, in particolare, senza pretese di esaustività, affronti le seguenti tematiche: (i) definizione della struttura *privacy*, dei ruoli dei soggetti anche attraverso la distribuzione delle competenze tra i propri uffici/aree organizzative interne; (ii) pianificazione di percorsi formativi per il personale in materia di trattamento dei dati; (iii) individuazione dei criteri per la selezione, la nomina e il controllo dei soggetti, esterni alla struttura del titolare, abilitati a trattare i dati per suo conto; (iv) individuazione dei criteri di nomina del DPO e disciplina delle funzioni dello stesso; (v) predisposizione di norme di comportamento e istruzioni[62] in materia di trattamento dei dati; (vi) predisposizione di norme di comportamento e istruzioni sull'utilizzo degli strumenti tecnologici e delle misure di sicurezza; (vii) disciplina di una procedura per il riscontro tempestivo in caso di esercizio dei diritti da parte degli interessati; (viii) regolamentazione di procedure in caso di *data breach*; (ix) predisposizione di presidi per il monitoraggio continuo dei rischi (criteri per *risk assessment*) e di meccanismi di controllo e vigilanza sulla corretta attuazione delle procedure (ad esempio attraverso la pianificazione di *audit* interni ed esterni e/o attraverso la nomina di un DPO) e l'aggiornamento costante della conformità delle stesse alla normativa vigente.

Il modello, unitamente alle valutazioni che ne sono alla base, necessita di affinamenti periodici, continui e costanti.

La predisposizione di un modello organizzativo "documentato"[63], seppur caldamente consigliata, rappresenta propriamente quella che il WP29, nel parere 3/2010, definisce come misura di *accoutability* di "secondo livello", allorquando stabilisce che «L'architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il *primo livello* sarebbe costituito da un obbligo di base vincolante per tutti i responsabili del trattamento [ci si riferisce, invero, ai titolari]. Tale obbligo comprenderebbe due elementi: l'attuazione di misure e/o di procedure, e la conservazione delle relative prove. Questo primo livello potrebbe essere integrato da disposizioni specifiche. Il *secondo livello* includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia delle misure (norme di attuazione eccedenti il livello minimo)».

---

[62] Attraverso l'individuazione di guide e direttive – ad esempio sulla compilazione del registro, sulle modalità per portare a conoscenza degli interessati le informative, sulla raccolta e il tracciamento dei consensi, sul termine di conservazione (c.d. *data retention*) dei dati personali – a corredo dei quali eventualmente allegare la relativa modulistica.

[63] Il riferimento alla documentazione del modello organizzativo non è ultroneo, difatti l'adozione di un'organizzazione efficiente (c.d. misure organizzative), sia pur non documentata, non è facoltativa affatto.

Nell'ambito delle misure ulteriori, di secondo livello, poste a presidio di un'organizzazione efficiente, un cenno meritano la nomina volontaria del DPO, oltre che l'affidamento a terzi dell'incarico di *audit* che aiutino a verificare e dimostrare la conformità della struttura alle disposizioni del GDPR[64].

2.6. Dalla responsabilità *ex ante* a quella *ex post*: i riflessi del principio di *accountability* sulla responsabilità civile (legittimazione passiva e prova liberatoria)

Il principio di responsabilizzazione, che si sostanzia in una "responsabilità *ex ante*", riverbera i propri effetti sulla responsabilità "civile", vale a dire quella propriamente intesa *ex post*, riempiendola di contenuto[65].

In particolare, i due principali profili della (nuova)[66] responsabilità civile in materia di trattamento dei dati personali in cui si riflette l'*accountability* sono rappresentati dalla legittimazione passiva all'azione civile e dall'onere probatorio.

Per quanto attiene al primo aspetto, l'art. 82 in materia di responsabilità civile stabilisce che «chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento»; in questo modo, su-

---

[64] In questo senso, cfr: GRUPPO DI LAVORO EX ART. 29, *Parere 3/2010*: «(…) il responsabile [*rectius*: il titolare] del trattamento potrebbe decidere di nominare un responsabile della protezione dei dati anche se la legge vigente non dispone un obbligo in tal senso. Ancora, il responsabile [*rectius*: il titolare] del trattamento potrebbe voler affidare a terzi l'incarico di eseguire un *audit* relativo a tutte le sue operazioni di trattamento dei dati, al fine di valutarne la conformità con il quadro giuridico in materia di protezione dei dati. Il Gruppo di lavoro apprezza queste iniziative e incoraggia il nuovo quadro giuridico di protezione dei dati a fornire incentivi affinché i responsabili del trattamento si orientino in tale direzione».
Con riguardo alla sola nomina del DPO, si veda il Commento all'art. 10 della Convenzione 108+ summenzionata: «87. Una possibile misura che potrebbe essere adottata dal titolare del trattamento per facilitare tale verifica e dimostrazione di conformità sarebbe la designazione di un "responsabile della protezione dei dati" incaricato dei mezzi necessari per adempiere al suo mandato».

[65] In particolare sul tema si vedano: F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati*. cit., p. 383; M. RATTI, *La responsabilità da illecito trattamento dei dati*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., pp. 615 ss.; S. THOBANI, *Comm. Art. 82*, in A. BARBA-S. PAGLIANTINI (a cura di), *Commentario del Codice Civile, Delle Persone*, cit., p. 1220; R. CATERINA-S. THOBANI, *Gdpr tra novità e discontinuità - Il diritto al risarcimento dei danni*, in *Giur. it*., 2019, 12, p. 2777; D. BARBIERATO, *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Resp. civ. e prev.*, 2019, 6, pp. 2151 ss.; D. AMRAM, *Responsabilità, danno e "accountability" nella società dell'informazione*, in *Danno e resp.*, 2019, 2, pp. 243 ss.; M. D'AGOSTINO PANEBIANCO, *Lineamenti di responsabilità derivanti dalla violazione al trattamento dati*, in *Eur. e dir. priv.*, 2020, 1, p. 237; E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno e resp.*, 2020, 4, p. 433; ID., *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contratto e impr*., 2020, 3, p. 1115; F. BILOTTA, *La responsabilità civile nel trattamento dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, 2019, Milano, p. 445.

[66] Riconducibile alla "nuova" regolamentazione introdotta dal GDPR.

perando l'indeterminatezza del precedente regime (che estendeva la responsabilità a "chiunque" avesse cagionato un danno per effetto del trattamento di dati personali)[67], il legislatore europeo approda a una configurazione ben definita dei soggetti danneggianti: il titolare e/o il responsabile del trattamento dei dati[68].

In particolare il titolare «risponde per il danno cagionato dal suo trattamento che violi il presente regolamento» (art. 82, par. 2)[69]; il responsabile, invece risponde «solo se non ha adempiuto gli obblighi del presente regolamento specificamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento».

Lo spettro della responsabilità del titolare è più ampio rispetto a quello del responsabile e ciò in quanto è il primo a decidere se porre in essere il trattamento, determinandone finalità e modalità, e per tale ragione è sua la responsabilità generale «per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto» (*considerando* 74). Va tuttavia rilevato che, anche laddove il titolare possa dimostrare di aver diligentemente scelto un responsabile che presentava adeguate garanzie e di avere controllato periodicamente la correttezza del suo operato (mediante sopralluoghi e *audit*), difficilmente si libererà della responsabilità, essendo il rapporto di preposizione (analogamente a quanto accade ai sensi dell'art. 1227 e dell'art. 2049 c.c.) sufficiente a ricondurre la responsabilità del responsabile indirettamente in capo al titolare[70], a condizione che il trattamento illecito da parte del responsabile sia stato reso possibile dai compiti e dalle funzioni affidatigli dal titolare medesimo[71].

Per quanto attiene al responsabile del trattamento, egli risponde dei danni nel caso di violazione degli obblighi a suo carico, indicati dall'art. 28 del Regolamento, che in generale si sostanziano nel «mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato»[72].

---

[67] Art. 15 del Codice *Privacy*.

[68] Continua ad essere discusso quale sia la disciplina per le eventuali condotte illecite in materia di trattamento dei dati personali poste in essere da soggetti non riconducibili al titolare né al responsabile.

[69] Si rinvia alle disposizioni richiamate ai parr. 2.2 e 2.3, che, sebbene non esaustive dell'intero panorama dei vincoli incombenti sul titolare, ne rappresentano una considerevole fetta.

[70] Il medesimo argomento a fortiori vale per le violazioni che siano riferibili ai c.d. incaricati, ossia i soggetti che realizzano le attività di trattamento dei dati, sotto il controllo del titolare o del responsabile (menzionati agli artt. 29 e 28, par. 3, lett. b).

[71] Ferma restando la possibilità di rivalsa del titolare sul responsabile.

[72] *Sic* art. 28, par. 1. Più precisamente il responsabile del trattamento, sulla base di un apposito atto giuridico o contratto che lo vincoli con il titolare del trattamento: «*a)* tratt[a] i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale (…); *b)* garantisc[e] che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; *c)* adott[a] tutte le misure richieste ai sensi dell'articolo 32; *d)* rispett[a] le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; *e)* tenendo conto della natura del trattamento, assist[e] il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; *f)* assist[e] il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli

Tralasciando, in questa sede, ogni altra considerazione che lambisca gli ulteriori profili (inerenti alla legittimazione passiva) della solidarietà fra i soggetti corresponsabili e quindi della ripartizione interna della responsabilità, si passerà ad affrontare brevemente l'altro versante della responsabilità civile su cui il principio di responsabilizzazione riverbera i propri effetti: l'onere probatorio e la prova liberatoria[73].

Il titolare del trattamento (o il responsabile del trattamento) è esonerato dalla responsabilità «se dimostra che l'evento dannoso non gli è in alcun modo imputabile».

Senza addentrarci in tematiche di sicuro rilievo, sul profilo speculativo e applicativo della fattispecie – quali ad esempio la natura della responsabilità *ex* art. 82 (contrattuale o *extra* contrattuale, ovvero oggettiva o da colpa presunta) – ma che necessiterebbero di un approfondimento che va oltre l'intento della presente trattazione (che mira esclusivamente a sottolineare il rapporto intercorrente fra il principio di responsabilizzazione e la responsabilità civile da trattamento illecito dei dati), ci limiteremo, in questa sede, a rilevare come il criterio di riparto dell'onere probatorio è definito, in linea generale, dal principio di *accountability*. Da esso, infatti, discende

articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; *g)* su scelta del titolare del trattamento, cancell[a] o gli restituisc[e] tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e *h)* mett[e] a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consent[e] e contribuisc[e] alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato (…) informa[ndo] immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati» (art. 28, par. 3); inoltre «Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche» (art. 28, par. 2) e, da ultimo, al subresponsabile eventualmente nominato impone, «mediante un contratto o un altro atto giuridico (…), gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento» (art. 28, par. 4).

[73] Più propriamente, e da un punto vista sostanziale, l'ingerenza dell'*accountability* è sul "criterio di imputazione": la questione probatoria ne rappresenta pertanto solo una superficiale manifestazione.

la gravosa incombenza, in capo al soggetto che tratta i dati, di dimostrare la liceità[74] del trattamento, in questo modo alleviando la posizione del danneggiato che potrà limitarsi a provare: che è stato effettuato un trattamento, che si è verificato un danno e il nesso fra di essi intercorrente, allegando la violazione commessa dal titolare e/o responsabile.

Quanto più è espresso puntualmente l'obbligo che si assume violato (e da cui deriva la lesione), tanto più agevolata sarà la posizione del danneggiato, che altrimenti vedrà arricchirsi il proprio onere motivazionale dell'indicazione precisa, del motivo e delle modalità per cui le condotte poste in essere dal danneggiante sarebbero, a suo dire, scorrette e, in generale, non conformi al Regolamento.

Una volta appurato che l'onere probatorio ricade sul danneggiante, occorre capire quale sia il contenuto della prova liberatoria, in grado di "assolverlo".

Anche in questo caso soccorre il principio di *accountability*. Alla classica prova liberatoria attingibile dal regime codicistico della responsabilità civile "oggettiva" (la sussistenza di un caso fortuito o una causa maggiore), si affiancherebbe, infatti, l'ulteriore dimostrazione, *ex multis*: che non erano disponibili misure tecniche atte a prevenire il rischio in concreto verificatosi, ovvero che i costi delle misure di prevenzione erano eccessivi rispetto a una bassa probabilità e/o gravità (che, va ricordato, si misura in via preventiva) del rischio[75].

In questo modo ed entro questi margini l'art. 82 viene riportato nell'alveo della responsabilità per colpa, ove però la colpa è presunta e qualificata. In quest'ottica diventa determinante – e forse questo risulta essere l'aspetto realmente innovativo – l'adozione da parte del titolare e/o del responsabile di un approccio prudenziale, propositivo, sistematico e completo, teso a documentare e procedimentalizzare l'attività posta alla base delle scelte effettuate in materia di trattamento dei dati personali.

2.7. Brevi cenni al rapporto fra *accountability* e responsabilità amministrativa

In conclusione del presente par. 2, preme dedicare un brevissimo cenno al rapporto fra il concetto "*overarching*" di *accountability* e la responsabilità amministrativa in materia di trattamento dei dati.

Rinviando la trattazione approfondita del tema al par. 3 che segue, giova rilevare che la violazione del principio di responsabilizzazione (e rendicontazione), unitamente alla violazione di alcune delle disposizioni summenzionate, riflesso del principio stesso (contenute agli artt. 7, 12, da 44 a 49), determina l'applicazione della misura sanzionatoria più aspra, prevedendo una sanzione pecuniaria fino a 20.000.000 euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 2).

---

[74] Intesa in senso lato, quale conformità ai principi e alle norme poste a presidio del trattamento dei dati.

[75] Ovviamente ci si riferisce a quelle norme, in parte tracciate al par. 2.2, che lasciano un significativo spazio di discrezionalità al titolare/responsabile del trattamento, non potendosi ravvisare invece una tale via d'uscita tutte le volte in cui l'obbligo, ovvero il divieto, viene disposto in modo specifico e puntuale (si pensi all'omissione del registro dei trattamenti o dell'invio dell'informativa, etc.).

Invece, per la violazione di altre delle disposizioni summenzionate (quelle contenute agli artt. 25, 27, 28, 29, 30, 32, 33, 34, 35, 37-39, 42 e 43), la sanzione prevista è quella meno grave, fino a 10.000.000 euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4).

La ricomprensione dell'art. 5 (che disciplina l'insieme dei principi, che, oltre all'*accountability*, presidiano il trattamento dei dati) nell'ambito delle disposizioni dalla cui violazione scaturisce l'applicazione della sanzione più gravosa, potrebbe rendere eludibile la più bassa soglia sanzionatoria stabilita per quelle violazioni che il legislatore europeo aveva valutato, evidentemente, come meno rilevanti[76]. La portata globale del principio di *accountability* difatti fagocita tutte le disposizioni menzionate *supra,* ai parr. 2.2 e 2.3, di talché la violazione di ciascuna di quelle disposizioni ben potrebbe qualificarsi come mancato rispetto del principio di responsabilità e conseguentemente subire la sanzione più gravosa[77].

3. Applicazione del principio nella casistica

3.1. Breve premessa

L'autorità Garante per la protezione dei dati personali in maniera significativa e sin dall'inizio dell'entrata in vigore del Regolamento europeo[78], è intervenuta in merito al mancato rispetto del fondamentale e rivoluzionario, stante il deciso cambio di prospettiva offerto in ambito *privacy*, principio di *accountability.* Invero, nei suoi provvedimenti, il Garante ha chiarito in che modo, concretamente, si debba tradurre

[76] Ovviamente, trattandosi di soglie decisamente elevate, la criticità rilevata acquista rilievo per le violazioni di elevato impatto, e quindi riguardanti i grandi operatori del mercato, che trattano rilevanti volumi di dati.

[77] Il tema si propone, non soltanto per le norme richiamate ai parr. 2.2 e 2.3, ma per tutte le disposizioni indicate all'art. 83, par. 4, che siano epifania di uno dei principi di cui all'art. 5, par. 1. Non resta che attendere l'interpretazione che verrà data nel "diritto vivente".

[78] Il Garante, nella Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali pubblicata sul proprio sito, afferma che «Il regolamento pone con forza l'accento sulla "responsabilizzazione" (*accountability* nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento». Per l'esame della Guida nella sua interezza si rimanda alla pagina https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili (verificato da ultimo in data 9 aprile 2023). Tra gli ultimi contributi dell'Autorità garante si segnala, invece, l'avvio, in data 26 novembre 2020, della procedura di adozione delle Linee Guida sull'utilizzo di *cookie* e di altri strumenti di tracciamento: nella Scheda di Sintesi, contenuta nell'Allegato 2, con riferimento alla normativa GDPR il Garante pone l'accento prioritariamente proprio sul principio di *accountabilty*. Per l'integrale consultazione si rimanda alla pagina https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9501061 (verificato da ultimo in data 9 aprile 2023).

la responsabilizzazione, nella sua accezione di *compliance* al Regolamento, che grava sul titolare del trattamento dei dati[79], sanzionando, da un lato, la mancata adozione delle misure tecniche ed organizzative tese a garantire il rispetto delle disposizioni previste dalla normativa europea e, dall'altro, la non comprovata e dimostrata conformità ai principi e alle prescrizioni del Regolamento.

Ai fini di un'analisi più compiuta del principio oggetto del presente approfondimento e per dar conto di come il principio di *accountability* operi nella prassi, si esamineranno di seguito alcuni dei provvedimenti più significativi emessi dall'Autorità Garante italiana negli anni compresi tra il 2020 ed il 2022 nonché, in breve, alcuni dei primi provvedimenti adottati da altre autorità di controllo europee[80].

3.2. *Accountability* e trattamento dati per finalità di marketing: i casi Tim S.p.a e Wind Tre S.p.a. nei provvedimenti del Garante

Nel provvedimento correttivo e sanzionatorio assunto nei confronti di Tim S.p.a. (di seguito anche solo Tim, Società o compagnia telefonica) il 15 gennaio 2020[81] rubricato al n. 7 del Registro dei provvedimenti (di seguito anche solo provvedimento), il Garante ha più volte richiamato la violazione del principio di *accountability* con riferimento, in particolare, alla non adeguata capacità della società di telefonia di comprovare l'esatto adempimento della disciplina in materia di protezione dei dati personali in violazione, quindi, degli artt. 5, par. 2, e 24, par. 1 e 2, del Regolamento europeo[82].

---

[79] Si segnala, relativamente all'applicazione del nuovo principio di *accountability* e agli oneri gravanti sul titolare del trattamento, a titolo esemplificativo, anche l'ordinanza della Cass., sez. I, ord. 17 settembre 2020, n. 19328. Il provvedimento, che affronta il tema del risarcimento del danno derivante da illecito trattamento dati, per una condotta precedente all'introduzione del GDPR, fa menzione del principio in questione definendo i gradi di responsabilità: «Pertanto, il danneggiato che lamenti la lesione dell'interesse non patrimoniale può limitarsi a dimostrare l'esistenza del danno e del nesso di causalità rispetto al trattamento illecito, mentre spetta al danneggiante titolare del trattamento, eventualmente in solido col responsabile, dimostrare di aver adottato tutte le misure idonee per evitare il danno. Questo schema è parzialmente confermato anche nel nuovo GDPR (art. 82.3 GDPR) che, sulla base del principio di responsabilizzazione (*accountability*) addossa al titolare del trattamento dei dati, eventualmente in solido con il responsabile il rischio tipico d'impresa (art. 2050 c.c.)».

[80] Si fa riferimento, in particolare, alle pronunce dell'Autorità Garante della Privacy tedesca (*Landesbeauftragte Für Den Datenschutz Und Die Informationsfreiheit – LfDI*, austriaca (*Datenschutzbehörde*), e del *Comissão Nacional de Proteção de Dados* (CNPD- Portogallo). Si tratta di alcuni tra i primi provvedimenti adottati dalle autorità europee subito dopo l'entrata in vigore del GDPR.

[81] GPDP, 15 gennaio 2020, doc. *web* n. 9256486. Cfr. poi la nota con cui l'Autorità riassueme i contenuti di tale ultimo provvedimento (GPDP, 1° febbraio 2020, doc. *web* n. 9256409).

[82] Il Garante per la protezione dei dati personali, nel provvedimento in esame, al par. 3.8 afferma: «Sotto un diverso profilo TIM ha rivelato di non avere sufficiente contezza e capacità di render conto di vari fondamentali aspetti dei trattamenti effettuati dalla medesima o mediante soggetti terzi *partner*, e quindi ha evidenziato una non adeguata capacità di comprovare l'esatto adempimento della normativa in materia, risultando così aver violato il fondamentale principio di *accountability* (artt. 5, par. 2 e 24, par. 1 e 2, Regolamento)».

La violazione di cui sopra è emersa nel corso dell'ispezione disposta dall'Autorità[83], tra il mese di novembre 2018 e il mese di febbraio 2019, resasi necessaria stante le numerose segnalazioni e reclami di utenti, sia intestatari di schede telefoniche Tim che non, inerenti al periodo compreso tra gli anni 2017 e 2019 e aventi ad oggetto una serie di condotte ritenute illegittime[84]. Tra queste il Garante ha, in particolare, evidenziato come Tim S.p.a. – in merito alle cosiddette chiamate definite "*fuori lista*"[85], effettuate dai propri *partner* commerciali, nella maggior parte dei casi *call center* – non sia stata in grado, secondo l'Autorità, di fornire un esaustivo elenco complessivo delle chiamate effettuate, escluse quelle effettivamente andate a buon fine perché associate a un *verbal order*[86]. Le difese della Società[87], nell'occasione,

[83] La complessa attività istruttoria è stata svolta anche con il supporto del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza.

[84] L'attività del Garante, nel caso citato, ha preso il via da una serie di segnalazioni e reclami – pervenuti a far data dal 1° gennaio 2017 fino ai primi mesi del 2019 – riguardanti trattamenti aventi ad oggetto la ricezione di chiamate promozionali indesiderate, nell'interesse di Tim S.p.a., effettuate (i) in assenza di consenso degli interessati oppure (ii) nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni; inoltre, anche (iii) dopo l'esercizio del diritto di opposizione nei confronti della suddetta compagnia telefonica o, ancora, (iv) nell'ambito di procedure finalizzate alla soluzione di guasti tecnici inerenti ai servizi di telefonia erogati agli altri interessati da altre compagnie telefoniche. La richiesta di chiarimenti avanzata dal Garante nei confronti della compagnia telefonica ha inoltre evidenziato (v) il mancato riscontro alle istanze formulate dagli interessati con riguardo ai diritti sanciti dalla normativa in materia di protezione dei dati personali e, in particolare, a quelli di accesso ai propri dati e di opposizione al trattamento per finalità promozionali, nonché (vi) la richiesta di un consenso unico e indistinto al trattamento dei dati per svariate finalità – anche ulteriori all'esecuzione del contratto – nell'ambito della modulistica predisposta per l'autocertificazione di possesso di linea prepagata. Nel periodo oggetto di indagine, inoltre, Tim S.p.a. ha notificato al Garante diverse violazioni di dati personali (c.d. *data breach*) che hanno evidenziato alcuni disallineamenti fra i sistemi che trattano i dati personali della clientela tali da provocare, ad esempio, l'errata attribuzione di linee telefoniche ai soggetti intestatari o l'errata associazione fra intestatari o l'errata associazione fra intestatari e i dati di contatto utilizzati dalla compagnia telefonica.

[85] Per chiamate "*fuori lista*" si intendono le telefonate promozionali effettuate da *partner* commerciali di Tim S.p.a. verso numerazioni non presenti nelle liste di contattabilità della compagnia telefonica, in assenza di consenso degli interessati o di altra idonea base giuridica.

[86] L'Autorità garante, nel provvedimento in esame, ha definito, la quantificazione delle telefonate *«parziale* e *indiretta»* nonché, al fine di comprendere l'ampiezza del fenomeno dei cosiddetti contatti fuori lista, ha evidenziato che il numero di *Verbal Order* (nel caso di specie 184.655) «fornisce un'indicazione per difetto delle chiamate sottostanti: ad esempio, nel corso degli accertamenti, ispettivi, XX ha dichiarato che, su clientela presente nel *customer base*, il numero dei contratti stipulati rappresenta il 9% delle chiamate promozionali effettuate nel caso di campagne *upselling*, mentre solo il 3% in caso di campagne destinate a nuove linee. Tale tasso di adesione, peraltro, risulta in genere ancora più basso nel caso di campagne promozionali rivolte a soggetti "*prospect*" in ragione della minore accuratezza dei dati (es. numerazioni non più attive o soggetti che hanno in essere contratti più vantaggiosi di quelli proposti» (cfr. par. 2.2, del provvedimento, avente ad oggetto le telefonate nei confronti di utenze non presenti nelle liste di contattabilità di TIM).

[87] Al riguardo la Società ha dichiarato, così come riportato nel paragrafo indicato al 2.2 del provvedimento, che: *«(…) ai partner* è vietato contrattualmente l'utilizzo di liste di contattabilità autonomamente reperite e non autorizzate da TIM», tuttavia *«(…) nel corso del contatto utile con la linea (…) presente nella lista di* contattabilità fornita da TIM, può avvenire che la persona richiamata richieda di essere richiamata su un'altra numerazione oppure indichi un'altra persona del nucleo familiare

non sono state ritenute sufficienti dal Garante. Peraltro, per la stessa tipologia di telefonate, l'Autorità era già intervenuta nei confronti di Tim S.p.a. nel 2016, con provvedimento del 22 giugno, vietando alla stessa il trattamento dati degli utenti per finalità di *marketing*[88]. Il principio di *accountabilty*, pertanto, secondo quanto emerge dalla lettura del provvedimento e dalle considerazioni fatte dall'Autorità, risulterebbe violato nel caso di specie, sia sotto il profilo della responsabilizzazione che, anche, della "*culpa in vigilando*" relativamente all'operato dei soggetti di cui la compagnia telefonica si è avvalsa per effettuare le chiamate promozionali[89].

Il Garante, per i numerosi trattamenti illeciti di dati legati all'attività di *marketing*, con il provvedimento correttivo e sanzionatorio del 15 gennaio 2020, ha irrogato a Tim S.p.a. una sanzione di 7.802.946,00 euro nonché ha imposto alla compagnia telefonica venti misure correttive, tra divieti e prescrizioni[90]. La sanzione,

a cui rivolgersi per l'offerta in questione, fornendo la numerazione (c.d. referenze) (…)». Tim ha altresì precisato, ancora relativamente alle chiamate "fuori lista", che le stesse «non possono essere note alla Società in quanto eseguite dai *partner* tramite i lori sistemi informatici/CRM (…)» se non nel momento in cui «il cliente/*prospect* accetti l'offerta commerciale (che) viene tracciata obbligatoriamente nel sistema del *Verbal Order* (di seguito anche VO) di TIM (cfr. pp. 7 e 8, riscontro 14/03/2019). Ciò sia che la numerazione contattata derivi dalle liste di contattabilità fornite dalla Società, sia che rientri fra i c.d. fuori lista».

88 GPDP, Provv. del 22 giugno 2016, doc. *web* n. 5255159.

89 Nel provvedimento cit., in particolare nella parte conclusiva del paragrafo indicato come 2.1, si legge come, «(…) oltre a prassi scorrette poste in essere dai partner con riferimento alle modalità di gestione dei dinieghi – emerga anche la mancata adeguata implementazione da parte della Società stessa di procedure gestionali condivise che, pur garantendo opportuna attenzione alle eventuali specifiche esigenze aziendali, delle imprese coinvolte – consentissero un adeguato controllo da parte di TIM quale committente e fornitrice di liste di contattabilità sulla complessiva gestione del trattamento per finalità promozionali, nonché il correlato obbligo di render conto delle proprie attività in linea con il principio di *accountability*». Nel paragrafo 4.8 si legge, in riferimento al medesimo obbligo di vigilanza: «Con riguardo al comportamento dei propri *partner*, per i quali TIM ha uno specifico obbligo di vigilanza (art. 28 del Regolamento), la Società – anche nel corso dell'audizione del 5 novembre 2019 e da ultimo con la nota del 12/11/2019 – non è stata in grado di chiarire compiutamente il mancato/tardivo inserimento nella *black list* dinieghi da parte dei *partner* nonché indicare e documentare le tempistiche relative all'effettivo inserimento dei dinieghi nei sistemi societari, manifestando un faticoso esercizio dell'obbligo di *accountability*».

90 Il Garante, in particolare, «ha vietato a Tim l'uso dei dati ai fini di *marketing* di chi aveva espresso ai *call center* il proprio diniego a ricevere telefonate promozionali, dei soggetti presenti in *black list* e dei non clienti che non avevano dato il consenso. La società non potrà più utilizzare neanche i dati della clientela raccolti mediante le *app* "My Tim", "Tim Personal", e "Tim Smart Kid" per finalità diverse dall'erogazione dei servizi senza un consenso libero e specifico. Fra le prescrizioni, il Garante ha ingiunto a Tim di verificare la consistenza delle *black list* utilizzate e di acquisire tempestivamente quelle eventualmente formate dai *call center* per riversale nella propria *black list* (…)». Ancora, ha imposto di «(…) rivedere il programma "Tim Party" e consentire l'accesso dei clienti a sconti e concorsi a premi eliminando il consenso obbligato al *marketing* (…)», «(…) verificare la procedura per l'attivazione di tutte le *app*, specificare sempre con linguaggio chiaro e comprensibile, i trattamenti svolti con l'indicazione delle finalità da perseguire e delle modalità di trattamento utilizzate, nonché acquisire un valido consenso. La Società dovrà inoltre implementare le misure tecniche ed organizzative relative alla gestione delle istanze di esercizio dei diritti degli interessati e rafforzare le misure volte ad assicurare la qualità, l'esattezza e il tempestivo aggiornamento dei dati personali trattati dai diversi sistemi della società» (cfr. «*Marketing: dal Garante privacy sanzione da 27 milioni e 800 mila euro a Tim*» del 1° febbraio 2020, consultabile alla pagina già indicata nella

comprensiva delle misure correttive, è stata comminata considerata l'ampia portata dei trattamenti, la gravità delle violazioni rilevate, la durata significativa delle violazioni, l'esistenza di numerosi precedenti provvedimenti, la sussistenza di rilevanti vantaggi economici, il carattere doloso di alcune condotte, nonché, testualmente, il «carattere gravemente negligente, più propriamente colposo, di alcuni trattamenti, come: la non adeguata attuazione dei fondamentali principi di *privacy by design* ed *accountability* (…)»[91].

L'attività di controllo nei confronti degli operatori telefonici, iniziata nell'anno 2020 con il provvedimento adottato verso Tim, è proseguita per tutto l'anno e ha interessato, per condotte analoghe a quelle sopra elencate, anche altri operatori telefonici[92].

Dall'esame dell'ordinanza di ingiunzione nei confronti di Wind Tre S.p.a. (di seguito anche solo Wind, Società o compagnia telefonica), emessa il 9 luglio 2020 e rubricata nel registro dei provvedimenti al n. 143[93] (di seguito anche solo provvedimento), è emersa con ancora più forza la centralità, per il Garante, del principio di *accountability* nonché la posizione sempre più netta dell'Autorità, a oltre due anni dall'avvio dell'applicazione del Regolamento, nei confronti di chi non provvede ad adeguare le proprie condotte al dettato normativo. Sotto quest'ultimo profilo l'attenzione dell'Autorità risulta ancora più mirata in tutti quei casi in cui, per la particolarità e le finalità dei dati trattati, per i prevedibili rischi, per gli strumenti a disposizione nonché, anche, perché si è trattato di soggetti già destinatari di pronunce similari[94], il mancato adeguamento è risultato ancora più arbitrario.

Si osservi che l'autorità Garante ha rilevato, al termine dello svolgimento della complessa attività istruttoria ed ispettiva[95] svolta nei confronti di Wind, le seguenti mancanze:

---

nota 5 del presente approfondimento e, per un esame completo, si rimanda al provvedimento il cui testo integrale è parimenti indicato *supra*, nella nota 81 del presente scritto). La sanzione in esame è parsa proporzionale alla violazione, in conformità dell'art. 83, considerati anche i precedenti provvedimenti assunti nei confronti della compagnia telefonica.

91 Cfr. par. 4 del provvedimento del 15 gennaio 2020, cit.

92 Si segnala, oltre ai due provvedimenti oggetto specifico del presente approfondimento, sempre in materia di *telemarketing* aggressivo e delle conseguenti sanzioni nei confronti di compagnie telefoniche, anche GPDP, Provv. del 12 novembre 2020, doc. *web* n. 9485681, provvedimento emesso nei confronti di Vodafone Italia S.p.a. e nel quale è stata parimenti considerata con grande attenzione la violazione del principio di *accountabilty* nonché di *privacy by design e by default*. Nel corso della riunione in cui è stato adottato il provvedimento nei confronti di Wind Tre S.p.a. del 9 luglio 2020 per il quale v. nota seguente, l'Autorità (GPDP, Provv. del 9 luglio 2020, doc. *web* n. 9435807) ha provveduto anche a sanzionare per 800 mila euro, Iliad, altro operatore telefonico risultato, all'esito della dedicata istruttoria, carente in relazione alle modalità di accesso dei propri dipendenti ai dati del traffico telefonico dei clienti.

93 GPDP, Provv. del 9 luglio 2020, doc. *web* n. 9435753.

94 Wind Tre S.p.a era già stata oggetto di un precedente provvedimento inibitorio e prescrittivo (GPDP, Provv. del 22 maggio 2018, doc. *web* n. 8995285) adottato in vigenza del Codice *Privacy* di cui al d.lgs. 196/2003.

95 Nell'ambito del procedimento condotto nei confronti di Wind Tre, conclusosi con l'ingiunzione oggetto del presente approfondimento, sono stati esaminati dal Garante oltre 100 fascicoli ed effettuate una serie di ispezioni presso la sede della Società, presso alcuni *partner* della stessa, nonché presso

1) l'inosservanza del rispetto dei dettami del Regolamento nell'espletamento dell'attività promozionale mediante sms, e-mail, fax, telefonate e chiamate autorizzate[96] attraverso: (*i)* contatti effettuati senza consenso[97]; (*ii*) contatti effettuati sulla base di un consenso da ritenersi non idoneo; *(iii*) consensi risalenti e non conformi al nuovo quadro normativo introdotto dal Regolamento[98]; (*iv*) consensi acquisiti direttamente dai *partner* commerciali; (*v*) consensi acquisiti mediante le *app* MyWind e My3; (*vi*) consensi prestati con modalità non legittime (manifestazione del consenso non libera); (*vii*) consensi di clienti di altro gestore acquisiti con modalità illegali[99]; *(viii*) contatti effettuati senza che sia stata documentata l'acquisizione di un idoneo consenso;
2) il Garante ha altresì rilevato, relativamente alle modalità di riscontro delle richieste di esercizio dei diritti da parte degli interessati: *(i*) istanze pervenute a recapiti non corretti; *(ii*) istanze non corredate da documenti di riconoscimento; (*iii*) istanze non riscontrate per errori o problemi di ricezione della posta cartacea o elettronica;
3) l'Autorità ha mosso censure anche per la violazione del principio di trasparenza, ai sensi e per gli effetti dell'art. 12 del Regolamento, nell'ambito di un mancato riscontro a una richiesta di accesso ai dati di traffico conservati per finalità di controllo della fatturazione;

---

un altro operatore telefonico. All'attività ha partecipato anche la Guardia di Finanza, con il proprio reparto speciale privacy.

96 Tra le segnalazioni ricevute, ve ne sono state alcune in cui è stata lamentata la ricezione di contatti anche dopo la revoca del consenso o l'esercizio del diritto di opposizione. Wind Tre, in riscontro alla richiesta di chiarimenti relativamente ai contatti, da un lato ha documentato l'acquisizione di uno specifico consenso mediante esibizione dei contratti sottoscritti dagli interessati ma, dall'altro, alla luce degli accertamenti condotti, è emerso che alcuni consensi erano stati acquisiti in modo inidoneo o, anche, che la società non è stata in grado di documentare l'avvenuta acquisizione.

97 In questo caso la Società ha dichiarato che il contatto è avvenuto per errore o che la revoca non era stata tempestivamente recepita.

98 In riferimento a questa contestazione, nel provvedimento, al paragrafo 2.1.2.1, alla luce della documentata acquisizione del consenso attraverso contratti sottoscritti negli anni 1988/1999, si legge che essi «(…) non consentono di documentare una volontà libera, specifica, e informata dell'interessato essendo previsto un solo consenso per finalità di trattamento diverse (…); a tal proposito si richiamano gli artt. 4, punto 11, e 7 nonché il contenuto del considerando n. 171 del Regolamento (…). Pertanto, è *onere del titolare* valutare se i consensi già acquisiti siano da considerarsi ancora conformi alle norme vigenti; tra queste, si richiamano anche le modifiche normative intervenute successivamente al 1999 volte a disciplinare, con disposizioni di carattere speciale, il trattamento posto in essere nell'ambito dei servizi di comunicazione elettronica (art. 130 del Codice e disposizioni in materia di Registro delle opposizioni) *da considerarsi ormai note a tutti gli operatori del settore, anche alla luce delle numerose pronunce del Garante*».

99 Relativamente agli esiti degli accertamenti del cosiddetto «procedimento B», richiamato anche nella premessa del provvedimento adottato nei confronti di Wind S.p.a., si rimanda ai parr. 2.1.2.5 e 4.2 del provvedimento; si precisa, al fine di agevolare la lettura, che nelle pagine successive del presente approfondimento, la tematica relativa al mancato controllo della filiera da parte di Wind Tre S.p.a., sarà oggetto di *focus* specifico.

4) infine, la pubblicazione, in alcun modo autorizzata, di dati personali negli elenchi telefonici[100].

In riferimento al tema dell'*accountability*, l'ordinanza emessa nei confronti di Wind assume rilievo nella parte in cui il Garante dettaglia specificatamente le proprie considerazioni di carattere giuridico. Infatti l'Autorità, nella pronuncia, dopo aver esaminato le difese della Società[101] e accertata, dettagliatamente, l'illiceità delle diverse condotte testé evidenziate, è entrata nel merito del (mancato) rispetto dei principi di *accountability* e *privacy by design*. Il Garante ha, nettamente, evidenziato la «condotta elusiva»[102] tenuta dalla compagnia telefonica. Il Garante ha ritenuto utilizzare tal netta definizione per descrivere l'atteggiamento di Wind soprattutto considerato il fatto che analoghi rilievi erano stati mossi in passato e pertanto, anche in virtù di questo aspetto, la Società aveva conoscenze e competenze nonché strumenti per ponderare i rischi connessi al trattamento dei dati e adottare conseguentemente procedure e tecniche organizzative adeguate[103]. Il Garante, a tal proposito, nel

[100] Per l'esame completo degli esiti dell'istruttoria svolta nei confronti di Wind Tre S.p.a., e, di conseguenza, per il quadro completo e dettagliato di tutti i rilievi evidenziati dal Garante, solo sintetizzati nei numeri da 1) a 4), si rimanda al paragrafo 2 del provvedimento oggetto del presente approfondimento.

[101] Le argomentazioni utilizzate da Wind Tre nelle proprie difese, così come la serie di misure correttive che la Società ha riferito di aver implementato, anche riguardo alla centralizzazione delle campagne promozionali, non sono state ritenute dal Garante sufficientemente esaustive. A titolo esemplificativo, all'interno del par. 4.5, relativamente a questo aspetto si legge: «D'altro canto, nel dare atto delle misure correttive apportate, in parte già prima della notifica dell'avvio del procedimento da parte del Garante, si intravedono potenziali soluzioni per rafforzare le garanzie. Ci si riferisce in particolare alla centralizzazione dell'attività promozionale nel sistema di *Campaign management* o alla previsione del registro dei contatti da tenere – per il momento solo – a cura degli agenti del canale fisico. Tali misure, tuttavia, potranno sviluppare un potenziale che, al momento può definirsi embrionale, solo nel momento in cui saranno sostenute con maggiori conseguenze sul piano contrattuale per i responsabili che non si attengano scrupolosamente a tali istruzioni. Ad esempio, il sistema centralizzato di *Campaign management*, già da tempo in uso presso la Società, non ha comunque impedito il verificarsi di contatti, portati all'attenzione del Garante, per i quali la Società non è stata in grado di fornire spiegazioni, senza contare il fatto che molti di questi sono stati realizzati utilizzando canali di contatto diversi da quello telefonico. Una così fervida attività promozionale non può essere semplicemente disconosciuta e rubricata come iniziativa autonoma di soggetti non autorizzati, dato che l'interesse ad agire non pare certo essere unicamente di questi ultimi. E tale interesse, evidentemente, non viene meno finché tale attività, seppur non autorizzata, viene comunque remunerata». Per l'integrale conoscenza delle stesse si rimanda al provvedimento oggetto del presente approfondimento con particolare riguardo al par. 3 dedicato a «La difesa del Titolare».

[102] Nel paragrafo della pronuncia indicato al numero 4.5, dedicato al rispetto dei principi di *accountability* e *privacy by design*, si legge: «Oltre a quanto già in dettaglio contestato nei punti precedenti, occorre evidenziare, anche in via più generale, una condotta dimostratasi complessivamente elusiva dei principi di *accountability* e *privacy by design*, enunciati dagli artt. 5, par. 2, 24, par. 1 del Regolamento».

[103] Nel par. 4.5 della pronuncia cit., dedicato al rispetto dei principi di *accountability* e *privacy by design*, si legge inoltre che: «Infatti, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" la Società disponeva di idonei strumenti e di sufficienti *conoscenze, veicolate anche dalle consolidate pronunce del Garante* (direttamente rivolte anche alla Wind Tre), per valutare i rischi connessi al trattamento e per predisporre, di conseguenza, procedure tecniche ed organizzative adeguate».

provvedimento cit., richiamando l'attività istruttoria, ha affermato: «Al contrario, le risultanze istruttorie hanno mostrato un quadro complessivamente inidoneo al soddisfacimento di tale requisito di adeguatezza, dal momento che più volte è stata rilevata la mancanza di idonee misure tecniche e organizzative, dovendosi in alcuni casi aggiungere l'aggravante della preordinazione della condotta (nei casi relativi alla raccolta del consenso tramite *app* e tramite sottoscrizione del contratto presso i *dealer*) e dovendo altresì rilevare come, in più occasioni, la Società non sia stata in grado di dimostrare la conformità alle norme dei trattamenti posti in essere e l'efficacia delle misure adottate, come invece prescritto dall'art. 5, par. 2 del Regolamento»[104].

Il provvedimento che l'Autorità ha adottato nei confronti di Wind risulta essere di particolare interesse, utile per meglio comprendere la portata attuativa delle tante forme che assume il principio di *accountability*, anche sotto il profilo dell'analisi dei rapporti tra titolare e responsabile del trattamento dei dati. Così come era accaduto per Tim S.p.a. nel corso dell'attività ispettiva e dell'istruttoria, oltre le numerose carenze proprie della compagnia telefonica, sono emerse gravi irregolarità all'interno della filiera dei *partner* commerciali utilizzati dalla compagnia telefonica. A seguito, infatti, di una serie di specifiche segnalazioni, il Garante, nell'ambito dell'attività di indagine nei confronti di Wind, ha aperto un secondo filone di attività ispettiva ed istruttoria denominandolo «procedimento B». Tale ulteriore approfondimento ha condotto alla scoperta della presenza, a Roma, di un *call center* che, per conto di Wind, si occupava di contattare clientela e presentare offerte di nuovi servizi telefonici, in spregio dei dettami del Regolamento e del Codice *privacy*. A capo di tali attività, a seguito degli accertamenti effettuati, risultava la [S.] s.r.l.s.[105] nella cui sede venivano acquisiti anche elementi significativi atti a far emergere uno stretto legame operativo con un'altra società, la [M.] S.r.l., che per conto della Wind avrebbe dovuto svolgere attività di commercializzazione dei prodotti della compagnia telefonica in forza di un contratto di agenzia al cui interno era prevista anche la nomina a responsabile del trattamento dati. La [M.] S.r.l., senza peraltro aver definito contrattualmente alcunché[106] con la [S.] s.r.l.s., aveva sub affidato a quest'ultima, identificata come procacciatore, intere fasi del trattamento dati che venivano raccolti illecitamente.

La [M.] S.r.l, a seguito del procedimento che si è aperto anche a carico di questa società, è stata sanzionata dal Garante per 200.000,00 euro e l'Autorità ha anche

[104] Cfr. par. 4.5 dedicato al rispetto dei principi di *accountability* e *privacy by design*.

[105] L'attività del *call center*, si legge nel provvedimento al par. 2.1.2.5, «si presentava come del tutto abusiva, in violazione non soltanto delle disposizioni in materia di protezione dei dati personali ma anche di quelle in ambito fiscale, tributario e lavorativo per le quali il nucleo *privacy* procedeva ad interessare le competenti articolazioni della Guardia di Finanza. Risultava inoltre condotta da una società non presente nel Registro degli operatori di comunicazione, utilizzando numerazioni non censite nel medesimo registro, in un quadro estremamente preoccupante di disinteresse per i diritti degli interessati e per le necessarie garanzie di sicurezza che avrebbero dovuto presiedere ogni operazione di trattamento».

[106] L'assenza di qualsivoglia mandato è stata confermata, con disarmante sottovalutazione della problematica, dalla [M.] S.r.l., in una comunicazione inviata mezzo e-mail il cui contenuto è riportato nel provvedimento emesso nei confronti di Wind: nel par. 2.1.2.5 si legge che «al momento di avviare nuove collaborazioni ai procacciatori il mandato scritto è l'ultima cosa che interessa (…)».

previsto il divieto di utilizzare i dati raccolti e trattati da agenti presenti sul territorio nazionale (i cosiddetti procacciatori)[107]. La [M.] S.r.l. è stata ritenuta responsabile anche per le condotte poste in essere dalla [S.] s.r.l.s.[108].

Alla luce dell'accertata violazione di numerose norme del GDPR e del Codice, considerata l'ampia portata dei trattamenti, la gravità delle violazioni rilevate, la durata significativa delle violazioni, il carattere doloso di alcune condotte, l'esistenza di un precedente provvedimento, la sussistenza di rilevanti vantaggi economici, «il carattere *gravemente negligente* di altri trattamenti, come: la *non adeguata attuazione dei fondamentali principi* di *privacy by design*, di *privacy by default* e di *accountability*»[109], è stata applicata nei confronti della compagnia telefonica un'importante sanzione amministrativa, considerato il valore del suo ammontare, pari a 16.729.600,00 euro.

3.3. (*segue*): i casi Fastweb S.p.a. ed Edison Energia Sp.a.

L'attività di controllo del Garante *privacy* volta alla verifica del rispetto del principio di *accountability* è costante. L'attenzione dell'autorità italiana per questo principio, ritenuto cardine nell'ambito della disciplina volta alla tutela dei dati personali, emerge infatti con chiarezza in tutti i pronunciamenti successivi a quelli *ut sopra* esaminati nel dettaglio.

[107] GPDP, 9 luglio 2020, doc. *web* n. 9435774.

[108] Nell'ordinanza ingiunzione emessa nei confronti della [M.] S.r.l. si legge infatti che «La mancanza di forme scritte di accordi e di designazioni in ambito *privacy* che leghino [M.] s.r.l. ai cd. "procacciatori", nonché l'assenza di attività di verifica e di controllo delle procedure poste in essere dai propri collaboratori, con riferimento al rispetto rigoroso delle disposizioni del Regolamento e del Codice, ha contribuito a far sì che la società [S.] s.r.l.s. instaurasse e consolidasse delle forme di acquisizione delle liste di potenziali clienti ai quali veicolare le proposte commerciali per conto di Wind, nonché modalità di contatto dei medesimi, in piena violazione della normativa sulla protezione dei dati personali. Inoltre, i dati illecitamente trattati da [S.] s.r.l.s. sono stati comunicati a [M.] s.r.l. senza che fra le due società intercorressero rapporti di titolarità/responsabilità idonei a consentire lo scambio dei dati medesimi ovvero senza che gli interessati avessero contezza e avessero autorizzato tali comunicazioni. I dati così acquisiti sono poi confluiti nei database della società Wind Tre S.p.A. per il perfezionamento delle proposte contrattuali. La società, in base a quanto stabilito dall'art. 1, comma 11, della legge n. 5/2018, è da ritenersi responsabile anche delle condotte poste in essere dalla società [S.] s.r.l.s. in violazione delle disposizioni della medesima legge».

[109] Per la sanzione nella sua interezza e per i criteri che hanno condotto alla determinazione dell'ammontare della stessa, si rimanda all'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e, in particolare, al par. 5.

Le sanzioni più elevate anche in riferimento alla violazione del principio di *accountability*, dall'entrata in vigore del GDPR ad oggi, sono state per lo più comminate nell'ambito del cosiddetto *telemarketing*[110] aggressivo[111].

Tra i pronunciamenti più significativi nel periodo compreso tra il 2021[112] e il 2022[113] si segnalano, senza pretesa di esaustività, sia la sanzione con cui il Garante ha ordinato a Fastweb S.p.A., in data 25 marzo 2021[114], il pagamento di una somma pari ad oltre 4 milioni e 500 mila euro sia il provvedimento inibitorio, prescrittivo e sanzionatorio adottato nei confronti di Edison Energia S.p.a. con cui in data 15 dicembre 2022[115] è stata applicata a quest'ultima società la sanzione amministrativa del pagamento della somma di euro 4 milioni e 900 mila, pari allo 0,1% dell'ultimo fatturato disponibile[116].

---

[110] Con provvedimento del GPDP n. 70 del 9 marzo 2023 è stato approvato il Codice di condotta per le attività di telemarketing e teleselling promosso da associazioni di committenti, *call center*, *teleseller*, *list provider* e associazioni di consumatori. Il Codice acquisterà efficacia una volta conclusa la fase di accreditamento dell'Organismo di monitoraggio (Odm) e la successiva pubblicazione in Gazzetta Ufficiale. L'Odm è un organismo indipendente chiamato a verificare l'osservanza del Codice di condotta da parte degli aderenti e a gestire la risoluzione dei reclami (cfr. www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9868813 verificato da ultimo in data 9 aprile 2023).

[111] L'autorità Garante ha evidenziato, in un comunicato diffuso in data 2 aprile 2021,di aver applicato fino a detta ultima data una serie di sanzioni, relative al cosidetto telemarketing aggressivo, per un importo complessivo pari a circa 70 milioni di euro (cfr. www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9570980 verificato da ultimo in data 9 aprile 2023). L'attenzione del Garante non si è comunque concentrata solo sui trattamenti dei dati personali posti in essere per attività di marketing e profilazione. A titolo esemplificativo ma non esaustivo, per l'anno 2023, si richiamano i seguenti pronunciamenti: GPDP, Provv. del 9 marzo 2023 n. 66, doc. *web* n. 9874604; GPDP, Provv. del 2 marzo 2023 n. 65, doc. *web* n. 9874480; GPDP, Provv. del 26 gennaio 2023 n. 25, doc. *web* 9863050.

[112] A titolo esemplificativo ma non esasutivo, per l'anno 2021, si richiamano anche i seguenti provvedimenti: GPDP, Provv. del 16 settembre 2021 n. 332, doc. *web* n. 9706389; GPDP, Provv. del 8 luglio 2021 n. 301, doc. *web* n. 9703122 e l'ordinanza ingiunzione del 16 dicembre 2021 n. 443, doc. *web* n. 9735672, annullata dal Tribunale di Roma in accoglimento del ricorso presentato dalla società destinataria del provvedimento.

[113] A titolo esemplificativo ma non esaustivo, per l'anno 2022, si richiamano anche i seguenti provvedimenti: GPDP, Provv. del 15 dicembre 2022 n. 429, doc. *web* n. 9852290; GPDP, Provv. del 1° dicembre 2022 n. 406, doc. *web* 9843805; GPDP, Provv. del 10 novembre 2022 n. 369, doc. *web* n. 9832838; GPDP, Provv. del 20 ottobre 2022 n. 348, doc. *web* n. 9825667; GPDP, Provv. del 28 luglio 2022 n. 272, doc. *web* n. 9812423; GPDP, Provv. del 24 marzo 2022 n. 107, doc. *web* n. 9767635.

[114] GPDP, Provv. del 2 aprile 2021, n. 112, doc. *web* n. 9570997.

[115] GPDP, Provv. del 15 dicembre 2022, n. 431, doc. *web* n. 9856345.

[116] Si rileva che il Garante, nel quantificare la sanzione elevata nei confronti della Edison Energia S.p.a., ha comunque tenuto conto quali elementi attenuanti, dell'assenza di procedimenti avviati a carico della società destinataria del provvedimento, del fatto che la società si è prontamente attivata presso l'Autorità giudiziaria per contrastare il fenomeno del *telemarketing* abusivo da parte di terzi, della tempestiva adozione di misure correttive, alcune delle quali avviate dopo la conclusione degli accertamenti ispettivi, dell'adozione, ancora prima dell'accertamento ispettivo, di misure atte ad evitare contatti fuori lista, dell'elevato grado di cooperazione nell'interazione con l'Autorità di controllo tale da rendere agevole, nonostante le dimensioni della società e della complessità dei trattamenti, lo svolgimento dell'attività di indagine in particolare nel delicato periodo di emergenza derivante dalla diffusione del Covid-19 ed, infine, della grave crisi socio-economica e dei suoi riflessi sull'andamento dell'occupazione.

Nel provvedimento testé richiamato e adottato nei confronti di Fastweb S.p.a. si legge, per quanto afferisce alla violazione del principio di *accountability*, che «si è già evidenziato che l'intero impianto del Regolamento si sostiene sulla *accountability* del titolare del trattamento. Questi, in ragione della circostanza che i dati personali dei soggetti contattati che abbiano aderito alle offerte promozionali sono destinati a confluire nei *database* societari, dovrebbe adottare misure di particolare garanzia al fine di comprovare che i contratti e le attivazioni registrati nei propri sistemi siano originati da contatti effettuati nel pieno rispetto delle disposizioni in materia di protezione dei dati personali (*omissis*); l'assenza di iniziative come sopra delineate (ossia di sistemi che richiedano ulteriori elementi per ogni attivazione oltre all'indicazione della lista di contatto), in particolare in presenza di un dato così rilevante in ordine alle chiamate disconosciute, ha determinato una grave falla nell'*accountability* di Fastweb (…)».

La mancata attenzione verso una conforme acquisizione del consenso è stata invece ritenuta sufficiente, anche ai fini della verifica del mancato rispetto del principio di *accountability*, dal Garante per emettere il provvedimento – già citato – nei confronti di Edison Energia S.p.a. In particolare, nel caso di specie, l'Autorità ha contestato che «la condotta di Edison, come prospettato già nella contestazione, risulta in contrasto con il principio di *accountability* poiché la Società non risulta essersi occupata, come invece necessario, di verificare l'effettiva conformità alla normativa dei consensi acquisiti dal fornitore».

3.4. L'*accountability* al suo esordio: le prime sanzioni delle autorità di controllo degli altri Paesi dell'EU

Le prime sanzioni delle autorità di vigilanza europee – emanate dopo un (breve) periodo di tolleranza immediatamente successivo a quello di avvio dell'applicazione del GDPR, voluto per consentire alle imprese di adeguarsi al nuovo sistema normativo – sono state caratterizzate da un elemento in comune e, cioè, l'inosservanza del principio di *accountability*.

Invero, sia che le sanzioni siano state adottate nei confronti di grandi società operanti sul mercato sia che abbiano interessato piccole (o singoli) realtà, l'analisi delle stesse – e delle ragioni sottese – fa emergere la condivisa difficoltà riscontrata dai titolari di adeguarsi al cambio di prospettiva che l'introduzione di detto principio fondamentale ha reso necessario.

La prima sanzione dell'autorità tedesca dello stato di Baden Württenberg (*Landesbeauftragte Für Den Datenschutz Und Die Informationsfreiheit – LfDI*), è stata emessa il 21 novembre 2018 nei confronti del *social network* «*Knuddels.de*»[117], un sito di *chat online* particolarmente conosciuto prima della raggiunta popolarità di Facebook. L'intervento del Garante teutonico si è reso necessario a seguito di un *data breach* che aveva portato alla diffusione di quasi due milioni di *username/password*

[117] Il comunicato stampa, contenente la sintesi del provvedimento, è consultabile all'indirizzo https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/11/LfDI-Baden-W%C3%BCrttemberg-verh%C3%A4ngt-sein-erstes-Bu%C3%9Fgeld-in-Deutschland-nach-der-DS-GVO.pdf (verificato da ultimo in data 9 aprile 2023).

e di circa 800 mila indirizzi e-mail[118]. A seguito dell'attività svolta per ricercare le ragioni dell'accadimento, è emersa la mancanza di misure di sicurezza adeguate a garantire la sicurezza dei dati degli utenti, ai sensi dell'art. 32 del GDPR che, appunto, a seguito di un attacco informatico, ha comportato la diffusione delle credenziali e delle restanti informazioni degli utenti[119]. La violazione del principio di *accountability* è stata alla base della sanzione che nel suo ammontare, pari a 20.000,00 euro, è stata determinata tenendo comunque conto dell'atteggiamento collaborativo che la società ha tenuto nei confronti dell'Autorità[120].

Un mese prima del provvedimento testé sintetizzato, l'Autorità austriaca (*Datenschutzbehörde*) ha erogato una sanzione, pari a 4.000,00 euro, nei confronti di un'azienda per l'utilizzo, in difformità delle indicazioni normative, del sistema di videosorveglianza: in particolare l'autorità di controllo competente, nel caso oggetto del pronunciamento, ha contestato la mancanza di idonea cartellonistica volta ad informare i terzi della presenza di telecamere ed inoltre la circostanza che le stesse erano state posizionate oltre il perimetro aziendale, inquadravano anche vicini spazi come il marciapiede[121].

Superiore rispetto ai precedenti indicati è invece l'importo – pari a 400.000,00 euro – della sanzione che l'Autorità portoghese, *Comissão Nacional de Proteção de Dados* (CNPD), ha erogato, sempre nell'anno 2018, nei confronti di una struttura ospedaliera, il *Centro Hospitalar Barreiro Montijo*[122]: all'ospedale, l'autorità di controllo competente aveva contestato il fatto che il personale (sanitario e non) poteva non solo accedere[123] ma persino modificare i dati particolari[124] dei pazienti ospiti. Nel corso dell'attività ispettiva è emerso chiaramente, in violazione del principio di *accountability*, che non erano state in alcun modo definite *procedure* atte a stabilire le regole per la creazione degli *account* e/o in ogni caso idonee a monitorare il sistema di trattamento dati.

4. Riflessioni conclusive

L'esame dell'inquadramento normativo del principio di *accountability*, l'indagine relativa alla portata dello stesso, la breve analisi di alcuni tra i primi provvedimenti assunti dalle Autorità europee, così come l'analisi articolata di due tra i prov-

[118] LfDI BW, 21 novembre 2018, O 1018/115.

[119] LfDI BW, 21 novembre 2018, O 1018/115.

[120] In riferimento all'intervento dell'Autorità tedesca, si precisa che la sanzione è stata comminata non per l'avvenuta intrusione nei sistemi informatici da parte dell'attaccante bensì perché i dati rilasciati dagli utenti erano conservati nelle memorie informatiche societarie senza l'utilizzo di necessari sistemi di cifratura (LfDI BW, 21 novembre 2018, O 1018/115).

[121] Sul punto si legga S. Fratepietro, *GDPR, prime sanzioni in Europa: quale lezione trarre per le aziende*, in *www.agendadigitale.eu*.

[122] Deliberazione CNPD 984/2018 – procedimento 9932/2018.

[123] A fronte di un numero di 296 medici, ben 985 gli *account* che avevano accesso ai dati, alcuni appartenenti anche a soggetti non più dipendenti della struttura sanitaria le cui credenziali di accesso non erano state disattivate.

[124] Per la definizione di dati particolari si rimanda all'art. 9 del GDPR.

vedimenti più significativi assunti dal Garante italiano dall'anno 2020[125] confermano come la rivoluzione operata dal GDPR, con l'introduzione del principio in esame, sia stata sin dal suo esordio un percorso in salita e non privo di ostacoli: un lento (ma inesorabile) processo di presa di coscienza, di "assunzione di responsabilizzazione", ancora in divenire, che impegna tutti i titolari del trattamento dei dati a prescindere, quindi, dalle dimensioni della società e/o dell'ente

Chiunque sia il titolare del trattamento dei dati, è comunque chiamato a dimostrare di aver adottato tutte le misure previste dal Regolamento e di essere quindi *compliant* con quelli che sono i dettami pensati e voluti per tutelare i dati oggetto di trattamento.

Questo si traduce, in termini concreti non solo in una preliminare e puntuale, nonché costante, verifica del rispetto dei principi generali del GDPR[126] ma, anche, in contestuali azioni come, a titolo esemplificativo, la tenuta del registro dei trattamenti, l'acquisizione del consenso ove necessario, la predisposizione della valutazione di impatto, se e quando richiesta, la nomina (o la mancata motivata nomina) del DPO, la stipula di scrupolosi *data processing agreement ex* art. 28 GDPR e di ogni altro adempimento necessario a definire, sia *ex ante* che *ex post*, come *compliant* la condotta del titolare del trattamento dati.

Il DPO, ove nominato, ha un ruolo da protagonista nel presidio del principio di *accountability*: sia nel momento in cui informa e fornisce consulenza al titolare del trattamento dati, nonché ai suoi dipendenti, sia nella sua attività di sorveglianza, sia quando viene coinvolto in merito alla valutazione di impatto e della vigilanza al momento dello svolgimento della stessa[127], il Responsabile della protezione dei dati può determinare, in meglio, le scelte dei soggetti che presiedono o che sono preposti al trattamento dei dati[128], orientandole verso la conformità ai dettami normativi, sin dall'inizio del trattamento e nell'adozione di tutte le misure necessarie alla riduzione dei rischi legati all'utilizzo dei dati.

Dallo studio dei provvedimenti che si sono analizzati è emerso come il Garante abbia rimarcato più volte che l'*accountability* passa attraverso l'esame degli orientamenti che l'autorità di controllo ha espresso valutando le fattispecie sottoposte alla

[125] Nell'anno 2020 le Autorità europee hanno erogato, complessivamente, sanzioni per un importo pari ad oltre 307 milioni di euro: in media, ciascuna Autorità, ha erogato 11,3 sanzioni. Tra queste spiccano quelle più severe emerse dall'Autorità francese che, con soli 8 procedimenti, ha erogato sanzioni per un importo di 138,3 milioni di euro. Le violazioni sono state emesse, in particolare, nei confronti del settore delle telecomunicazioni destinatario di 69 provvedimenti. Quella inflitta dal Garante italiano a Tim S.p.a., oggetto anche del presente approfondimento, è stata la più elevata. A fini di un migliore approfondimento, si rimanda allo studio di Federprivacy sul punto al seguente indirizzo https://www.federprivacy.org/informazione/societa/violazioni-privacy-307-milioni-di-euro-di-sanzioni-in-europa-nel-2020 (verificato da ultimo in data 9 aprile 2023).

[126] Si fa riferimento ai principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

[127] Si rimanda all'art. 39 del GDPR nella sua interezza e, relativamente al ruolo del DPO, in termini generali, si rinvia al prezioso contributo di A. AVITABILE, *Il responsabile della protezione dei dati*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 335 ss.

[128] Ci si intende riferire qui sia ai titolari che ai responsabili del trattamento dati.

sua attenzione: nei provvedimenti con cui il Garante decide sulla casistica concreta viene individuata la corretta applicazione delle norme del Regolamento che i titolari, nella prospettiva dell'*accountability*, non possono non conoscere. Di qui l'importante ruolo del DPO che, con i compiti di informazione e consulenza attribuitagli dal GDPR, è chiamato a veicolare gli indirizzi espressi dal Garante nei provvedimenti con cui decide sulla casistica concreta, consentendo il recepimento di detti indirizzi interpretativi sul piano operativo.

Nelle realtà ove, invece, la figura del DPO non è designata, perché non obbligatoria né ritenuta necessaria la nomina, la concretizzazione del principio in esame implica uno sforzo ulteriore in termini di cambio di prospettiva[129] che investe, inevitabilmente, con maggiore forza, tutti i processi aziendali e tutte le risorse umane aziendali, ciascuna nel proprio ruolo e rispetto ai propri compiti. Ancor più significativamente indispensabile, in tale contesto, appare il ruolo della formazione, sia delle figure apicali che dei dipendenti, in materia di protezione dei dati personali: la formazione dovrà essere capillare al fine di generare un meccanismo virtuoso che prende il via, qualsiasi sia il livello, con la presa di coscienza del concetto di dato personale, passa poi per la consapevolezza del significato di trattamento dello stesso e si conclude, infine, con l'utilizzo corretto – e protetto da idonee misure – delle informazioni a disposizione del titolare del trattamento.

Quel che preme rilevare, in ultima analisi, è come l'*accountability* sia un principio che deve essere di volta in volta declinato rispetto alla singola fattispecie: tale operazione va necessariamente condotta sia nel momento in cui si intende valutare il rispetto dello stesso, quindi *ex post*, sia, prima, nel momento in cui si adottano le misure idonee.

[129] Si fa riferimento, in particolare, alla necessità, specie nelle piccole e medie realtà, di rafforzare l'idea che sia necessario individuare, preventivamente, quante più possibili azioni tese a tutelare il dato personale di valore significativo. La resistenza, che in ogni caso non investe solo le PMI, è legata a spese giudicate, aprioristicamente, antieconomiche. In realtà – e qui sta il cambio di prospettiva – si tratta di costi volti a supportare un nuovo modello di gestione che, peraltro, può positivamente investire altri aspetti della conduzione dell'attività economica, con potenziali ricadute anche sull'immagine ed il buon nome della stessa. Si pensi, ad esempio, ai grandi operatori sul mercato che richiedono, nell'ambito delle proprie previsioni contrattuali, elevati standard di *compliance* anche rispetto alla tutela dei dati personali. Con riferimento più specificatamente al panorama italiano, si consideri in ogni caso che, piccole e medie realtà, al pari delle grandi, si misurano o si misureranno con norme come quelle del d.lgs. n. 81 del 2008 o, di recente, del Codice della crisi di cui al d.lgs. n. 14 del 2019, che sono costruite intorno al principio di *accountability*.

Capitolo XIV
Il principio di solidarietà

Fabio Bravo

Sommario: 1. Inquadramento normativo. – 1.1. La solidarietà come principio normativo e la sua declinazione nel settore della datificazione della società, dell'economia e delle istituzioni. – 1.2. Il principio di solidarietà nel GDPR e nel *Data Governance Act* (Reg. UE 868/2002) e il *data altruism*. – 2. Portata del principio. – 2.1. Le direzioni del principio di solidarietà al cospetto (del trattamento) dei dati personali: (i) la solidarietà come "limite" per il titolare del trattamento. – 2.2. (*segue*): (ii) …e per l'interessato. La «funzione sociale» al cospetto (del trattamento) dei dati personali. – 2.3. (*segue*): (iii) la solidarietà come "orizzonte", secondo le logiche dell'inclusione. – 2.4. (*segue*): (iv) …e secondo le logiche della condivisione e dell'altruismo (*data altruism*). – 3. Applicazione del principio nella casistica. – 3.1. Il principio di solidarietà nei provvedimenti del Garante. – 3.2. Il principio di solidarietà nelle pronunce della Cassazione in tema di «funzione sociale» e in tema di risarcimento del danno da illecito trattamento di dati personali (ed altre significative sentenze della giurisprudenza di merito). – 3.3. Riflessioni critiche sulla deriva giurisprudenziale in tema di "solidarietà-tolleranza" e sui filtri selettivi della "gravità della lesione" e della "serietà del danno". Le peculiarità in tema di protezione dei dati personali. – 3.4. La sentenza della Corte di giustizia dell'UE del 4 maggio 2023 (C-300/21) sull'inammissibilità di soglie minime di risarcibilità del danno non patrimoniale relative alla gravità del danno (ed alla serietà della lesione) in materia di protezione dei dati personali e il parziale *revirement* della Corte di Cassazione.

1. Inquadramento normativo

1.1. La solidarietà come principio normativo e la sua declinazione nel settore della datificazione della società, dell'economia e delle istituzioni

Il principio di solidarietà è un principio normativo[1], la cui delimitazione concreta ha sofferto di una certa ambiguità, per essere stato a lungo confinato al "mondo delle idee"[2], a tal punto da farlo apparire come un principio "utopistico", benché si tratti – come rimarcato da Stefano Rodotà – di un'«utopia necessaria»[3].

È principio di rilevanza costituzionale, presente negli ordinamenti nazionali e in quello europeo[4]. La vaghezza della sua accezione e le connotazioni – anche ide-

[1] G. Alpa, *Solidarietà. Un principio normativo*, Bologna, 2022, *passim*; G. Alpa, *Note sul principio di solidarietà come principio precettivo nel diritto interno e nel diritto dell'Unione europea*, in *Lo Stato*, 2022, 18, pp. 11-56.

[2] *Ibidem*.

[3] S. Rodotà, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2016, *passim*.

[4] G. Alpa, *Note sul principio di solidarietà come principio precettivo nel diritto interno e nel diritto dell'Unione europea*, in *Lo Stato*, 2022, 18, pp. 11-56, nonché Id., *Solidarietà. Un principio norma-*

ologiche – che in molteplici direzioni ne hanno espanso l'accezione[5], non ne fanno vacillare la dimensione giuridica, né la sua valenza normativa[6].

Non è però solamente la vaghezza della sua accezione ad averne compromesso, per molto tempo, la sua "giuridificazione"[7], quanto piuttosto – come ben rilevato da Stefano Rodotà – l'antagonismo con la tutela del diritto di "proprietà"[8]. Quest'ultima, nel suo manifestarsi quale *jus excludendi alios*, nel tipico atteggiarsi dei diritti assoluti, s'è palesata come l'antitesi stessa della "solidarietà" (o "fraternità", nella declinazione francese «*liberté, égalité, fraternité*»), a cui pertengono, invece, le opposte logiche dell'inclusione e della condivisione[9]. Nella contrapposizione tra l'una e l'altra s'è individuata la ragione prima della «debolezza della fraternità [che] non può essere fatta derivare da un suo carattere astratto, da un suo intimo formalismo. È piuttosto una sorta di sua incompatibilità con la sempre più trionfante logica proprietaria a determinarne l'emarginazione in un contesto così precocemente mutato. Siamo di fronte a un classico conflitto tra inclusione (fraterna) e esclusione (proprietaria) (…)»[10].

Proprio su tali rilievi merita di essere ricordato come originariamente, nel celeberrimo saggio di Samuel Warren e Louis Brandeis, anche il diritto alla *privacy* era modellato sulle logiche dell'esclusione: «*the right to privacy*» era inteso come «*the right to be let alone*» e, dunque, come *ius excludendi alios*, non dal luogo in cui

---

tivo, cit.

5 Per l'indagine sulle connotazioni ideologiche del principio di solidarietà, incluso quella cattolica e quella socialista, cfr. G. ALPA, *I principi generali*, in *Trattato di diritto privato*, a cura di G. Iudica e P. Zatti, Milano, 2006, 2a ed., pp. 395 ss.

6 G. ALPA, *Solidarietà. Un principio normativo*, cit., *passim*

7 Sui temi della giuridificazione e sulle sue accezioni cfr. G. RESTA-V. ZENO ZENCOVICH, *La storia "giuridificata"*, in G. RESTA-V. ZENO ZENCOVICH (a cura di), *Riparare Risarcire Ricordare. Un dialogo tra storici e giuristi*, Napoli, pp. 11 ss.; B. MARCHETTI-M. RENNA (a cura di), *La giuridificazione*, Firenze, 2016 (vol. III di *A 150 anni dall'unificazione amministrativa italiana. Studi*, a cura di L. FERRARA-D. SORACE). In termini sostanzialmente equivalenti si parla anche di "giuridicizzazione". Quanto alla solidarietà come fenomeno di giuridificazione o giuridicizzazione della "fraternità", seppur in ambito pubblicistico, si rimanda al contributo di A. MATTIONI, *Solidarietà giuridicizzazione della fraternità. La fraternità come principio di diritto pubblico*, Roma, 2007, pp. 7-43.

8 S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., pp. 21 ss.

9 Per tale prospettiva si veda, ad es., S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., pp. 21 ss., ove si trova rimarcato che «Della triade francese rivoluzionaria proprio la fraternità si rivelò precocemente la componente più debole, o quella più difficilmente accettabile, tanto che Napoleone, nel suo proclama del 18 brumaio, si sarebbe presentato ai francesi come il difensore di "libertà, eguaglianza, proprietà". La fraternità non compare, sopraffatta dal primato della proprietà, diritto a escludere gli altri dal godimento di un bene, dunque destinato a spezzare quel legale tra gli uomini che attraverso la fraternità si intende stabilire. In quel momento, il diritto non è più "fraterno", s'imbatte nella durezza del nudo potere del proprietario, che separa e non unisce, e così rende impossibile il vero compito affidato alla fraternità, quello di "costruire (o produrre) la Nazionale", intuizione precoce del ruolo riconosciuto in tempi successivi alla solidarietà come antidoto alla frammentazione sociale. E quella sua scomparsa renderà più deboli pure libertà e uguaglianza, subordinate anch'esse a una logica che indicava nella proprietà la misura pria dei rapporti tra le persone». Così, aggiunge ancora Rodotà, «Quando, nel Novecento, si vorrà costruire un contesto costituzionale che individui i limiti della proprietà, sarà appunto al principio di solidarietà che si farà riferimento» (*Ibidem*, p. 22).

10 S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., p. 23.

si celebra la propria vita privata – com'è invece per il diritto di proprietà, con cui si tutela anche il domicilio o la residenza e, con esso, la vita privata e familiare in essa condotta nella dimensione della riservatezza – bensì come *ius excludendi alios* dalla sfera privata e familiare *tout court*, in senso assoluto, indipendentemente dal luogo in cui la dimensione personale e familiare trovano il loro svolgimento[11]. S'è passati dunque alla protezione *indiretta* della persona, tramite la tutela del luogo in cui la vita privata e familiare si svolgono, alla protezione *diretta* della persona in quanto tale, ossia della sfera personale e familiare, indipendentemente dal luogo in cui essa snoda le proprie vicende. La proprietà, prima dell'affermazione del diritto alla *privacy*, aveva cioè una duplice funzione: da un lato quella "*reale*", tipica del *ius in re propria*, dall'altro lato quella relativa alla tutela della propria riservatezza, personale e familiare, che tramite la *res* il proprietario riusciva ad assicurarsi indirettamente, escludendo dal proprio dominio tutti i soggetti non graditi.

Da tale tutela, mediata, delle prerogative che il soggetto vanta sulla *res* attraverso la tutela della proprietà, si è passati, con la teorizzazione di Warren e Brandeis, a riconfigurare gli strumenti di tutela della riservatezza: la *privacy* è divenuta non più un effetto indiretto della tutela del diritto sulla *res*, ma autonomo diritto inquadrabile nel novero dei diritti fondamentali della persona, tutelando quest'ultima in quanto tale.

Il passaggio è importante, perché, con la configurazione del diritto alla *privacy* quale diritto della persona, nel Novecento si affievolisce al contempo la tutela della proprietà: quest'ultima, di fronte all'affermazione di specifici strumenti per tutelare la *privacy* individuale e familiare, perde la sua "sacertà", tipicamente riconosciutale nel Settecento e nell'Ottocento[12] in cui il diritto di proprietà veniva ricondotto anche

[11] Cfr. S. Warren-L. Brandeis, *The right to privacy*, in *Harvard Law Review*, 1890, 4, pp. 193 ss. Si veda anche V. Frosini (a cura di), *Jus solitudinis*, Milano, 1993.

[12] Si pensi, in Francia, all'art. 17 della Dichiarazione dei diritti dell'uomo e del cittadino, approvata a Parigi dall'Assemblea Nazionale il 26 agosto del 1789, ove veniva statuito che «La *proprietà* essendo un *diritto inviolabile* e *sacro*, nessuno può esserne privato, salvo quando la necessità pubblica, legalmente constatata, lo esiga in maniera evidente, e previa una giusta indennità». La predetta Dichiarazione, con tutti i diritti ivi contemplati, venne materialmente replicata anche all'interno del Preambolo della Costituzione liberale francese del 1791, ove si legge: «I rappresentanti del popolo francese, costituiti in Assemblea nazionale, considerando che l'ignoranza, l'oblio o il disprezzo dei diritti dell'uomo sono le sole cause delle sventure pubbliche e della corruzione dei governi, hanno deciso di esporre, in una solenne dichiarazione, i diritti naturali, inalienabili e sacri dell'uomo, affinché questa dichiarazione, costantemente presente a tutti i membri del corpo sociale, rammenti loro continuamente i loro diritti e i loro doveri; affinché gli atti del potere legislativo e quelli del potere esecutivo ritraggano maggior rispetto dal poter essere in ogni istante messi a confronto con il fine di ogni istituzione politica; affinché i reclami dei cittadini, avendo d'ora in poi a proprio fondamento princìpi incontestabili, abbiano sempre per risultato il mantenimento della costituzione e la felicità di tutti. In conseguenza, l'Assemblea nazionale riconosce e dichiara in presenza e sotto gli auspici dell'Essere Supremo, i seguenti diritti dell'uomo e del cittadino. (…) Art. 17 – La *proprietà* essendo un *diritto inviolabile* e *sacro*, nessuno può esserne privato, salvo quando la pubblica necessità, legalmente constatata, lo esiga in maniera evidente, e a condizione di una giusta e preventiva indennità». Nel preambolo della Costituzione francese del 1958 i diritti contenuti nella Dichiarazione non vengono più materialmente trascritti, ma sono comunque formalmente richiamati: «Il Popolo francese proclama solennemente la sua fedeltà ai diritti dell'uomo e ai principi della sovranità nazionale

tra i diritti fondamentali dell'uomo[13], e viene piegata ad esigenze di solidarietà, in ragione della sua conclamata «funzione sociale»[14].

Il discorso riguarda anche la nuova connotazione del diritto alla *privacy* quale diritto alla protezione dei dati personali, che rimane intriso del principio di solidarietà nelle venature della nuova disciplina del GDPR, ad iniziare dal *considerando* n. 4, ove si afferma che «Il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua *funzione sociale* e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[15] e,

definiti dalla Dichiarazione del 1789, confermata ed integrata dal preambolo della Costituzione del 1946, e ai diritti e doveri definiti nella Carta dell'ambiente del 2004».
In sintonia con la dichiarazione di sacertà contenuta nella Dichiarazione di Parigi del 1789 e con la successiva Costituzione del 1791, il *Code Civil* del 1804 stabiliva, all'art. 544, che «*La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les réglemens*» (La proprietà è il diritto di godere e disporre delle cose *nel modo più assoluto*, a condizione che non se ne faccia un uso vietato da leggi o regolamenti) e, all'art. 545, che «*Nul ne peut être contraint de céder sa propriété, si ce n'est pour cause d'utilité publique, et moyennant une juste et préalable indemnité*» (Nessuno può essere costretto a cedere la propria proprietà, se non nell›interesse pubblico e in cambio di un equo e preventivo compenso).
In Italia, lo Statuto albertino del 1848 riferiva la sacertà e l'inviolabilità solamente alla figura del Re (v. art. 4, secondo cui «La persona del Re è *Sacra* ed *inviolabile*»), mentre la proprietà veniva definita *tout court* "*inviolabile*", ma *non* "*sacra*", subordinabile all'interesse pubblico legalmente accertato secondo i principi già sperimentati nell'ordinamento francese (v. art. 29, ai sensi del quale «Tutte le proprietà, senza alcuna eccezione, sono *inviolabili*. Tuttavia quando l'interesse pubblico legalmente accertato lo esiga, si può esser tenuti a cederle in tutto od in parte mediante una giusta indennità conformemente alle leggi»).
Oggi la *sacertà* e l'*inviolabilità* della proprietà è affermata in tutt'altro contesto nella Costituzione cinese del 1982 (*verbatim*, all'art. 12, co. 1), ma con riferimento alla sola *proprietà pubblica* non invece, non invece a quella *privata*, nonostante gli emendamenti apportati con la riforma del 1999 da cui è emersa l'apertura verso le altre forme di proprietà, inclusa, appunto, la proprietà privata (su tali aspetti del diritto cinese si veda, in particolare, L. MOCCIA, *Il sistema giuridico cinese: caratteri tradizionali e lineamenti attuali*, in *Riv. trim. dir. proc. civ.*, 2000, 4, pp. 1251 ss.).

[13] Il diritto di proprietà era infatti annoverato tra «i diritti naturali, inalienabili e sacri dell'uomo», nell'ordinamento francese di fine Settecento, all'interno della Dichiarazione dei diritti dell'uomo e del cittadino del 1789 e nella successiva Costituzione liberale francese, con richiami anche nelle successive Costituzioni (v. nota precedente). Oggi il diritto di proprietà viene considerato quale «diritto fondamentale» della persona al rispetto dei propri beni in virtù dell'art. 17 della Carta dei diritti fondamentali dell'UE (in materia si rimanda alle pregevoli riflessioni di D. MEMMO, *Proprietà e autonomia privata alla luce della giurisprudenza delle Corti europee*, in *Contratto e impresa*, 2016, 6, pp. 1299 ss.).

[14] Con riguardo alla funzione sociale della proprietà si vedano, tra tutti, S. PUGLIATTI, *La proprietà nel nuovo diritto*, Milano, 1964; M. COSTANTINO, *Contributo alla teoria della proprietà*, Napoli, 1967, pp. 25 ss.; P. RESCIGNO, *Per uno studio sulla proprietà*, in *Riv. dir. civ.*, 1972, I, p. 5 ss.; S. RODOTÀ, *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, 9a ed., Bologna, 2013 (1a ed., 1981), *passim*; A. GAMBARO, *Il diritto di proprietà*, in *Tratt. dir. civ. comm.*, diretto da Cicu-Messineo-Mengoni, VIII, 2, Milano, 1985, pp. 213 ss.; F. GALGANO, *Trattato di diritto civile e commerciale*, Padova, 2009, I, pp. 334 ss.

[15] Per un'analisi più estesa si rimanda all'approfondimento di A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 2, pp. 586 ss.

nell'art. 5, par. 1, lett. *a)*, del medesimo Regolamento, ove si declama il principio di «*correttezza*»[16], a cui va informato ogni trattamento dei dati personali[17].

Com'è stato per la proprietà, anche il diritto alla *privacy* – finanche nella sua accezione attuale, comprensiva del diritto (non necessariamente escludente) alla protezione dei dati personali – s'è dovuto confrontare con il *principio di solidarietà*, che insieme finisce per rappresentare un "*limite*", nella prospettiva dell'inclusione e dell'apertura, e un "*orizzonte*", nella logica della condivisione. Si tratta di un confronto che va collocato in un più lungo percorso di maturazione, destinato a intraprendere la strada dell'utilizzabilità ulteriore dei dati, rispetto all'originaria finalità del trattamento (c.d. *secondary use*), per giungere – da ultimo – alla dimensione altruistica del trattamento, scolpita nel *Data Governance Act* (Reg. UE n. 868/2022).

Nella nostra Costituzione, com'è noto, il principio di solidarietà ha una valenza forte, impressa con chiarezza nell'art. 2 Cost., ove, dopo la declamazione con cui viene affermato il riconoscimento e la tutela dei diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, compare anche l'affermazione in ordine al necessario adempimento dei *doveri* inderogabili di *solidarietà* politica, economica e sociale[18]. Proprio in tema di danni da illecito trattamento di dati personali, tali doveri costituzionali di solidarietà sono stati percorsi dalla giurisprudenza della Suprema Corte per negare richieste risarcitorie ove, pur a fronte del positivo accertamento della condotta illecita e dell'esistenza del danno, quest'ultimo si dimostri di lieve entità, attenendo a questioni considerate "bagatellari"[19].

Il riferimento alla solidarietà pervade la nostra Carta costituzionale anche in altri numerosi passaggi, segno di una matura attenzione a tale principio, che viene declinato in diversi contesti, facendo in modo che la genericità e l'astrattezza del concetto possa trovare migliore collocazione in ambiti diversi, evitando una per-

[16] Sulla relazione tra principio di correttezza e principio di solidarietà si vedano, nel presente volume, i richiami riportati nel Cap. III, par. 2.1. e, ivi, spec. nota n. 31.

[17] In materia di *data protection*, ora disciplinata nell'ordinamento eurounitario dal GDPR (Reg. UE n. 679/2016), il principio di solidarietà ha assunto dunque forme variegate (soprattutto nelle riferite direzioni della «*correttezza*» dei comportamenti da parte del titolare del trattamento, per un verso, e della «*funzione sociale*» riconosciuta al diritto alla protezione dei dati personali nel suo bilanciamento con altre esigenze di tutela, per altro verso). V'è però da precisare, anticipando quanto più diffusamente si dirà nel par. 3 del presente scritto, che tale principio non ha avuto un'applicazione evidente nei provvedimenti del Garante, ove i riferimenti espliciti alla «solidarietà» sono del tutto sporadici.

[18] Sul punto v. G. Alpa, *I principi generali*, cit., pp. 393 ss.

[19] Cfr., *amplius*, par. 3 del presente contributo. Si tratta di un indirizzo giurisprudenziale di grande impatto in tema di protezione dei dati personali, che tuttavia non convince per una serie di motivi, inclusa la compatibilità con la nostra Carta costituzionale e con il diritto europeo: proprio in materia di danni da illecito trattamento di dati personali si è pronunciata, di recente, la C.G.U.E. con sent. 4 maggio 2023, resa nella causa C-300/21, negando, *inter alia*, l'ammissibilità di filtri selettivi sulla gravità del danno e dell'entità della lesione ai fini della risarcibilità del danno ai sensi dell'art. 82 GDPR. Sul punto v., F. Bravo, *Il principio di solidarietà tra* Data Protection *e* Data Governance, in *Dir. inf.*, 2023, 3, pp. 488 s. e, ivi, nt. 20 e, nel presente capitolo, il par. 3.4.

dita o una riduzione dell'efficacia normativa del principio medesimo[20]. In ambito privatistico, il principio di solidarietà è significativamente presente nelle pronunce giurisprudenziali ed emerge soprattutto per l'applicazione della clausola di buona fede e correttezza, che nel codice civile ha precisi riferimenti nell'art. 1175 c.c., per i rapporti obbligatori (inclusi quelli incentrati sul trattamento dei dati personali) e negli art. 1337 3366 e 1375, con riguardo ai rapporti contrattuali[21].

Più tenue è il riferimento alla solidarietà in altri contesti, di carattere internazionale. Ad esempio, «Nelle carte universali dei diritti la solidarietà non è citata in modo espresso, ma è un valore soffuso sia nella Dichiarazione del 1948 sia nella Convenzione europea del 1950, ove si richiamano i doveri e le responsabilità dei singoli»[22]. Nell'ordinamento dell'UE, però, il riferimento alla solidarietà è esplicito e ben radicato nella Carta dei diritti fondamentali dell'UE, posta al vertice delle fonti dell'ordinamento. Ivi compare sia nel preambolo («l'Unione si fonda sui valori indivisibili e universali di dignità umana, di libertà, di uguaglianza e di *solidarietà*»), sia nell'intitolazione del Capo IV («*Solidarietà*»), ove vengono affrontati, in particolare, i temi del lavoro, della vita privata e professionale, della sicurezza sociale e dell'assistenza sociale, della protezione della salute, dell'accesso ai servizi di interesse economico generale, della tutela dell'ambiente e della protezione dei consumatori.

Con particolare riguardo all'innovazione tecnologica e alla datificazione della società, dell'economia e delle istituzioni l'UE ha posto recentemente una rinnovata attenzione al principio di solidarietà, a cui è dedicata, nella prospettiva dell'inclusione (appunto, contrapposta alle logiche dell'esclusione a cui s'è fatto riferimento in apertura del discorso), il *Chapter II* dell'«*European Declaration on Digital Rights and Principles for the Digital Decade*», resa dalla Commissione europea il 26 gennaio 2022, COM(2022)28 final, , per poi essere formalmente adottata dal Parlamento europeo, dal Consiglio e dalla Commissione il 23 gennaio 2023[23].

Nel citato *Chapter* II, intitolato «*Solidarity and inclusion*», viene affermato che «*Technology should be used to unite, and not divide people. The digital transformation should contribute to fair and inclusive society and economy in the UE*»[24]. Qui

[20] Per un attento esame della declinazione del principio normativo di solidarietà nella nostra Costituzione si veda, ancora, G. ALPA, *I principi generali*, cit., pp. 393 ss., nonché, più recentemente, G. ALPA, *Solidarietà. Un principio normativo*, cit., cap. VI; nonché, con una lettura giuspubblicistica, A. MORELLI, *I principi costituzionali relativi ai doveri inderogabili di solidarietà*, in *Forum di Quaderni Costituzionali*, 2015, pp. 1 ss.

[21] Diffusamente, sul punto, si veda l'ampia ricostruzione di G. ALPA, *Solidarietà. Un principio normativo*, cit., p. 231 ss., ove si parla anche di «solidarietà costituzionale nei rapporti tra privati», con riferimento alla quale vengono discussi casi emblematici afferenti al recesso *ad nutum*, alla riduzione d'ufficio della clausola penale, all'inerzia del creditore, alla nullità selettiva, all'esclusione della polizza fideiussoria, tenendo poi presente che la solidarietà opera, in ambito privatistico, anche nei rapporti tra coniugi, nel trattamento dei figli, nelle dinamiche associative e societarie, soprattutto nelle società cooperative e mutue, oltre che in tema di responsabilità sociale d'impresa e nei programmi di sostenibilità e così via.

[22] Così G. ALPA, *I principi generali*, cit., p. 393.

[23] La *European Declaration on Digital Rights and Principles for the Digital Decade* è stata pubblicata in G.U.U.E., nella sua versione definitiva, in data 23 gennaio 2023 (2023/C 23/1). Su di essa si veda, più diffusamente, quanto riportato nel Cap. I, par. 5, del presente volume.

[24] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., Chapter II.

la solidarietà e inclusione sono intese, nel contesto tecnologico, come un'endiadi, in antagonismo con la prospettiva dell'esclusione tipica della proprietà e dell'originaria concezione del diritto alla *privacy*. Nel preambolo la solidarietà è richiamata, insieme all'inclusione, con riguardo alla visione antropocentrica che dovrebbe connotare le scelte dei decisori politici nella transizione al digitale, così come le scelte delle imprese e degli altri soggetti interessati nello sviluppo e nella diffusione delle nuove tecnologie. Solidarietà e inclusione, percepite unitariamente, insieme agli altri valori fondativi dell'UE, devono essere poste a base della «transizione digitale che mette al centro le persone»[25].

Ancora, nel citato *Chapter II* si trova ulteriormente affermato, quale impegno delle istituzioni dell'UE a realizzare la solidarietà e l'inclusività nel nuovo contesto tecnologico: «*We commit to*: (i) *making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their exercise and promote solidarity and inclusion*; (ii) *a digital transformation that leaves nobody behind. It should benefit everyone, archieve gender balance, and include notably elderly people, people living in rural areas, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. It should also promote cultural and linguistic diversity*; (iii) *developing adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all people living in the EU*».

Le iniziative concrete richiamate nella *European Declaration on Digital Right and Principles for the Digital Decade* sono enunciate in quattro specifiche direzioni: (1) *Connectivity*; (2) *Digital education, training and skills*; (3) *Fair and just working conditions*; (4) *Digital public services online*[26].

Si tratta cioè di azioni volte a creare i presupposti per l'accesso agli strumenti e ai servizi digitali e per le effettive condizioni di loro utilizzo, nei cui confronti la libera circolazione dei dati, bilanciata dalle esigenze di protezione riconosciute dall'ordinamento europeo, è il presupposto necessario di funzionamento.

La visione normativa-programmatica del principio di solidarietà, che lascia intravedere l'orizzonte di manovra delle istituzioni eurounitarie, va tuttavia correlata alla visione normativa-precettiva del medesimo principio, che si coglie maggiormente nella dimensione della *data protection* e della *data governance*.

---

[25] *European Declaration on Digital Rights and Principles for the Digital Decade*, cit., Chapter I e Chapter II. Significativamente, poi, nel testo definitivo della Dichiarazione si trova ora affermato, al n. 1 del Preambolo, che «*The European Union (EU) is a 'union of value', as enshrined in Article 2 of the Treaty on European Union, founded on respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. Moreover according to the Charter of fundamental rights of the European Unione, the EU is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity. (...)*».

[26] Per tali direzioni in cui viene declinato il principio di solidarietà e di inclusione si veda, *amplius*, il par. 2.2.

1.2. Il principio di solidarietà nel GDPR e nel *Data Governance Act* (Reg. UE 868/2002) e il *data altruism*

Il principio di solidarietà acquista, come s'è già avuto modo di rimarcare, sfumature diverse. Dalla riferita declinazione nel senso dell'inclusione, in antagonismo con la prospettiva escludente della proprietà e della riservatezza – nell'originaria accezione del diritto alla *privacy* quale diritto di escludere gli altri dalla dimensione della propria sfera privata, personale e familiare – il principio di solidarietà ha, nella disciplina della *data protection*, il senso della correlazione con altri diritti fondamentali, ovvero della necessità di un bilanciamento proporzionale degli interessi, facendo in modo che le logiche della protezione dei dati non vadano ad impedire quelle del *free movement of personal data*.

Il testo del GDPR, nel rimarcare ciò, presenta alcune forzature lessicali, che si registrano soprattutto nell'art. 1, ove, nello stabilire l'oggetto e le finalità del Regolamento, dopo aver individuato, al par. 1, la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati quale oggetto della disciplina normativa e dopo aver affermato, al par. 2, l'esigenza di proteggere i diritti e le libertà fondamentali delle persone fisiche con riguardo, in particolare, al diritto alla protezione dei dati personali – scolpito nei suoi tratti essenziali all'art. 8 della Carta dei diritti fondamentali dell'UE – il legislatore europeo s'è preoccupato di precisare al par. 3, con una formulazione piuttosto ambigua, che «La libera circolazione dei dati personali dell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali»[27]. Non si è voluto affermare, ovviamente, la supremazia dell'un principio all'altro, secondo logiche assiologiche valutate aprioristicamente, ma la necessità di effettuare un bilanciamento proporzionale, che tenga conto di come la fattispecie concreta di volta in volta si atteggi, cercando di fare in modo che – a fronte di tale bilanciamento – non venga meno, nella sua essenza ed al cospetto dell'affermazione del diritto alla protezione dei dati personali, la libertà di circolazione dei medesimi.

In altre parole, a ben guardare, le esigenze di contemperamento proporzionale degli interessi, volte a salvaguardare l'esistenza dei contrapposti valori in gioco che l'interprete ha il compito di contemperare, si traducono nell'abbandono della logica esclusiva – tipicamente riscontrabile nello *jus excludendi ali*os – e nel recupero della logica dell'inclusione, tipica della solidarietà, declinata nella specifica materia della protezione dei dati personali.

La logica inclusiva della solidarietà nel trattamento dei dati personali è stata evidenziata anche nelle scelte lessicali del *considerando* n. 4 del GDPR, ove si enfatizza la *funzione sociale* del diritto alla protezione dei dati personali, nel senso già chiarito della necessità di contemperamento proporzionale di tale diritto con altri diritti fondamentali, inclusi quelli che attengono alla libertà di espressione e d'informazione ed alla libertà di impresa. La funzione sociale, però, ha ora altre coloriture,

[27] Sull'interpretazione di tale formulazione si rimanda, più diffusamente, a F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, pp. 190 ss., nonché F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 1, pp. 190-216.

perché si è espansa ulteriormente nella dimensione altruistica emersa con l'altruismo dei dati delineato nel *Data Governance* Act, all'interno degli articoli su cui ci si soffermerà nel prosieguo del discorso, non prima di aver rimarcato l'atteggiarsi dell'ulteriore declinazione della solidarietà nel GDPR: quella che passa attraverso il principio di correttezza indicato all'art. 5, par. 1, lett. *a)*. Il legislatore europeo ivi richiede, infatti, che i dati personali siano «trattati in modo lecito, *corretto* e trasparente nei confronti dell'interessato ("liceità, *correttezza* e trasparenza")».

La correttezza richiede quegli inderogabili obblighi di solidarietà sociale che, nel nostro sistema giuridico, si rinvengono anche nel diritto delle obbligazioni, in generale, e, nel corpo del GDPR, nell'adempimento di quei particolari obblighi di protezione che il legislatore ha posto normativamente a carico del titolare del trattamento per l'esigenza di tutela dei diritti e delle libertà dell'interessato. Ecco allora che, oltre al principio di liceità e a quello di trasparenza, compare, con la sua autonomia, il principio di correttezza, che acquista in tale materia una colorazione nuova, là dove necessita di essere applicato nei rapporti titolare del trattamento-interessato. Si coglie, in questa sfumatura della correttezza, improntata a quegli obblighi di collaborazione solidale verso l'interessato, l'esigenza di ricollocare il contemperamento degli interessi in gioco, in modo che il trattamento, espressione della libertà di circolazione, non sia posto in essere nel segno della prevaricazione, ma rispetti le esigenze di tutela dell'interessato nella prospettiva di un bilanciamento proporzionale che spesso è rimesso proprio nelle mani del titolare del trattamento, oggi più che mai vista l'operatività congiunta del principio di *accountability*.

Si pensi, a tal riguardo, al bilanciamento proporzionale richiesto, ad esempio, dall'art. 6, par. 1, lett. *f)*, del GPDR per i trattamenti necessari a perseguire un interesse legittimo del titolare o di soggetti terzi, che devono avvenire «a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore». Anche in questa norma si trova un'estrinsecazione del principio di solidarietà, che per un verso reclama la correttezza in ordine alle modalità di trattamento che il titolare deve porre in essere per salvaguardare le esigenze di protezione dell'interessato e, dall'altra parte, fa muovere il diritto alla protezione dei dati personali nel senso dell'inclusività, facendo sì che non pregiudichi le legittime esigenze di utilizzo del dati personali, imponendo un sacrificio (proporzionale) delle proprie istanze, per realizzare quella «funzione sociale» auspicata nel *considerando* n. 4 del GDPR.

L'inquadramento normativo del principio di solidarietà al cospetto della disciplina relativa ai dati personali non può poi prescindere dal recente Reg. UE n. 868/2022 in tema di *Data Governance*, ove rileva sia la dimensione del *riutilizzo dei dati*, personali e non personali, della pubblica amministrazione[28], per finalità commerciali o non commerciali, sia la dimensione dell'*altruismo dei dati*[29].

[28] Cfr. il Capo II («*Riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici*»), artt. 3-9, del *Data Governance Act*. In materia si veda, *amplius*, F. Bravo, *Data Governance Act and Re-Use od Fata in Public Sector*, in *European Review of Digital Administration and Law (Erdal)*, 2022, 2, pp. 13 ss.

[29] Cfr. il Capo Capo IV («*Altruismo dei dati*»), artt. 16-25, del *Data Governance Act*.

Con riguardo al riuso dei dati nella disponibilità della p.a., la logica della solidarietà si spinge verso dinamiche inclusive della libera circolazione dei dati, anche se non sempre secondo la dimensione altruistica[30]. Qui "solidarietà" è "inclusività" – in contrapposizione a quell'"esclusività" su cui si basava originariamente la tutela della "*privacy*" – nell'utilizzo dei dati, affinché sia possibile trarre benefici da essi per finalità diverse da quelle di prima acquisizione, in sintonia con la logica della circolazione dei dati, sia per scopi commerciali che non commerciali. Questa logica mira a realizzare il *secondary use*, ad uso di soggetti privati, dei dati raccolti e trattati dalla pubblica amministrazione[31], ove però la p.a. può pretendere anche tariffe per la copertura dei costi necessari per la gestione del procedimento, in relazione alle seguenti voci: «*a)* la riproduzione, la fornitura e la diffusione dei dati; *b)* l'acquisizione dei diritti; *c)* l'anonimizzazione o altre forme di preparazione dei dati personali e commerciali riservati (…); *d)* il mantenimento dell'ambiente di trattamento sicuro; *e)* l'acquisizione del diritto di consentire il riutilizzo a norma del presente capo da parte di terzi esterni al settore pubblico, nonché; *f)* l'assistenza ai riutilizzatori nel richiedere il consenso degli interessati e l'autorizzazione dei titolari dei dati i cui diritti e interessi possono essere interessati da tale riutilizzo»[32].

La solidarietà assurge invece alla dimensione sociale ed altruistica, scevra da connotati commerciali, nella disciplina del *data altruism* di cui all'intero Capo IV (intitolato appunto «*Altruismo dei dati*»), che consta degli articoli da 16 a 25. Anche in tal caso la "solidarietà" è "inclusione" e "circolazione" dei dati, con loro sottrazione alle logiche dell'esclusione (ovvero, dello *jus excludendi alios*): l'altruismo dei dati passa infatti per la *condivisione volontaria* e a titolo *gratuito* di dati medesimi, personali e non personali, basata sul consenso accordato dagli interessati ai sensi degli artt. 6 e 9 GDPR, nel primo caso, o sulle autorizzazioni di altri titolari dei dati, nel secondo caso, anche mediante un apposito «modulo europeo di consenso all'altruismo dei dati»[33]. Nel *data altruism*, tuttavia, la solidarietà è esaltata non solo dalla

[30] L'art. 2, par. 1, n. 2, del *Data Governance Act* intende il «*riutilizzo*» dei dati come «l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico».

[31] Il riutilizzo concerne in particolare i «dati detenuti da enti pubblici, che sono protetti per motivi di: *a)* riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; *b)* riservatezza statistica; *c)* protezione dei diritti di proprietà intellettuale di terzi; o *d)* protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024». Così l'art. 3, par. 1, del *Data Governance Act*.

[32] Cfr. art. 6 («*Tariffe*») del *Data Governance Act*.

[33] L'art. 25 («*Modulo europei di consenso all'altruismo dei dati*») stabilisce che «1. Al fine di facilitare la raccolta dei dati basata sull'altruismo dei dati, la Commissione adotta atti di esecuzione per l›istituzione e l'elaborazione di un modulo europeo di consenso all'altruismo dei dati, previa consultazione del comitato europeo per la protezione dei dati, tenendo conto del parere del comitato europeo per l'innovazione in materia di dati e coinvolgendo opportunamente i pertinenti portatori di interessi. Il modulo permette di raccogliere il consenso o l'autorizzazione in un formato uniforme in tutti gli Stati membri (…).

2. Il modulo europeo di consenso all'altruismo dei dati utilizza un approccio modulare che ne consente la personalizzazione in funzione di settori specifici e finalità diverse.

condivisione e dalla circolazione dei dati e, dunque, dalla dimensione inclusiva della circolazione dei dati, ma soprattutto dalla ontologica *assenza di corrispettivo*, in denaro o altra controprestazione, salvo eventualmente il rimborso dei costi sostenuti per mettere a disposizione i propri dati *per obiettivi di interesse generale*.

La solidarietà del *data altruism* è destinata a spiegare i maggiori effetti nel settore dell'assistenza sanitaria, della lotta ai cambiamenti climatici, del miglioramento della mobilità, nonché dell'agevolazione, elaborazione, produzione e divulgazione di statistiche ufficiali, ma anche del miglioramento della fornitura dei servizi pubblici, e dell'elaborazione delle politiche pubbliche o, ancora, nel settore della ricerca scientifica condotta nell'interesse generale. Si noti che il principio di solidarietà finisce, per certi versi, per integrarsi con i concetti di sostenibilità (digitale) sociale, economica e ambientale.

La nuova disciplina europea sull'altruismo dei dati prevede l'emanazione di norme *ad hoc* da parte degli ordinamenti nazionali, di carattere organizzativo o tecnico, per facilitare concretamente l'altruismo dei dati, oltre che la previsione di politiche nazionali specifiche in tale materia, anche al fine di prestare assistenza agli interessati per fare quanto occorra al fine di rendere disponibili i propri dati su base volontaria, per finalità altruistiche nell'interesse generale, anche con riguardo ai dati detenuti dalla pubblica amministrazione[34]. Alla normativa di competenza nazionale si affianca anche un'ulteriore regolamentazione affidata alla Commissione europea, che adotta atti delegati al fine di integrare il *Data Govenance Act* in materia di altruismo dei dati, con l'istituzione di uno specifico Codice, previsto all'art. 22, per una disciplina di dettaglio elaborata in stretta collaborazione con le organizzazioni per l'altruismo dei dati e i loro rispettivi *stakeholders*[35].

È poi contemplata l'istituzione di specifici registri pubblici nazionali delle organizzazioni riconosciute per l'altruismo dei dati, la cui tenuta è affidata ad autorità competenti individuate presso i singoli Stati membri, affiancata dall'istituzione

3. Qualora siano forniti dati personali, il modulo europeo di consenso all'altruismo dei dati garantisce che gli interessati possano dare e revocare il proprio consenso a una specifica operazione di trattamento dei dati conformemente alle prescrizioni di cui al regolamento (UE) 2016/679.

4. Il modulo è disponibile in un formato stampabile e facilmente comprensibile nonché in un formato elettronico predisposto per la lettura automatica».

[34] Cfr. art. 16 («*Disposizioni nazionali per l'altruismo dei dati*») del *Data Governance Act*.

[35] In tale *codice* la Commissione europea dovrebbe prevedere, in base all'art. 22, par. 1, del *Data Governance Act*, «*a)* adeguati requisiti in materia di informazione per garantire che gli interessati e i titolari dei dati ricevano, prima di dare il consenso o l'autorizzazione all'altruismo dei dati, informazioni sufficientemente dettagliate, chiare e trasparenti sull'utilizzo dei dati, sugli strumenti per concedere e revocare la concessione del consenso o dell'autorizzazione, e sulle misure adottate per evitare l'utilizzo improprio dei dati condivisi con l'organizzazione per l'altruismo dei dati; *b)* adeguati requisiti tecnici e di sicurezza per garantire l'opportuno livello di sicurezza per la conservazione e il trattamento dei dati, nonché per gli strumenti per la concessione o la revoca del consenso o dell'autorizzazione; *c)* tabelle di marcia per la comunicazione con un approccio multidisciplinare per sensibilizzare i pertinenti portatori di interessi, in particolare i titolari dei dati e gli interessati che potrebbero condividere i loro dati, per quanto riguarda l'altruismo dei dati, la designazione in qualità di organizzazione per l'altruismo dei dati riconosciuta nell'Unione e il codice stesso; *d)* raccomandazioni sulle norme di interoperabilità pertinenti».

di un ulteriore registro pubblico, centralizzato presso l'UE, delle organizzazioni per l'altruismo dei dati, tenuto dalla Commissione europea a scopi informativi[36].

Per poter essere iscritti in tali registri, gli enti che intendono operare come organizzazioni per l'altruismo dei dati riconosciute devono possedere una serie di requisiti generali previsti dall'art. 18 e segnatamente: «*a)* svolgere attività di altruismo dei dati; *b)* essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile; *c)* operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro; *d)* svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività; *e)* rispettare il codice di cui all'articolo 22, paragrafo 1, al più tardi entro 18 mesi dopo la data di entrata in vigore degli atti delegati di cui a tale paragrafo»[37].

Le organizzazioni riconosciute operanti nel settore dell'altruismo dei dati sono quindi tenute a rendere pubbliche una serie nutrita di informazioni, come la denominazione e la loro forma giuridica, il registro pubblico presso cui sono iscritti e il numero di registrazione, lo statuto (se opportuno) e le fonti di approvvigionamento economico, la sede principale e quelle secondarie, con l'indirizzo dell'ente e del legale rappresentante, le persone di contatto e i relativi recapiti, nonché gli obiettivi di interesse generale che l'ente vuole promuovere raccogliendo i dati, nonché la natura dei dati che l'ente intende controllare o trattare e, nel caso in cui si tratti di dati personali, l'indicazione specifica della categoria di dati personali e, infine, un sito *web* pubblicamente accessibile, presso cui sia possibile reperire tutte le informazioni aggiornate[38].

L'operatività di ciascuna organizzazione per l'altruismo dei dati riconosciuta è poi soggetta ad ulteriori obblighi di trasparenza, essendo tenuta a predisporre e tenere aggiornati, a propria volta, appositi registri riguardanti: «*a)* tutte le persone fisiche o giuridiche cui è stata data la possibilità di trattare i dati detenuti da tale

[36] Cfr. art. 17 («*Registri pubblici delle organizzazioni per l'altruismo dei dati riconosciute*») del *Data Governance Act*, ove, al par. 2, viene previsto anche che «Purché sia registrata nel registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute conformemente all'articolo 18, un'entità può utilizzare, nelle proprie comunicazioni scritte e orali, il titolo "organizzazione per l'altruismo dei dati riconosciuta nell'Unione" nonché un logo comune», con la precisazione che «Per garantire che le organizzazioni per l'altruismo dei dati riconosciute siano facilmente identificabili in tutta l'Unione, la Commissione stabilisce, mediante atti di esecuzione, un disegno per il logo comune. Le organizzazioni per l'altruismo dei dati riconosciute espongono il logo comune in modo chiaro su ogni pubblicazione *online* e *offline* relativa alle loro attività di altruismo dei dati. Il logo comune è accompagnato da un codice QR con un *link* al registro pubblico dell'Unione delle organizzazioni per l'altruismo dei dati riconosciute». La Commissione europea ha provveduto alla realizzazione e alla pubblicazione dei loghi per i fornitori sei servizi di intermediazione dei dati e per le organizzazioni di *data altruism* riconosciute nell'UE, che possono essere scaricati online ed utilizzati ai sensi del *Data Governance Act* (DGA): v. COMMISSIONE EUROPEA, *Logos for data intermediaries and data altruism organisations recognised in the Union*, 9 August 2023, all'url https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union (consultato da ultimo in data 28 agosto 2023).

[37] Cfr. art. 18 («*Requisiti generali per la registrazione*») del *Data Governance Act*.

[38] Cfr. art. 19 («*Registrazione delle organizzazioni per l'altruismo dei dati riconosciute*») del *Data Governance Act*.

organizzazione per l'altruismo dei dati riconosciuta, e i loro recapiti; *b)* la data o la durata del trattamento dei dati personali o dell'utilizzo di dati non personali; *c)* le finalità del trattamento, quali dichiarate dalla persona fisica o giuridica cui è stata data la possibilità di effettuarlo; *d)* le eventuali tariffe pagate dalle persone fisiche o giuridiche che trattano i dati»[39]. Gli obblighi di trasparenza di traducono poi anche nella predisposizione di una relazione annuale delle attività svolte, da trasmettere all'autorità competente per la registrazione delle organizzazioni per l'altruismo dei dati, in cui siano contenuti, specificamente: «*a)* informazioni sulle attività dell'organizzazione per l'altruismo dei dati riconosciuta; *b)* una descrizione delle modalità con cui, nel corso dell'esercizio finanziario in questione, sono stati promossi gli obiettivi di interesse generale per le quali sono stati raccolti i dati; *c)* un elenco di tutte le persone fisiche e giuridiche che sono state autorizzate a trattare i dati detenuti dall'entità, corredato di una descrizione sintetica degli obiettivi di interesse generale perseguiti da tale trattamento dei dati e di una descrizione dei mezzi tecnici impiegati a tal fine, compresa una descrizione delle tecniche utilizzate per tutelare la vita privata e la protezione dei dati; *d)* una sintesi dei risultati dei trattamenti dei dati autorizzati dall'organizzazione per l'altruismo dei dati riconosciuta, se opportuno; *e)* informazioni sulle fonti di entrate dell'organizzazione per l'altruismo dei dati riconosciuta, in particolare tutte le entrate derivanti dall'autorizzazione all'accesso ai dati, e sulle spese»[40].

Vengono infine contemplati specifici obblighi di tutela dei diritti e degli interessi dei soggetti a cui si riferiscono i dati personali («interessati», ai sensi del GDPR), oltre che dei soggetti, anche diversi dalle persone fisiche, che hanno il diritto di concedere l'accesso a determinati dati personali o non personali e di condividerli («titolari dei dati», ai sensi del DGA). A ciò è deputato l'art. 21 del Reg. UE n. 868/2022, in forza del quale sono previsti obblighi informativi, da assolvere in maniera chiara e facilmente comprensibile agli interessati e ai titolari dei dati, prima di qualsiasi trattamento dei loro dati, in ordine sia «agli obiettivi di interesse generale e, se opportuno, alla finalità determinata, esplicita e legittima per cui i dati devono essere trattati, e per i quali acconsentono al trattamento dei loro dati da parte di un utente dei dati»[41], sia «all'ubicazione e agli obiettivi di interesse generale per cui acconsentono a eventuali trattamenti effettuati in un paese terzo, nel caso in cui il trattamento sia effettuato dall'organizzazione per l'altruismo dei dati riconosciuta»[42]. Viene poi fissato l'esplicito divieto, per le organizzazioni per l'altruismo dei dati riconosciuta, di utilizzare «i dati per altri obiettivi diversi da quelli di interesse generale per i quali gli interessati o i titolari dei dati acconsentono al trattamento (…)»[43]. Il divieto

[39] In questo senso si veda l'art. 20 («*Obblighi di trasparenza*»), par. 1, del *Data Governance Act*.
[40] Così l'art. 20, par. 2, del *Data Governance Act*.
[41] Cfr. art. 21 («*Obblighi specifici di tutela dei diritti e degli interessi degli interessati e dei titolari dei dati per quanto riguarda i loro dati*»), par. 1, lett. *a)*, del *Data Governance Act*.
[42] Cfr. art. 21, par. 1, lett. *b)*, del *Data Governance Act*.
[43] V. art. 21, par. 2, prima parte, del *Data Governance Act*.

si estende esplicitamente anche al ricorso «a *pratiche commerciali ingannevoli* per sollecitare la fornitura di dati»[44].

Altri obblighi imposti alle organizzazioni per l'altruismo dei dati riconosciute richiedono che le medesime forniscano «*strumenti per ottenere il consenso* degli interessati o le autorizzazioni al trattamento dei dati messi a disposizione dai titolari dei dati (…), [oltre che] strumenti per l'agevole *revoca* di tale consenso o autorizzazione»[45] e l'adozione di «*misure* intese a garantire un livello adeguato di *sicurezza* per la conservazione e il trattamento di dati non personali che ha raccolto sulla base dell'altruismo dei dati»[46], che si aggiungono agli obblighi di adozione delle misure di sicurezza per il trattamento dei dati personali previsti nel GDPR[47].

Ulteriori obblighi sono poi indicati al par. 5 dell'art. 21 cit., ai sensi del quale «L'organizzazione per l'altruismo dei dati riconosciuta *informa* senza ritardo i titolari dei dati in caso di trasferimento, accesso o utilizzo non autorizzati dei dati non personali che ha condiviso», analogamente a quanto previsto dall'art. 34 GDPR in caso di *data breach* riguardante dati personali. Infine, in forza dell'art. 21, par. 6, del *Data Governance Act*, «Qualora l'organizzazione per l'altruismo dei dati riconosciuta agevoli il trattamento dei dati da parte di terzi, anche fornendo strumenti per ottenere il consenso degli interessati o le autorizzazioni a trattare i dati messi a disposizione dai titolari dei dati, essa specifica, se del caso, la giurisdizione del paese terzo in cui i dati sono destinati a essere utilizzati».

Le disposizioni volte ad assicurare l'altruismo dei dati nel nuovo regolamento europeo sono poi presidiate dalle funzioni di monitoraggio svolte dalle «autorità competenti per la registrazione delle organizzazioni per l'altruismo dei dati», a cui spetta il compito di monitorare e controllare la conformità della prescrizioni, con poteri di accertamento e di intervento, che possono giungere anche all'adozione di misure adeguate e proporzionate per assicurare l'osservanza della disciplina *de qua*, la cui violazione può comportare, per l'organizzazione operante nel settore dell'altruismo dei dati, la perdita del diritto di utilizzare il titolo acquisito (di «organizza-

[44] In tal senso v. art. 21, par. 2, ult. parte, del *Data Governance Act*. Su tali aspetti, a titolo esemplificativo, si richiama il caso *Facebook* affrontato dall'AGCM, culminato con il provv. 27432 del 29 novembre 2018, a cui hanno fatto seguito le sentt. nn. 260 e 261 del 2021 del TAR Lazio, Roma, e, infine, le sentr. del Cons. St. nn. 2630 e 2631 del 2021, ove è stata confermata l'esistenza della pratica commerciale scorretta nella condotta del noto *provider* che aveva omesso adeguate informazioni sulle effettive modalità di utilizzo per fini commerciali dei dati personali degli utenti, rappresentando loro un'asserita gratuità del servizio (attraverso il *disclaimer* «Iscriviti! È gratis e lo sarà per sempre»), senza neanche rendere palese che il conferimento dei dati personali da parte degli utenti per l'uso commerciale al fine di rendere remunerativo il servizio costituisce la controprestazione per la fornitura del servizio medesimo, non a titolo gratuito, ma in cambio di una prestazione non pecuniaria. Sul punto si veda, in particolare, F. BRAVO, *La «compravendita» di dati personali?*, in *Diritto di Internet*, 2020, 3, pp. 521-540; nonché V. RICCIUTO, *L'equivoco della* privacy. *Persona* vs *dato personali*, Napoli, 2022, pp. 95 ss., il quale pone l'accento anche sui poteri regolatori delle autorità amministrative indipendenti, non solo a difesa della persona, ma anche come «"conformatori", costruttori e regolatori di più complesse dinamiche, anche economiche», ovvero del mercato, incluso quello concernente i dati personali o, meglio, le attività di trattamento sui dati personali.

[45] Cfr. art. 21, par. 3, del *Data Governance Act*.

[46] Cfr. art. 21, par. 4, del *Data Governance Act*.

[47] Qui il riferimento è all'art. 32, nonché agli artt. 24, 25 e 35 del GDPR.

zione per l'altruismo dei dati riconosciuta dall'Unione») e la rimozione dal registro pubblico nazionale e da quello dell'UE[48].

2. Portata del principio

2.1. Le direzioni del principio di solidarietà al cospetto (del trattamento) dei dati personali: (i) la solidarietà come "limite" per il titolare del trattamento

Il principio di solidarietà, come s'è potuto ricavare dall'analisi del suo inquadramento normativo, si rivolge in molteplici direzioni quando si misura con il regime applicabile ai dati personali[49].

La prima direzione è quella della solidarietà come *limite* delle prerogative dell'interessato o del titolare del trattamento e, insieme, come *obbligo* di attivarsi per le esigenze dell'altro soggetto con cui si è legati all'interno di un *vinculum iuris*, là dove si considera il principio in questione nella sua collocazione di dovere di solidarietà politica, economica e sociale declamato dall'art. 2 Cost.[50], riallacciabile anche al dovere di comportarsi secondo buona fede[51].

La solidarietà unisce prospettive molteplici del vivere sociale, essendo espressione di un legame, giuridicamente rilevante, sia in senso verticale tra l'autorità sovrana e il singolo, sia in senso orizzontale *inter personas*.

L'indagine sulle radici del principio in esame diviene fondamentale per comprende appieno la sua attuale portata. La dottrina più accorta ha rimarcato come il principio *de quo* sia il portato di istanze emerse a partire dalla rivoluzione francese, ove la "fraternità" aveva inizialmente la valenza di «strumento politico per rafforzare lo spirito patriottico (…)»[52], ma che presto assunse invece «un significato diverso e più pregnante»[53], capace di trascendere la dimensione nazionale: ciò sin dalla stesura progetto di dichiarazione dei diritti, ad opera di Roberspierre il 24 aprile 1973, ove «la fraternità indica un valore universale: gli uomini di tutti i paesi sono riconosciuti come fratelli e i differenti popoli "devono aiutarsi tra di loro secondo il loro potere,

---

[48] Si veda, in marito a tali aspetti, il tenore dell'art. 24 del *Data Governance Act*, rubricato «*Monitoraggio della conformità*».

[49] Per una trattazione approfondita del principio di solidarietà, nella sua portata più ampia (a prescindere dalla materia concernente il trattamento dei dati personali, qui considerata), si rimanda alle preziose pagine di G. Alpa, *Solidarietà. Un principio normativo*, cit., *passim*, e di S. Rodotà, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2016. Si veda anche P. Mengozzi, *L'idea di solidarietà nel diritto dell'Unione europea*, Bologna, 2022.

[50] Sulla «solidarietà come limite e come obbligo» si veda G. Alpa, *I principi generali*, cit., pp. 402 ss., ove l'A. avverte che il limite opera sia orizzontalmente, tra privati, sia verticalmente, tra lo Stato e il cittadino.

[51] Cfr. G. Alpa, *I principi generali*, p. 398 e D. Corradini, *Il processo costituzionale nella Francia rivoluzionaria e il diritto privato*, in M.A. Cattaneo (a cura di), *Diritto e Stato nella filosofia della Rivoluzione francese*, 1992, p. 202.

[52] G. Alpa, *I principi generali*, p. 398.

[53] *Ibidem*.

come i cittadini dello steso Stato"»[54]. V'è di più, dato che «La fraternità gioca un ruolo importante anche nei rapporti tra privati, là dove nelle contrattazioni le nuove leggi richiedono alle parti di comportarsi secondo buona fede»[55].

Si registra un punto di contatto con il dovere di correttezza nei rapporti obbligatori[56], ma la solidarietà appare ben più ampia, sia per la sua dimensione (non solo orizzontale, ma anche) verticale, sia perché, ove ci si collochi nei soli rapporti tra privati, ha contenuti più estesi della correttezza, benché in parte sovrapponibili.

Quanto alla sua connotazione verticale, la solidarietà si distingue dalla "fratellanza" e dall'"amicizia", ovvero dalla dimensione esclusivamente individualista, per assurgere anche a dimensione comunitaria[57]. È questa, ad esempio, la solidarietà "*inclusiva*" a cui tende l'UE (e, con essa, gli Stati nazionali che ne fanno parte) nel percorso avviato con la *European Declaration on Digital Right and Principles* (v. Chapter II, «*Solidarity and inclusion*»)[58].

L'interprete deve guardare con particolare attenzione anche alla dimensione orizzontale della solidarietà, che colloca nei rapporti *inter privatos* il limite e l'obbligo in cui essa si traduce[59]. A tal proposito, volgendo ancora lo sguardo alle indagini sulle radici del principio in esame, la dottrina ha ricordato che la solidarietà, declinata ancora come fraternità, era impressa anche nella Costituzione francese del 1795, ove «per la prima volta compaiono in un testo fondamentale i doveri, oltre che i diritti dell'uomo. Tra i doveri si richiamano i precetti "non fare agli altri ciò che non vorresti fosse fatto a te" e "fate costantemente agli altri ciò che vorreste ricevere" (art. 2); si precisa che "non è buon cittadino chi non è buon figlio, buon padre, buon fratello, buon amico, buon coniuge" (art. 4) (…). Ecco che la fraternità, e la solidarietà, pur sfumate nella loro fisionomia, presentano un contenuto di doverosità: è il dovere di attivarsi, di fare il bene, che per la prima volta compare in un testo normativo»[60]. È proprio questa la genesi della solidarietà di tipo "orizzontale". Si tratta di dimensione operante all'interno di rapporti intersoggettivi, siano essi sociali,

---

[54] *Ibidem*.

[55] *Ibidem*, ove richiama D. CORRADINI, *op. cit.*, p. 202.

[56] Su tale aspetto cfr. G. ALPA, *I principi generali*, p. 402 (con richiami a S. RODOTÀ, *Il diritto privato nella società moderna*, Bologna, 1980): «I civilisti riscoprono la solidarietà, rivalutando l'applicazione diretta della Costituzione ai rapporti tra privati, facendo uso delle clausole generali che si riferiscono alla buona fede, alla correttezza, all'equità. Se ne propone l'applicazione in materia di proprietà ove all'individualismo proprietario si contrappone la concezione della funzione sociale della proprietà; in materia di attività economiche, ove alla libertà di mercato si contrappone l'utilità sociale dell'iniziativa economica; alla libertà contrattuale ove si contrappone al potere negoziale dell'impresa la tutela del contraente debole, sia nel settore del lavoro, sia nel settore dei consumi e in quello dei risparmi: in materia di illecito, ove si dà maggior rilievo alla persona e alla quantificazione del danno, si favorisce la teoria del rischio d'impresa, e si tenta di superare il principio di tipicità delle ipotesi di colpa omissiva».

[57] G. ALPA, *I principi generali*, cit., pp. 399 e 400.

[58] Cfr., *infra*, par. 1.1, nonché il Cap. I, par. 2.2, del presente volume.

[59] Con rifermento al principio di solidarietà nel nostro ordinamento, s'é ben rimarcato che «L'interprete italiano ha (…) a disposizione un testo costituzionale ricco di riferimenti e di spunti e un codice civile avaro di spinte solidaristiche. Un'operazione di applicazione diretta delle norme costituzionali ai rapporti tra privati è quindi necessaria». Così G. ALPA, *I principi generali*, cit., p. 401.

[60] G. ALPA, *I principi generali*, cit., p. 399.

economici o politico-istituzionali, che, con il principio ad esame, vengono "giuridificati", attraverso l'instaurazione di un vincolo che limita l'agire individualistico[61].

Il principio-dovere di solidarietà confina con le esigenze di correttezza, senza tuttavia confondersi con essa. La solidarietà si manifesta come dovere di tutelare anche le istanze di cui è portatore l'altro soggetto della relazione giuridica. In materia di protezione dei dati personali i doveri del principio in esame sono ambivalenti, perché operanti sia nei confronti dell'interessato che del titolare del trattamento.

Per quest'ultimo la dimensione della solidarietà impone di garantire, innanzitutto, la protezione dell'interessato, già accuratamente scolpita nel regime di tutela normativa in tema di *data protection*, facendo però in modo che i margini di discrezionalità previsti dall'applicazione della norma siano effettivamente orientati alle esigenze di tutela dei diritti e delle libertà del soggetto a cui i dati trattati si riferiscono e non al mero rispetto formale del dettato normativo. Si pensi, ad esempio, alla scelta in ordine alle modalità di trattamento e al sistema di sicurezza approntato, alla scelta dei soggetti coinvolti nel trattamento e alle modalità di acquisizione e circolazione dei dati, in rapporto alle finalità del trattamento. In questa prospettiva, la solidarietà confina certamente con il principio di *accountability*[62]. Ancora, per il titolare la solidarietà verso l'interessato si esplica anche nel senso della correttezza e della leale cooperazione, in relazione alle esigenze, agli interessi, ai diritti e alle libertà fondamentali di quest'ultimo. Qui la solidarietà ha punti inevitabili di contatto con il principio di correttezza, ma lo colora in una direzione diversa dalla trasparenza, in cui spesso il principio di correttezza finisce per risolversi, dando sfumature di carattere sostanziale e non formale: il titolare è tenuto a comportarsi in maniera solidale, evitando comportamenti decettivi (ad es. nelle modalità di acquisizione e utilizzo dei dati) o in condotte che possano tradursi in pratiche commerciali scorrette, sleali o ingannevoli (già censurate, con riguardo all'utilizzo dei dati, sia dall'AGCM che dalla giustizia amministrativa, come per il caso Facebook e il caso WhatsApp)[63]. La solidarietà rileva non solo sul versante di obblighi "negativi", aventi ad oggetto condotte omissive (i divieti poc'anzi richiamati), ma anche sul versante di obblighi

[61] Preziose, a tal riguardo, sono ancora una volta le parole dell'insigne Maestro: «Ma perché elevare a regola giuridica, cioè a norma vincolate e coattiva, la solidarietà? Perché si avverte l'esigenza di sottrarre la solidarietà al mondo dei rapporti non giuridificati, al mondo dell'operare spontaneo e amichevole, al mondo del caso e del capriccio? La risposta, a tempo stesso banale e semplice, è presto detta: perché la solidarietà è connotato peculiare delle società moderne e civili, ispirate alla tutela dell'altro, del diverso, dell'emarginato; ma è connotato che tende ad essere sommerso, quando non debellato, dall'individualismo (o peggio, dall'egoismo) insito nella natura umana. "*Homo homini lupus*" è una verità storica, insuperata e forse insuperabile. Ed è appunto per temperare questa spinta naturale, per conservare la stessa coesione sociale, per elevare la convivenza bruta a convivenza civile, che la solidarietà deve essere non solo riconosciuta ma anche imposta come valore e come principio. Elevare la solidarietà a principio di diritto significa rendere coattivo l'atto o il comportamento "solidale"». Così G. Alpa, *I principi generali*, cit., pp. 402 e 403.

[62] Sul principio di *accountability* o di responsabilizzazione cfr. G. Finocchiaro, *Il principio di* accountability, in *Giust. it.,* 2019, pp. 2778 ss., nonché il Cap. XIII del presente volume.

[63] Sul caso Facebook v.: AGCM, provv. 27432 del 29 novembre 2018; TAR Lazio, Roma sentt. nn. 260 e 261 del 2021; Cons. St., sentt. nn. 2630 e 2631 del 2021; sul caso WhatsApp v.: AGCM, provv. n. 26597 dell'11 maggio 2017.

aventi ad oggetto condotte positive, di tipo "collaborativo", volte a rafforzare sul piano sostanziale la posizione del *data subject*, consentendogli di realizzare, nella maggior misura possibile, gli interessi a cui anela nell'ambito del trattamento dei dati a cui è esposto. Si tratta di un'accezione "orizzontale" della solidarietà che porta ad una forma di "giuridificazione", nei rapporti tra titolare e interessato, di istanze tipiche della responsabilità sociale di impresa (o *Corporate Social Responsibility*, CSR), destinate altrimenti a rimanere al di fuori dell'ambito giuridico-noramtivo[64].

2.2. (*segue*): (ii) …e per l'interessato. La «funzione sociale» al cospetto (del trattamento) dei dati personali

Per l'interessato i doveri connessi alla dimensione orizzontale della solidarietà si atteggiano in modo in parte diverso. Il diritto alla protezione dei dati personali è, primariamente, diritto all'autodeterminazione informativa, sicché il dovere di solidarietà non può spingersi fino a configurare l'obbligo, per l'interessato, di porre in essere condotte volte a favorire la realizzazione dell'interesse del titolare del trattamento, ove tale interesse non coincida con quello dell'interessato medesimo o non vada per lo meno nella medesima direzione (come ad esempio nel caso in cui il paziente adotti condotte volte a favorire il trattamento dei dati personali per le finalità di cura a cui il trattamento posto in essere dal medico o dalla struttura sanitaria è orientato).

Il dovere di solidarietà dell'interessato verso il titolare è però ravvisabile nella logica del bilanciamento degli interessi contrapposti, non solo qualora entrano in contrapposizione diversi diritti fondamentali, facenti capo rispettivamente al titolare e all'interessato, ma segnatamente quando il bilanciamento è effettuato anche tra interessi di altro tenore, come quelli sociali o economici ad esempio. Emblematico è il confronto dinamico tra le esigenze dei due soggetti protagonisti del trattamento in occasione dell'esercizio del diritto di opposizione da parte dell'interessato nei trattamenti per i quali le condizioni di liceità siano date dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o, ancora, di perseguire un legittimo interesse del titolare o di soggetti terzi, ai sensi dell'art. 6, par. 1, lett. *e)* e *f)*, GDPR. Ebbene, l'art. 21, par. 1, GDPR prevede che «L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria». A fronte del diritto di opposizione si apre una valutazione sul bilanciamento degli interessi in gioco, rimessa al titolare del trattamento, che non culmina necessariamente con il blocco del trattamento, salve le ipotesi di trattamenti per finalità di *marketing* con-

[64] Sulla *Corporate Social Responsibility* si rimanda a G. CONTE (a cura di), *La responsabilità sociale dell'impresa*, Roma-Bari, 2008, *passim*.

template al par. 2 dell'art. 21 cit. Sicché l'assetto degli interessi potrebbe culminare legittimamente a favore del titolare del trattamento, non essendo automatica la prevalenza delle istanze dell'interessato, a fronte dell'esercizio del diritto di opposizione. Nell'ambito di tale dinamica può percepirsi l'operatività del principio di solidarietà, quale dovere orizzontale dell'interessato verso il titolare del trattamento, tenuto a favorire il raggiungimento degli interessi di quest'ultimo o di terzi o il compito di interesse pubblico o connesso all'esercizio di pubblici poteri rimesso all'azione del titolare del trattamento, anche qualora ciò comporti un sacrificio per l'interessato medesimo. Tali disposizioni del GDPR, a ben vedere, altro non sono che l'applicazione del dovere di solidarietà per l'interessato verso il titolare del trattamento, operanti nei limiti in cui all'interessato medesimo possa essere chiesto – giuridicamente – un sacrificio proprio, per doveri di solidarietà sociale, politica ed economica, a fronte della realizzazione di un beneficio altrui, a favore del soggetto titolare del trattamento o di un soggetto terzo [nel caso in cui rilevi la condizione di liceità di cui all'art. 6, par. 1, lett. *f)*, cit.] o della collettività [ove la condizione di liceità rilevane sia quella di cui all'art. 6, par. 1, lett. *e)*, cit.].

Altre volte – secondo logiche che per la verità non appaiono del tutto condivisibili, esplorate dalla giurisprudenza della Cassazione[65] – il principio *de quo* dovrebbe imporre all'interessato, in forza dei doveri di solidarietà sociale scolpiti nell'art. 2 Cost., di astenersi dall'avanzare richieste risarcitorie qualora l'attività di trattamento si traduca in danni sopportabili, in lesioni tollerabili, nell'ambito di questioni da considerarsi "bagattellari", ancorché frutto di illeciti accertati[66].

Il tema del bilanciamento tra le contrapposte posizioni giuridiche del titolare e dell'interessato, se rapportate sul piano dei diritti fondamentali[67], evoca l'altra accezione orizzontale del principio di solidarietà in materia di protezione dei dati personali, legato alla dichiarata «*funzione sociale*» che il trattamento dei dati personali può avere e che impone il proporzionale sacrificio dei diritti dell'interessato, al fine di consentire l'esercizio di altri diritti di pari rango vantati dal titolare del trattamento[68]. Il *considerando* n. 4 del GDPR, segnatamente, rimarca innanzitutto che «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo (…)», il che rimanda all'idea di un uso non necessariamente utilitaristico e secondo logiche individuali delle attività di trattamento poste in essere da parte del titolare, sui dati dell'interessato. In tale prospettiva, come già s'è avuto modo di anticipare *supra*, nel medesimo *considerando* si aggiunge anche che «(…) Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua *funzione sociale* e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (…)», con l'ulteriore precisazione che il GDPR

[65] Cfr., *amplius*, par. 3 del presente scritto.

[66] Sul punto si rinvia a quanto più ampiamente illustrato al par. 3.2 del presente scritto, nonché a F. Bravo, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, pp. 413 ss.

[67] F. Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 1, pp. 190-216.

[68] F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 162-166, nonché pp. 189 ss.

«(…) rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

Ovviamente l'enunciato non intende affatto mettere in dubbio che il diritto alla protezione dei dati personali, come tutti i diritti fondamentali della persona, sia un "diritto assoluto", ovvero esercitabile *erga omnes*: le espressioni sopra riportate intendono evitare, invece, che tale diritto possa essere considerato prevalente rispetto ad altri diritti fondamentali e che possa pertanto essere utilizzato aprioristicamente per inibire l'esercizio di questi ultimi, senza effettuare l'operazione di bilanciamento proporzionale tra gli interessi in gioco. I diritti fondamentali sono soggetti a limitazioni, proprio per la necessità di operare un bilanciamento con altri diritti di pari rango o per ragioni di interesse collettivo[69]. Il *considerando* n. 4 cit. enfatizza la logica del limite a cui va incontro il diritto fondamentale alla protezione dei dati personali immediatamente dopo l'enunciazione dell'utilità del trattamento, che «dovrebbe essere posto al servizio dell'uomo», per poi svilupparne ulteriormente il concetto nella conclamata «*funzione sociale*», solo apparentemente riferita al diritto alla protezione dei dati personali, ma da ricollegare in realtà ad altro[70]. Analizzando la *ratio* della norma, sia nel testo italiano che nelle ulteriori differenti versioni linguistiche (in inglese si fa riferimento alla "funzione *nella* società"), la dottrina che si è occupata del tema ha avuto modo di rimarcare che la «funzione sociale» invocata dal *considerando* n. 4 cit. non è da attribuire al diritto in sé, ma all' "oggetto" della tutela, rinvenuto, secondo una possibile ricostruzione, nelle informazioni di carattere personale su cui viene vantato il diritto fondamentale e che, tuttavia, può essere piegato anche ad esigenze diverse, ultraindividuali[71]. Invero, mi sembra preferibile una ricostruzione

---

[69] F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, cit., pp. 190-216; ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., pp. 188 ss.; A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., pp. 600-602.

[70] A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., p. 604.

[71] Tale impostazione è del resto in linea con un'interessante pronuncia della C.G.C.E. del 1974, ricordata da Annarita Ricci (ID., *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., p. 607), del 14 maggio 1974, *Nold Kohlen-Und Baustoffgrosshandlung c. Commissione delle Comunità Europee*, causa C-4/73, ove anche nella versione inglese si parla di "*social function*", al pari della versione italiana, in cui si menziona la "funzione sociale" riferita all'oggetto del diritto, quale limite al diritto stesso. L'A. ricorda, a tal riguardo, che «la Corte afferma che, benché l'ordinamento costituzionale di tutti gli Stati membri tuteli il diritto di proprietà e di analoga tutela fruisca il libero esercizio del commercio, del lavoro e di altre attività economiche, "i diritti così garantiti, lungi dal costituire prerogative assolute, vanno considerati alla luce della *funzione sociale* dei beni e delle attività *oggetto della tutela*. Per questa ragione, la garanzia concessa ai diritti di tal sorta fa generalmente salve le limitazioni poste in vista dell'interesse pubblico, considerato che nell'ordinamento giuridico comunitario appare legittimo sottoporre questi diritti a limiti giustificati da obiettivi di interesse generale perseguiti dalla Comunità", a condizione che tali restrizioni non comportino una lesione sostanziale del diritto fondamentale garantito. Evidente è l'interesse della decisione, i cui termini sono identici a quelli utilizzati a distanza di quaranta anni dal Regolamento europeo sul

parzialmente diversa, che riferisca la funzione sociale non già all'informazione di carattere personale, ma al suo utilizzo effettuato dal titolare del trattamento mediante le operazioni sui dati, per finalità determinate. In altre parole, la funzione sociale, più che al *dato* in sé, pare legata all'utilizzo che ne viene fatto e, dunque, al *trattamento* che viene posto in essere o che può essere realizzato con il dato personale, in ragione delle finalità perseguite, ovvero degli scopi a cui protendono le operazioni effettuate sulle informazioni di carattere personale.

A prescindere da tale distinzione, s'è precisato, condivisibilmente, che «Il contemperamento degli interessi, cui è preordinata la formula della funzione sociale, è connaturale alla duplice valenza del dato personale: da un lato, elemento essenziale per la libera circolazione delle persone, dei beni e dei servizi; dall'altro lato, componente dell'identità personale, strumento di esplicazione della personalità e di esercizio delle libertà individuali. Il contemperamento degli interessi è quindi la conseguenza del connotato sociale del dato, che non si identifica necessariamente in uno scopo di pubblica utilità»[72].

Un chiaro esempio in cui opera la «funzione sociale» delle informazioni di carattere personale – o, meglio, del loro trattamento – nella prospettiva del principio di solidarietà, mi pare senz'altro ravvisabile nella funzione svolta dai trattamenti per il tracciamento dei contatti al fine di individuare i casi di positività al Covid-19 durante la crisi pandemica, posti in essere tramite *app* di *contact-tracing* (Immuni) per salvaguardare esigenze collettive di sanità pubblica[73]. Qui il trattamento dei dati personali è avvenuto su base volontaria, da parte degli interessati, i cui dati sono stati trattati anche a beneficio di terzi e dell'intera collettività, secondo logiche solidaristiche che travalicano la "dimensione interindividuale" ma che hanno reso legittimo il trattamento in funzione delle esigenze di contenimento del *virus*[74], anche per «motivi

trattamento dei dati personali, nel sancire la chiave di lettura dell'espressione "funzione sociale", criterio da declinarsi con riferimento all'oggetto della prerogativa riconosciuta dalla legge» (*Ibidem*, p. 607).

[72] A. Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., p. 604.

[73] Sul rapporto tra App Immuni e potezione dei dati personali si rimanda a D. Poletti, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, in *Persona e mercato*, 2020, pp. 65 ss., nonché Id., *Contact tracing e app immuni: atto secondo*, in *Persona e mercato*, 2021, pp. 92 ss.; G. Resta, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, in *Giustiziacivi-le.com*, 5 maggio 2020; Id., *La app "Immuni": pregi e limiti del tracciamento digitale dei contatti*, in *MediaLaws*, 15 giugno 2020; V. Cuffaro-R. D'orazio, *La protezione dei dati personali ai tempi dell'epidemia*, in *Corr. giur.*, 2020, pp. 729 ss.; F. Pizzetti, *Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei garanti*, in *MediaLaws*, 29 giugno 2020.

[74] Cfr. D. Poletti, *Contact tracing e app immuni: atto secondo*, cit., p. 92, secondo cui «Una delle principali risposte delle autorità pubbliche alla situazione determinata dalla diffusione del Covid-19, che ha costretto una larga parte della popolazione mondiale a misurarsi con vantaggi e limiti della società digitale, è rappresentata dall'impiego di sistemi che combinano soluzioni tecnologiche e utilizzo dei dati, in specie dei dati inerenti alla salute. In questo contesto, l'uso delle applicazioni *software* (*app*) di *contact tracing* da installare sullo *smartphone* è stato al centro di un particolare interesse e di un vivacissimo dibattito, capace di spaziare dalle ricostruzioni del loro funzionamento, esaminate soprattutto dall'angolatura della protezione dei dati personali, fino alle disposizioni costituzionali coinvolte dal loro utilizzo. Soprattutto, ha posto all'attenzione degli studiosi della *data protection* (e non solo) la considerazione degli effetti di un impiego "su larga scala" – per usare una

di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero»[75].

Altro chiaro esempio di «funzione sociale» (del trattamento) dei dati personali è stato ravvisato nella permanenza delle informazioni di carattere personale di un imprenditore nel registro delle imprese tenuto dalle Camere di Commercio, relative alla qualità di amministratore unico e liquidatore di una società soggetta a fallimento molti anni prima e di cui ormai era avvenuta la liquidazione e la cancellazione dal predetto registro[76]. Il caso, sottoposto anche all'attenzione della Corte di giustizia dell'UE (C-398/15), è stato affrontato dalla Cassazione con ordinanza interlocutoria del 17 luglio 2015, n. 15096, con cui ha respinto le pretese dell'interessato alla cancellazione dei propri dati personali, considerando la funzione che il regime di pubblicità, realizzato tramite il registro delle imprese, assolve nei rapporti sociali ed economici[77].

Qui va rimarcato, però, che la «funzione sociale» opera nell'ambito del *principio* normativo *di solidarietà*: il sacrificio che si impone all'interessato è necessario per rendere edotta la collettività in ordine a informazioni che possono avere una rilevante incidenza nelle valutazioni economiche, veicolate tramite registri pubblici volti a rendere sicuri o comunque più agevoli i rapporti economici e sociali. Si tratta di sacrificio che, secondo la richiamata sentenza della Cassazione, è a carico dell'interessato e posto a beneficio degli altri consociati, ovvero dell'intera comunità, proprio in ragione dell'applicazione del «principio di solidarietà» specificamente operante in materia di protezione dei dati personali, nella prospettiva del raggiungimento di un giusto equilibrio tra gli interessi, individuali e collettivi, giuridicamente rilevanti[78].

Del resto ciò è il portato della libertà di circolazione dei dati personali, che è fenomeno insieme giuridico, economico e – inevitabilmente – sociale. La circolazione dei dati, come fatto sociale, porta di necessità a considerare il trattamento dei dati

espressione del Regolamento generale sulla protezione dei dati personali UE/2016/679 (GDPR) – di una soluzione digitale per aiutare le iniziative volte al contenimento della diffusione del Covid-19. Questo scenario oltrepassa la dimensione interindividuale del rapporto medico (o struttura ospedaliera)-paziente che ha sempre connotato il trattamento di dati "particolari" come quelli alla salute e tratteggia un orizzonte più articolato e ancora più complesso».

[75] Ved. art. 9, par. 2, lett. *i)*, GDPR.

[76] L'indicazione di tale caso quale esempio di "funzione sociale" con riferimento al trattamento dei dati personali è di A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., p. 604.

[77] Sul punto si veda, ancora, una volta, A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., la quale, in relazione a tale vicenda, osserva «che i dati, anche di natura personale, iscritti nel registro delle imprese sono informazioni peculiari in ragione della loro funzione. Si tratta di informazioni economiche, sottoposte ad un regime di pubblicità, la cui libera accessibilità è posta a garanzia del corretto funzionamento del mercato e a tutela della correttezza e trasparenza dei rapporti ivi instaurati. Declinando il diritto alla protezione del soggetto cui si riferiscono le informazioni iscritte nel registro delle imprese alla luce della "funzione sociale", si rivela la necessità di bilanciare la pretesa dell'interessato al controllo sulle informazioni riferite alla sua persona con il diritto dei terzi alla certezza dei rapporti economici e alla trasparenza degli assetti imprenditoriali, reso quest'ultimo effettivo dal regime di pubblicità legale dei registri».

[78] Cass., ord. 17 luglio 2015, n. 15096, par. 4.4.5, su cui si ritornerà anche nel terzo paragrafo del presente scritto, dedicato all'applicazione del principio di solidarietà nella casistica.

e le esigenze di tutela dell'interessato all'interno di una logica più estesa rispetto alla sola dimensione individuale, in cui si rischia di essere confinati se si concentra l'attenzione sulla sola situazione giuridica dell'interessato. Le informazioni di carattere personale vanno dunque collocate in un contesto più ampio, nelle relazioni sociali in cui è coinvolto il soggetto a cui i dati si riferiscono, sicché le istanze di protezione dell'interessato devono essere valutate in relazione a tali dinamiche sociali, avendo riguardo alla "funzione" che il trattamento dei dati personali può avere nella prospettiva circolatoria, al cui cospetto esercita un ruolo anche il dovere di solidarietà politica, sociale ed economica declamato nell'art. 2 della nostra Carta costituzionale.

2.3. (*segue*): (iii) la solidarietà come "orizzonte", secondo le logiche dell'inclusione

Vi sono però ulteriori direzioni, in cui il principio di solidarietà opera non come un "limite" alle prerogative soggettive, ma come un "orizzonte" o, se si vuole, un "allargamento" o un "potenziamento", nella logica di valorizzazione degli interessi rilevanti, che l'ordinamento giuridico intende favorire, soprattutto nell'ambito di strategie concertate a livello europeo.

Per tali aspetti il principio normativo di solidarietà si estende secondo logiche pubblicistiche, più che privatistiche, configurandosi come un obbligo o un impegno giuridico a rimuovere gli ostacoli che impediscono l'inclusione sociale e a favorire positivamente quest'ultima con iniziative concrete. La solidarietà come valore e come principio si traduce, in questo senso, in un vincolo giuridico per il legislatore e per il governo, nazionale o eurounitario, verso la realizzazione di rapporti sociali maggiormente equi e migliori condizioni di vita[79].

La direzione della solidarietà, qui, si orienta verso le logiche dell'inclusione e della condivisione, che sono quelle percorse dalla Commissione europea sia nella Comunicazione sulla Strategia europea per i dati [COM(2020) 66 final], sia nella *European Declaration on Digital Rights and Principles for the Digital Decade* (2023/C 23/01), il cui Chapter II, già richiamato in precedenza, viene interamente dedicato alla «*Solidariety*» intesa (soprattutto) come «*Inclusion*», declinata innanzitutto come diritto di accesso alla rete, partecipazione inclusiva al processo di trasformazione digitale, formazione all'uso degli strumenti digitali e all'acquisizione di competenze

[79] In tal senso si vedano, ad es., le parole di G. Alpa, *I principi generali*, cit., p. 403, là dove ha chiarito che «Elevare la solidarietà a principio di diritto significa rendere coattivo l'atto o il comportamento "solidale". Finché la norma vincola il legislatore non si riscontrano problemi: egli si fa interprete della coscienza sociale e, nei limiti in cui ciò sia richiesto dalle spinte verso una maggiore eguaglianza sociale e sia consentito dalla situazione economica e politica, di volta in volta interviene a favore delle categorie deboli, emarginate, discriminate. La costruzione del c.d. stato sociale risponde a queste esigenze il rifluire della coscienza sociale verso l'individualismo, l'egoismo, la concorrenza brutale, accompagnata dalla tendenza alla privatizzazione dei servizi, alla previdenza e assistenza private e facoltative, provoca lo smantellamento dello stato sociale e la ricerca non di modelli generali di giustizia, ma di sfere separate e graduate di giustizia – Solidarietà è quindi – in questa prospettiva pubblicistica – al tempo stesso un limite all'azione individuale dettato da regioni sociali e un obbligo (assunto dallo stesso legislatore ma imposto anche ai singoli) ad operare per la realizzazione di più equi rapporti sociali e di più umane condizioni di vita».

che consentano di intessere relazioni sociali e di partecipare adeguatamente alla vita lavorativa e alla fruizione dei servizi pubblici nel nuovo contesto digitale, in una società ormai "datificata" per via dell'inesorabile progressivo avvento di una tecnologia che si fa sempre più pervasiva, invasiva e complessa.

A fronte dell'innovazione tecnologica e della transizione (della società, dell'economia e delle istituzioni) verso il digitale, risponde ad un principio normativo di solidarietà la realizzazione di una società "inclusiva", in cui nessuno sia lasciato indietro: il *gap* tecnologico, oggi, si traduce in una esclusione dalle dinamiche sociali, politiche, istituzionali, economiche, lavorative, arrivando finanche ad un'esclusione dalla elementare fruizione dei servizi pubblici. Il dovere di solidarietà impone qui di creare i presupposti per il vivere sociale, nelle sue diverse manifestazioni, secondo logiche che avvicinano il principio stesso di *solidarietà* a quello di *uguaglianza* sostanziale e, nel contempo, consentono all'individuo che ne beneficia di essere parte della comunità e, al tempo stesso, di esercitare le sue prerogative individuali, perseguendo i propri interessi, esercitando i propri diritti, sviluppando la propria personalità, in un contesto sociale in cui si è inclusi e riconosciuti e, dunque, non tecnologicamente discriminati[80].

2.4. (*segue*): (iv) …e secondo le logiche della condivisione e dell'altruismo (*data altruism*)

Altro recente orizzonte a cui tende la direzione percorsa dal principio di solidarietà *in subjecta materia* è quella che punta al riutilizzo dei dati e al *data altruism.*

Si è già avuto modo di riportare, nella prima parte del presente scritto dedicata all'inquadramento normativo, i contenuti delle disposizioni aventi ad oggetto tali aspetti, tracciati da ultimo nel *Data Governance Act*. In queste pagine si intende darne una lettura critica, vagliando la loro portata e i problemi applicativi che ne conseguono, in relazione al principio di solidarietà.

[80] Benché riferita ad altro contesto, quello dell'immigrazione e della globalizzazione, valgono qui le illuminanti parole di Stefano Rodotà, là dove ha affermato che «compito della *solidarietà*, dal quale non può essere separata, è *l'inclusione*. (…) Il *riconoscimento* si presenta (…) come ulteriore elemento costitutivo della solidarietà, con effetti immediati sul modo in cui si istituisce il suo rapporto con *l'eguaglianza*. Se si considera, tra i monti riferimenti possibili, la Carta dei diritti fondamentali dell'Unione europea, lì si coglie con immediatezza come fondamento e ragioni dell'eguaglianza siano il riferimento alla diversità e il rifiuto della discriminazione. Non soltanto l'articolo 22 riconosce esplicitamente la diversità culturale, religiosa e linguistica. Soprattutto l'articolo 21 la declina analiticamente attraverso un lungo elenco del suo concreto articolarsi, che comprende le cause di discriminazione storicamente più consolidate, come il sesso o la razza, e alte di più recente riconoscimento, tra le quali le caratteristiche generiche, l'handicap, il patrimonio, l'orientamento sessuale. Una norma come questa costituisce una legittimazione dei molteplici modi dell'essere "diversi", sorretta dal divieto di ogni forma di discriminazione» (S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., pp. 86-87). Nel nuovo contesto tecnologico i rischi di discriminazione, a cui il principio di solidarietà e di uguaglianza sostanziale possono porre rimedio, sono dettati dal *gap* tecnologico che potrebbe escludere dalle relazioni sociali, economiche, lavorative, politiche e dalla fruizione dei servizi, pubblici e privati, chi non abbia i mezzi e le conoscenze per poter operare nel mondo digitale. In quest'ambito la solidarietà non passa per l'accettazione delle condizioni in cui si trovi l'altro, ma nella rimozione degli ostacoli che gli impediscano, di fatto, la partecipazione alla società.

All'art. 2, par. 1, n. 16), di tale Regolamento UE, l'«*altruismo dei dati*» viene definito, testualmente, come «la *condivisione* volontaria di dati sulla base del consenso accordato dagli interessai al trattamento dei dati personali che li riguardano, o sulle autorizzazione di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di *interesse generale*, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

Su tale istituto sono state sollevate alcune osservazioni critiche da parte dell'*European Data Protection Board* (EDPB) e dell'*European Data Protection Supervisor* (EDPS), i quali, nel loro parere congiunto n. 03/2021 reso sul testo della proposta di regolamento relativo alla *governance* europea dei dati (vers. 1.1), hanno chiarito che, in verità, non siamo di fronte ad una facoltà nuova, ma solamente alla formalizzazione di facoltà che già erano ravvisabili, almeno con riferimento ai dati di carattere personale, nell'ambito della disciplina prevista dal GDPR. Segnatamente, nel citato parere si precisa che il *Data Governance Act* «non "crea" bensì "formalizza/codifica" la possibilità (…) di rendere disponibili dati in via volontaria, già contemplata dal GDPR. Di fatto un interessato può già oggi acconsentire al trattamento di dati personali che lo riguardano, tra l'altro per finalità di ricerca scientifica»[81].

Ancora, l'EDPS e l'EDPS ritengono non sufficientemente chiaro il concetto stesso di "altruismo dei dati", così come il suo «valore aggiunto (…), tenendo conto del quadro giuridico già esistente a norma del GDPR, che prevede condizioni specifiche per la validità del consenso»[82].

In realtà la disciplina del *data altruism* contenuta nel Reg. UE 868/2022 (DGA, *Data Governance Act*) risulta ben più ampia rispetto a quella ad esso applicabile a norma del GDPR, perché oltre ai dati personali (su cui l'*interessato* conserva poteri e facoltà tipici dell'autodeterminazione informativa) tale istituto riguarda anche i dati di carattere non personale, sui quali poteri e facoltà di controllo sono esercitati non dall'«*interessato*», ma dal «*titolare dei dati*», definito ora – nella versione finale del *Data Governance Act* pubblicata in G.U.U.E. del 3 giugno 2022 – come «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica *che non è l'interessato* rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli».

Inoltre, anche là dove l'altruismo dei dati sia esercitato dall'interessato e sia dunque relativo a dati di carattere personale, la disciplina in questione, contenuta nel *Data Governance Act*, va bel al di là delle statuizioni del GDPR: la medesima,

[81] EDPB-EDPS, *Parere congiunto n. 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla* governance *europea dei dati (Atto sulla* governance *dei dati)*, vers. 1.1, del 9 giugno 2021, p. 41.

[82] EDPB-EDPS, *Parere congiunto n. 03/2021*, cit., pp. 41 e 42.

infatti, individua, struttura e disciplina un apparato di soggetti e di strumenti – sia di controllo sia di tutela – non previsti nel regolamento europeo sulla protezione dei dati (Reg. UE 679/2016). Mi riferisco alle già menzionate «organizzazioni per l'altruismo dei dati» (artt. 17 ss.) e alla previsione di «registri pubblici delle organizzazioni per l'altruismo dei dati riconosciute» (art. 17), con indicazione dei requisiti generali di registrazione (art. 18) e specificazione di una disciplina *ad hoc* per la registrazione di tali organizzazioni (art. 19). Mi riferisco, ancora, alla previsione, a carico delle organizzazioni per l'altruismo dei dati riconosciute, di puntuali obblighi di trasparenza (art. 20) ed altri obblighi specifici di tutela dei diritti e degli interessi in favore sia degli interessati che dei titolari dei dati, nonché alla previsione un codice *ad hoc*, che sarà emanato in stretta collaborazione con le organizzazioni per l'altruismo dei dati e i pertinenti *stakeholders*, ad integrazione delle disposizioni del *Data Governance Act*, in base ad atti delegati della Commissione europea (art. 22). Mi riferisco, ancora, all'istituzione di «Autorità competenti per la registrazione di organizzazioni per l'altruismo dei dati» e alla previsione di un «Monitoraggio della conformità» (art. 23) per assicurare la *compliance* al sistema normativo» (art. 24).

Certo, anche tale disciplina non è esente da altri rilievi critici, in quanto, ad esempio, non è chiaro se la registrazione da parte delle organizzazioni per l'altruismo di dati sia obbligatoria e vincolante o no, come invece sembra di capire[83].

Si tratta comunque di disciplina che mira a incentivare la condivisione dei dati, personali e non personali, la loro circolazione, il loro "*secondary use*", con un apparato di norme che non lasci il settore sprovvisto di meccanismi di controllo e di tutela, anche aggiuntivi rispetto a quelli rinvenibili nella disciplina in materia di protezione dei dati personali, della quale occorrerà comunque tenere conto.

L'*altruismo dei dati* ha punti di contatto evidenti con il *principio di solidarietà*, perché vengono delineati strumenti per l'uso non autoreferenziale del dato, che circola nella prospettiva del soddisfacimento di interessi altri rispetto a quelli propri del soggetto a cui i dati si riferiscono o appartengono. È un meccanismo di solidarietà, tuttavia, che qui opera in maniera diversa rispetto alle altre ipotesi di applicazione del principio in parola: non si configura più come "dovere" (nella sua dimensione privatistica, di tipo orizzontale, o nella sua dimensione pubblicistica, di tipo verticale), ma come "atto volontario", come esercizio di autonomia privata, come atto di autodeterminazione informativa orientato al raggiungimento di interessi altrui o collettivi.

Qui la solidarietà non opera nella dimensione del dovere o dell'obbligo, a cui sembra essere confinata leggendo l'art. 2 Cost.: qui la solidarietà, personale e sociale, opera nella dimensione del diritto soggettivo, nella dimensione dei poteri e delle facoltà che sono rimesse al soggetto a cui i dati appartengono, in forza di un atto di autonomia privata che, come tale, è il frutto dell'autodeterminazione. È cioè espressione di libertà. Non siamo dunque al cospetto di una "solidarietà imposta", di

[83] Sul punto sono intervenute ulteriori rilievi critici da parte dell'EDPB e dell'EDPS. Cfr. EDPB-EDPS, *Parere congiunto n. 03/2021*, cit., p. 45, nella parte in cui si sollevano dubbi sulla mancanza di chiarezza in ordine all'obbligatorietà o meno della registrazione e all'applicabilità o meno di tale disciplina anche alle organizzazioni che decidano di non registrarsi, qualora ciò risulti possibile.

una solidarietà che si fa "dovere", ma di una "solidarietà volontaria", che non solo ha i tratti della "spontaneità"[84], ma è anche espressione della libera determinazione dell'individuo e che, quindi, si fa "diritto"[85].

Ciò si coglie bene nei presupposti con cui l'altruismo dei dati opera: il consenso dell'interessato, così come l'autorizzazione del titolare dei dati, è atto necessario, nell'impianto del *Data Governance Act*. Come può essere accordato, però, può anche essere revocato. A tal riguardo, nel loro parere congiunto, l'EDPB e l'EDPS

[84] Ricorda P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, Napoli, 2006, p. 435, che «La persona è inseparabile dalla solidarietà: aver cura dell'altro fa parte del concetto di persona. Il solidarismo è suscettibile di una pluralità di significati: solidarietà ai fini dello Stato o dei cittadini, *spontanea o imposta autoritativamente* (…)». L'A. prosegue declinando ulteriori possibili "significati" della solidarietà, con riferimento anche alle comunità intermedie, ai membri della famiglia, alle società commerciali e allo Stato. Tra gli atti di solidarietà spontanea e volontaria, collegata all'autodeterminazione dell'individuo che rifulge le logiche di mercato Stefano Rodotà annovera le "donazioni" di organi effettuate con anonimato bilaterale (v. S. Rodotà, *Solidarietà. Un'utopia necessaria*, cit., p. 55-56).

[85] Intendendo qui "diritto" non in senso oggettivo, ma nell'accezione soggettiva, come facoltà o potere. Come s'è già avuto modo di argomentare altrove, mi pare corretto inquadrare il consenso dell'interessato come rimozione di un vincolo giuridico che l'ordinamento ha posto per la tutela dell'interessato, al fine di consentire al titolare del trattamento il libero esercizio del proprio diritto a trattare dati personali, che il medesimo ricava dall'ordinamento giuridico non dall'atto di disposizione dell'interessato, ma da proprie prerogative, come avviene del resto qualora l'attività di trattamento sia posta in essere sulla base di altro fondamento giuridico, alternativo al consenso (v. F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., p. 116 ss.). La prestazione del consenso dell'interessato, così come la revoca di tale consenso, sono facoltà e poteri che l'ordinamento attribuisce all'interessato e quindi diritti di cui l'interessato gode, in funzione dell'autodeterminazione affermativa in cui si sostanzia il diritto alla protezione dei dati personali. Ciò non toglie, però, che tra titolare e trattamento possano venirsi ad instaurare anche rapporti di natura contrattuale tali da regolamentare in maniera specifica le dinamiche di trattamento relative ai dati personali, inclusa la facoltà di *utilizzo* dei dati (ovvero la facoltà di porre in essere *attività di trattamento* sui dati) per scopi di natura patrimoniale e commerciale, immettendo nuovi facoltà e nuovi obblighi, di natura pattizia, all'interno della cornice normativa delineata *ex lege*. La regolamentazione introdotta dal *Data Governance Act*, diversamente dall'impianto del GDPR, sembra spingere la circolazione verso logiche di *governance* sui dati improntate sul modello delle "licenze" (v. F. Bravo, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 241).
Sulla contrattualizzazione degli attributi della persona v. G. Resta, *Autonomia contrattuale e diritti della persona nel diritto UE*, in *Dig. disc. priv*., Agg. n. 8, Torino, 2013, pp. 92 ss. e, ivi, spec. pp. 96-97; ma anche Id., *La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della Carta dei diritti)*, in *Riv. dir. civ.*, 2022, II, pp. 801 ss. Sul rapporto tra consenso al trattamento dei dati personali e consenso contrattuale, nonché sulla contrattualizzazione dei rapporti successivamente al rilascio del consenso al trattamento dei dati personali da parte dell'interessato v. F. Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, pp. 34-58; Id., *Le condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, pp. 140 ss.; nonché G. Resta, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679*, in A.M. Gambino-A. Stazi (a cura di), *La circolazione dei dati. Titolarità, strumenti negoziali diritti e tutele*, Pisa, 2020, p. 74. Sulla matrice contrattuale del rapporto titolare-interessato si veda, inoltre, quanto diffusamente argomentato da V. Ricciuto, *L'equivoco della* privacy. *Persona* vs *dato personale*, cit., *passim* e, ivi, spec. pp. 118 ss.

rimarcano che «devono essere soddisfatti tutti i requisiti relativi al consenso stabiliti dal GDPR»[86] e che, pertanto, «la persona interessata non può in nessun modo "rinunciare" al diritto fondamentale alla protezione dei dati di carattere personale, neppure tramite un "atto di altruismo" relativo ai dati personali. Il titolare del trattamento (l'organizzazione per l'altruismo dei dati) resta pienamente vincolato dalle norme e dai principi in materia di dati personali anche quando l'interessato ha dato all'organizzazione per l'altruismo dei dati il proprio consenso al trattamento di dati personali che lo/la riguardano per una o più finalità specifiche»[87].

Sicché, all'art. 21, par. 3, del *Data Governance Act*, viene chiarito che «L'organizzazione per l'altruismo dei dati riconosciuta fornisce strumenti per ottenere il consenso degli interessati o le autorizzazioni al trattamento dei dati messi a disposizione dai titolari dei dati. L'organizzazione per l'altruismo dei dati riconosciuta fornisce altresì strumento per agevole revoca di tale consenso o autorizzazione». La disciplina, tuttavia, favorisce concretamente il rilascio del consenso, tramite il «Modulo europeo di consenso all'altruismo dei dati», contemplato all'art. 25 del *Data Governance Act*, ma in tale norma non si fa alcun riferimento alla revoca, sicché la previsione normativa finisce per facilitare la raccolta dei dati basata sul consenso e la loro successiva circolazione attraverso l'introduzione di un modello europeo per la raccolta del consenso al *data altruism*, ma trascura di estendere il modello europeo anche per l'esercizio del diritto di revoca del consenso già prestato, salvo un accesso alla possibilità di utilizzare il modello per la revoca di una specifiche operazione di trattamento (ma non del trattamento in sé, che potrebbe continuare con altre operazioni)[88].

V'è poi da dire che il consenso "solidaristico" al trattamento dei dati personali, in tale contesto, va sempre coordinato con gli altri principi in materia di trattamento, i quali conservano la loro portata anche a fronte dell'uso altruistico dei dati medesimi. Pertanto, anche ove fosse concesso il consenso al trattamento dei dati per

[86] EDPB-EDPS, *Parere congiunto n. 03/2021*, cit., p. 42.

[87] *Ibidem*.

[88] L'art. 25 del *Data Governance Act*, rubricato «*Modulo europeo di consenso all'altruismo dei dati*», statuisce significativamente al par. 1, che «Al fine di facilitare la raccolta dei dati basata sull'altruismo dei dati, la Commissione adotta atti di esecuzione per l'istituzione e l'elaborazione di un modulo europeo di consenso all'altruismo dei dati (…). Il modulo permette di raccogliere il consenso o l'autorizzazione in un formato uniforme in tutti gli Stati membri. (…). Al successivo par. 2 si precisa poi che «Il modulo europeo di consenso all'altruismo dei dati utilizza un approccio modulare, che ne consente la personalizzazione in funzione di settori specifici e finalità diverse». Si tratta di disposizioni che non menzionano la revoca del consenso, che invece appare contemplata al par. 3, con l'intento però di ridurla ad alcune operazioni soltanto, facendo in modo che possa essere mantenuto il consenso per le restanti operazioni di trattamento e, così, permettere il persistente utilizzo dei dati per finalità altruistiche. Nel par. 3 cit., infatti, si stabilisce che «Qualora siano forniti dati personali, il modulo europeo di consenso all'altruismo dei dati garantisce che gli interessati possano dare e revocare l proprio consenso a una specifica operazione di trattamento dei dati conformemente alle prescrizioni di cui al regolamento (UE) 2016/679». Nessun riferimento, invece, viene contemplato all'utilizzo del modulo europeo per revocare il consenso al trattamento dei dati personali per finalità altruistiche, ove lo stesso sia stato già conferito. L'ultimo paragrafo dell'articolo, infatti, si concentra su altri aspetti, affermando che «Il modulo è disponibile in un formato stampabile e facilmente comprensibile nonché in un formato elettronico predisposto per la lettura automatica» (par. 4).

finalità altruistiche, opera pur sempre il principio di minimizzazione dei dati, che imporrebbe tra l'altro il loro trattamento in forma anonima qualora ciò fosse possibile e adeguato alla finalità solidaristica per i quali i dati vengono trattati[89].

Altro aspetto delicato riguarda la specificazione delle finalità altruistiche: il consenso al trattamento dei dati personali, ai sensi del GDPR, deve essere granulare, nel senso che deve essere dato con riferimento ad un trattamento determinato e per finalità specifiche e anch'esse determinate. Tuttavia, già nel GDPR si chiarisce, nel *considerando* n. 33, che per la ricerca scientifica, in molti casi, non sia «possibile individuare pienamente la finalità del trattamento dei dati personali (…) al momento della raccolta dei dati. Pertanto dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settore della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica»[90]. Si tratta di applicazione in deroga alle disposizioni generali sul consenso, che sembrano trovare spazio nella normativa in esame proprio in base al principio di solidarietà: in ragione di essa, là dove viene richiesto il consenso dell'interessato, quest'ultimo viene mitigato nella sua portata. Viene dunque affievolita l'applicazione dell'autodeterminazione informativa, in ragione dell'interesse generale. Del resto è quanto ribadito all'interno del principio di limitazione delle finalità, di cui all'art. 5, par. 1, GDPR, ove si precisa che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali»[91].

Tale aspetto peculiare della disciplina del GDPR potrebbe trovare più ampio spazio nel *Data Governance Act*, perché si estende agli altri contesti in cui si esercita la "solidarietà volontaria" tipica del *data altruism*. Certo è che non è possibile prestare il consenso al trattamento per finalità di interesse generale in quanto tali, ossia «non rigorosamente definite e riferite a scopi possibilmente diversi e molto più ampi della ricerca scientifica»[92].

Il principio di solidarietà, in tale ambito dell'ordinamento, è destinato a intrecciarsi con il principio di autonomia privata ed appare comunque distante dalla portata deontica tracciata nella nostra Costituzione.

Il passaggio dalla *privacy* intesa come *the right to be let alone* (nella sua originaria accezione) alla *privacy* intesa come diritto alla protezione dei dati personali a fronte della loro necessaria circolazione e come autodeterminazione informativa

[89] Il rilievo è rinvenibile, ancora una volta, in EDPB-EDPS, *Parere congiunto n. 03/2021*, cit., p. 42.

[90] Cfr. EDPB-EDPS, *Parere congiunto n. 03/2021*, cit., p. 43, ove vengono richiamate anche le Linee Guida 5/2000 dell'EDPB sul consenso, con particolare riferimento al consenso per la ricerca scientifica, ivi a pp. 30-32, nonché le Linee Guida n. 03/2020 dell'EDPB sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19, ivi punti 42-43, e, infine, la portata applicativa dell'art. 89, par. 1, GDPR.

[91] Ved. art. 5, par. 1, GDPR. Cfr. anche il *considerando* n. 50 del *Data Governance Act*.

[92] EDPB-EDPS, *Parere congiunto n. 03/2021*, cit., p. 43. Ivi inoltre, a p. 44, viene criticata apertamente l'incertezza concernente la definizione di finalità di interesse generale nell'ambito dell'altruismo dei dati, rimasta non soddisfacentemente delineata nel testo della proposta ma anche nella versione definitiva, ove s'è preferito procedere con un elenco esemplificativo, contenuto nella definizione di altruismo dei dati di cui all'art. 2, par. 1, n. 16), lasciando al diritto nazionale degli Stati membri l'ulteriore puntuale specificazione.

(nella sua accezione attuale), implica l'abbandono della logica solipsistica ed autoreferenziale, che mira a confinare i dati nel solo perimetro della persona a cui i medesimi si riferiscono[93]. Si sta però assistendo ad un'ulteriore transizione, che mira ad esaltare le logiche di circolazione dei dati: siamo di fronte al passaggio dalla *protezione* alla *govenance* dei dati, ove però si ravvisano forme di controllo e di gestione in cui l'interessato si affiancano altri soggetti, pubblici e privati, che si pongono in posizione di intermediazione nel trattamento dei dati[94].

3. Applicazione del principio nella casistica

3.1. Il principio di solidarietà nei provvedimenti del Garante

Il Garante per la protezione dei dati personali, nei propri provvedimenti, ha fatto un ricorso davvero parco alla solidarietà. Viene ad esempio menzionata nelle Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti *web* esclusivamente dedicati alla salute (provvedimento n. 32 del 25 gennaio 2012, doc. web n. 1870212, pubblicato in G.U. n. 42 del 20 febbraio 2012), ove, nelle premesse, si sottolinea che «Il ricorso alle potenzialità del web con riferimento alle tematiche relative alla salute rappresenta una realtà in costante evoluzione. Lo scambio quotidiano tra utenti di informazioni, consigli, commenti e testimonianze, nei siti che si occupano di tali tematiche, testimonia l'utilità e il valore di queste esperienze sia con riguardo alla condivisione di conoscenze scientifiche sia con riguardo alla creazione di uno spazio di *solidarietà* e di reciproco sostegno umano.

Anche per questo è opportuno che il trattamento dei dati personali identificativi e sensibili degli utenti nell'ambito di siti *web* dedicati esclusivamente alla salute, all'interno dei quali si richiedono consigli, si scambiano informazioni e si inviano commenti, avvenga oltre che nel rispetto della disciplina sulla protezione dei dati personali e, in particolare, dei principi di pertinenza e non eccedenza, di correttezza

[93] L'evoluzione del concetto di *privacy* da tutela della riservatezza ad autodeterminazione informativa, ha generato una serie di equivoci, ben rimarcati da V. RICCIUTO, *L'equivoco della* privacy. *Persona* vs *dato personale*, cit., *passim*, tra cui quello di ritenere «che la *privacy* dovesse assurgere ad istituto *bon à tout faire* nella disciplina del rapporto tra individuo e nuovi strumenti della comunicazione e dell'informazione e dell'economia digitale» (*Ibidem*, p. 29), nonostante l'evidente «cambiamento (…) di nozione e funzione» che si vorrebbe però forzatamente ricomprendere sotto il medesimo allargato concetto di *privacy*, nonostante «la problematica coesistenza di due diverse nature e, appunto, funzioni: quella di protezione della propria sfera personale e privata, anche in chiave di rivisitazione dell'originaria riservatezza, certo anche dinanzi alla pervasività dei nuovi strumenti tecnologici; e quella di controllo e gestione che l'individuo può avere e deve fare delle proprie informazioni, in una prospettiva dinamica di governo della loro circolazione fuori dalla propria sfera privata, allorché il dato personale si propone nell'ottica delle relazioni esterne, con gli altri consociati e, tra queste, dei rapporti di scambio» (*Ibidem*, p. 30).

[94] Nel *Data Governance Act* rilevano, in particolare: (i) le pubbliche amministrazioni nell'ambito del riutilizzo in favore di terzi, per scopi commerciali e non commerciali, dei dati detenuti da enti pubblici (artt. 3-9); (ii) il fornitore dei servizi di intermediazione dei dati (artt. 10-15); nonché le organizzazioni per l'altruismo dei dati (artt. 16-25).

e buona fede (art. 11 del Codice), anche delle specifiche indicazioni contenute nelle presenti Linee-guida».

Il Garante, cioè, prende in considerazione la solidarietà quale esigenza aggiuntiva, ai fini dell'applicazione della disciplina, rispetto ai principi vigenti in materia di protezione dei dati, già contemplati nell'art. 11, poi abrogato, del Codice in materia di protezione dei dati personali e, successivamente, nell'art. 5 del GDPR.

Sicché, si precisa ancora nelle richiamate linee guida, «Con il presente provvedimento il Garante ritiene utile fornire indicazioni e raccomandazioni, allo scopo di prevenire i rischi connessi alla pubblicazione e diffusione dei dati relativi alla salute in Internet e, in particolare, di evitare un'impropria esposizione delle persone e dei loro dati più intimi nella rete. Ciò anche al fine di consentire agli utenti di partecipare, con maggior consapevolezza, a questi spazi di scambio di informazioni e di reciproca manifestazione di *solidarietà*».

La solidarietà viene qui invocata dall'*Authority* per orientare l'applicazione della disciplina, considerando la rilevanza della fattispecie ivi affrontata, ma non assurge, nel contesto del provvedimento ad esame, a criterio ordinante o a principio vincolante. Pare comunque indirizzare il Garante verso la dimensione della "funzione sociale" del trattamento dei dati personali, successivamente esplicitata dal legislatore europeo nel cit. *considerando* n. 4 del GDPR. La solidarietà viene qui utilizzata, dunque, come criterio interpretativo per l'applicazione della disciplina in esame, al fine di tener conto della "*funzione sociale*", con declinazione solidaristica, che il trattamento è in grado di realizzare.

In altri provvedimenti del Garante la "*solidarietà*" entra invece in rilievo, ai fini della decisione ivi adottata, quale particolare aspetto dell'obbligo di agire secondo *correttezza* nei rapporti contrattuali, che impone al titolare del trattamento di salvaguardare gli interessi dell'altro contraente al mantenimento della riservatezza. Poiché tuttavia il principio di correttezza è espressamente codificato, nella disciplina in materia di protezione dei dati personali, mentre quello di solidarietà no, l'Autorità interviene facendo esplicita applicazione del primo, ma non del secondo, benché nella sostanza operino, in tale contesto, congiuntamente[95].

[95] La correttezza si atteggia spesso, in materia di protezione dei dati personali, con i connotati della trasparenza. Celebre è ad es. il caso esaminato dal Garante nel provv. 10 ottobre 2006, doc. *web* n. 1345622 (e, in senso analogo, nel provv. 14 dicembre 2006 n. 1370954), relativo ad un servizio televisivo realizzato nell'ambito del programma «Le Iene», ove, per verificare tramite un *drug-test* se alcuni parlamentari all'uscita della sede istituzionale avessero assunto sostanze stupefacenti, era stato «utilizzato il duplice artificio di chiedere un'intervista per una non individuata tv satellitare e di far intervenire una finta truccatrice, la quale, simulando un intervento per asciugare la fronte dei parlamentari "intervistati", ha raccolto un campione di sudore su ciascun tampone, utilizzato poi per effettuare il predetto test in base alla tecnica del *drug-wipe*», con violazione dei principi di trasparenza e di correttezza). La trasparenza non è però il tratto connotante tipico della correttezza, dato che a quest'ultima deve essere riconosciuta una propria autonomia nel novero dei principi indicati all'art. 5, par. 1, lett. *a)*, del GDPR, come dimostrano le connessioni della correttezza con il principio di solidarietà, nell'ambito del quale, come rimarcato in queste pagine, la stessa correttezza finisce per prendere una direzione opposta rispetto alla trasparenza, come riscontrabile di fronte alla casistica che si sta considerando in queste pagine, dedicate alle dinamiche applicative del principio di solidarietà nel contesto della protezione dei dati personali.

In questa direzione, ad esempio, il Garante ha censurato un istituto di credito, titolare del trattamento, per non aver protetto la riservatezza e la "condifenzialità" delle informazioni di una propria cliente, delle quali aveva la disponibilità nell'ambito del rapporto contrattuale. Ci si riferisce al provvedimento del 23 maggio 2001, doc. web n. 39821, in tema di segreto bancario e comunicazione dei dati a soggetti terzi. Nel caso di specie, più precisamente, il dipendente di un istituto di credito per motivi d'ufficio aveva contatti di lavoro con un avvocato esterno all'istituto medesimo e, a fronte di una specifica richiesta proveniente da detto professionista, provvedeva a comunicargli o confermargli informazioni di natura economica relative ad una cliente della banca, avverso cui l'avvocato stava predisponendo delle difese per conto di un soggetto terzo. Il difensore, infatti, aveva ricevuto mandato dal di lei ex marito per resistere ad una domanda giudiziale proposta dalla donna per ottenere un aumento dell'assegno divorzile. L'interessata, però, contestava all'istituto di credito la violazione degli obblighi di segretezza derivanti dal segreto bancario e del dovere, di cui all'art. 1375 c.c., di comportarsi secondo buona fede nell'esecuzione delle prestazioni che discendono dalle obbligazioni contrattualmente assunte. Viceversa, l'istituto di credito riteneva che la comunicazione dei dati personali di natura economica dell'interessata, relativi al rapporto di conto corrente e di deposito titoli (che il legale aveva dichiarato di conoscere già e di cui richiedeva conferma), non fosse avvenuta in violazione di legge, sia perché non vi sarebbe una normativa che obbliga al c.d. segreto bancario, sia perché la disciplina in materia di protezione dei dati personali contempla, tra le condizioni di liceità del trattamento, anche quella relativa alla necessità di tutelare un diritto in sede giudiziaria.

Il Garante, nel dirimere la questione sottoposta alla sua attenzione, ha precisato, preliminarmente, che è priva di rilievo, ai fini dell'accertamento dell'illiceità della comunicazione, la circostanza addotta dall'istituto di credito, secondo cui la trasmissione dei dati economici dell'interessata al legale sarebbe avvenuta in buona fede e nel presupposto che il professionista fosse già a conoscenza di tali dati, e ciò «in quanto il dipendente, quand'anche si raggiungesse la prova che si è trattato di una semplice verifica e conferma dell'esattezza di dati già conosciuti dal legale, ha comunque posto in essere una "comunicazione" divulgando notizie od elementi che hanno fornito un contributo aggiuntivo di conoscenza al terzo richiedente (…)»[96].

Quanto ai presupposti di liceità della comunicazione, ha chiarito, nel provvedimento in esame, che la disciplina in materia di protezione dei dati personali «(…) permette al titolare del trattamento di comunicare dati personali senza il consenso dell'interessato, qualora la loro comunicazione sia necessaria per far valere o difendere un diritto in sede giudiziaria anche da parte di un terzo. Tale fattispecie prevede però per il titolare del trattamento una mera facoltà di fornire dati e non determina a suo carico l'obbligo giuridico di comunicarli. Simmetricamente, la norma non riconosce al terzo che richiede i dati il diritto di ottenerli»[97]. Tuttavia, precisa ancora il Garante, «Nell'esercitare o meno tale facoltà, il titolare del trattamento, oltre a valutare l'effettiva necessità della comunicazione ai fini dell'esercizio del diritto di

[96] GPDP, Provv. 23 maggio 2001, doc. *web* n. 39821.
[97] GPDP, Provv. 23 maggio 2001, doc. *web* n. 39821.

difesa, deve verificare che la natura dei dati, il contesto in cui essi sono trattati e, in particolare, il rapporto giuridico che lega il titolare medesimo all'interessato permetta di esercitare tale facoltà senza violare obblighi nascenti dalla legge o da un rapporto contrattuale. Nel caso di specie, il rapporto di conto corrente e quello legato alla gestione dei titoli precludeva la comunicazione dei dati in assenza del consenso dell'interessata o di un obbligo normativo»[98].

È proprio qui che entra in rilievo il principio di solidarietà, nel suo connubio con il principio di correttezza, colorando quest'ultimo – nella fattispecie qui esaminata – in direzione opposta rispetto alla trasparenza, a cui spesso si affianca quando le condotte passate al vaglio attengono al trattamento dei dati personali.

Il Garante ha chiarito, segnatamente, che «Nei rapporti delle banche con la clientela viene infatti in considerazione il c.d. segreto bancario, inteso come obbligo di mantenere il riserbo sulle operazioni, sui conti e sulle posizioni concernenti gli utenti dei servizi bancari (v., in particolare, Corte Cost. 3-18 febbraio 1992, n. 51). Tale obbligo, comunemente configurato come connaturato al rapporto banca-cliente in applicazione dei *principi di correttezza e buona fede* nell'esecuzione del contratto (artt. 1175, 1375 e 1337 del codice civile), è anche espressamente richiamato o presupposto da diverse disposizioni normative in materia fiscale e tributaria o in materia di riciclaggio, in relazione ai poteri di accertamento che permettono a determinati soggetti pubblici di acquisire notizie ed informazioni presso istituti di credito (…)[99]. I *doveri di confidenzialità* connessi al c.d. segreto bancario trovano anche riscontro negli usi e nelle consuetudini bancarie, nonché negli impegni che gli istituti di credito assumono nei confronti della clientela allorché dichiarano di rispettare le regole di comportamento indicate dalla relativa associazione di categoria, anche per ciò che attiene alla riservatezza nella raccolta e nel trattamento delle informazioni sui clienti (…)»[100].

Conclusivamente, pertanto, l'Autorità ha affermato che «fuori dei casi di operazioni di comunicazione di dati connesse alle prestazioni richieste o ai servizi erogati (e dei casi di adempimento di obblighi normativi in base ai quali gli istituti di credito devono fornire determinate informazioni a soggetti pubblici), gli istituti stessi ed il relativo personale devono mantenere il riserbo sulle informazioni relative ai propri clienti e non divulgarle a terzi. Il dipendente (…) che ha fornito i dati al legale li ha quindi comunicati in violazione del principio secondo cui i dati devono essere trattati lecitamente e secondo correttezza (…) e degli impegni assunti dalla banca

[98] GPDP, Provv. 23 maggio 2001, doc. *web* n. 39821.

[99] GPDP, Provv. 23 maggio 2001, doc. *web* n. 39821. Ivi il Garante aveva considerato, a titolo esemplificativo, «(…) l'art. 10, comma 2, n. 12) della l. 9 ottobre 1971, n. 825; l'art. 4 l. 9 agosto 1993, n. 328 di ratifica della convenzione di Strasburgo sul riciclaggio dell'8 novembre 1990; le norme sull'anagrafe dei rapporti di conto e di deposito, di cui all'art. 20, comma 4, l. n. 413/1991 e al d.m. 4 agosto 2000, n. 269 del Ministro del tesoro, del bilancio e della programmazione economica; Corte cost., 3-6 luglio 2000, n. 260 e Cass. civ., Sez. I, 7 agosto 1990, n. 7953, in materia di ordine di esibizione rivolto dal giudice civile ad un istituto di credito; v. anche la deliberaz. Consob n. 11522/1998 di attuazione del d.lgs. n. 58/1998, che impone al personale delle banche e degli altri intermediari precisi obblighi di riservatezza sulle informazioni di carattere confidenziale acquisite dagli investitori o di cui si disponga in ragione della propria funzione».

[100] GPDP, Provv. 23 maggio 2001, doc. *web* n. 39821.

(che assume la responsabilità giuridica della violazione quale titolare del trattamento) nei confronti della clientela in relazione ai servizi prestati, senza che l'interessata ne venisse peraltro informata. La segnalazione dell'interessata è pertanto fondata. Deve quindi ritenersi che la comunicazione non sia avvenuta nel rispetto del predetto principio»[101].

Il Garante, in aderenza ai principi codificati espressamente nella disciplina in materia di trattamento dei dati personali, tra i quali non compare espressamente quello di solidarietà, si appella alla correttezza, che tuttavia si colora di istanze solidaristiche, di protezione dell'interessato, in sintonia con l'analogo dovere di comportarsi secondo buona fede di cui all'art. 1375 c.c., che si affianca anche alle norme, di fonti diverse, in tema di segreto bancario. La *solidarietà* dunque non è stata menzionata espressamente nelle motivazioni del Garante, ma orienta la *correttezza* secondo logiche diverse rispetto alla *trasparenza*, traducendosi, nella fattispecie in esame, come obbligo di "confidenzialità", ossia come obbligo del titolare del trattamento (istituto di credito) di tutelare gli interessi dell'interessato (in questo caso l'altra parte contraente, ossia l'interessato), di fronte alla pretesa di terzi di acquisire informazioni giuridicamente rilevanti, che invece occorre mantenere riservate (e ciò nonostante fosse astrattamente applicabile la condizione di liceità che consentirebbe la comunicazione dei dati senza il consenso dell'interessato ove necessari per difendere un diritto in sede giudiziaria, invocabile anche qualora trattasi di diritto di un soggetto terzo).

Proprio in tema di segreto bancario, tuttavia, il principio di solidarietà potrebbe spingere nella diversa direzione il titolare del trattamento nella direzione opposta a quella analizzata nel caso precedente, traducendosi in un obbligo di comunicazione dei dati per esigenze superindividuali, connesse all'accertamento dei reati o alla necessità di assicurare che il concorso alle spese pubbliche in ragione della propria capacità contributiva.

Il riferimento espresso alla «solidarietà», con riguardo alle ipotesi di applicazione del segreto bancario ed alla sua ambivalente applicazione tra esigenze di confidenzialità a tutela della clientela e quelle di accessibilità e pubblicità connesse alla salvaguardia di interessi superindividuali, compare esplicitamente nelle «Linee guida per trattamenti dati relativi al rapporto banca-clientela» che il Garante ha reso il 25 ottobre 2007 (doc. *web* n. 1457247), pubblicate in G.U. n. 273 del 23 novembre 2007, ove, nella nota n. 13, si chiarisce che gli obblighi di protezione dei dati personali in tale materia sono «in armonia con il c.d. segreto bancario che si sostanzia nel dovere della banca di mantenere il riserbo in ordine alle notizie riguardanti i clienti nell'esercizio dell'attività bancaria, rispetto alle quali sussiste un interesse, meritevole di tutela, a che non siano divulgate o comunicate a terzi. Peraltro, come è noto, la Corte costituzionale (sentenza 18 febbraio 1992, n. 51) ha precisato che la tutela del c.d. segreto bancario, talora desunto dalla clausola generale di correttezza e di buona fede tra banca e cliente (artt. 1175 e 1375 c.c.), non può spingersi "fino al punto di fare di questo ultimo un ostacolo all'adempimento di doveri inderogabili di *solidarietà*, prima fra tutti quella di concorrere alle spese pubbliche in ragione

[101] GPDP, Provv. 23 maggio 2001, doc. *web* n. 39821.

della propria capacità contributiva (art. 53 della Costituzione), ovvero fino al punto di farne derivare il benché minimo intralcio all'attuazione di esigenze costituzionali primarie, come quelle connesse all'amministrazione della giustizia e, in particolare, alla persecuzione dei reati" (…)»[102].

Questo modo di intendere la *solidarietà* è invero legata alla «*funzione sociale*» del trattamento, che, in linea con quanto statuito dal *considerando* n. 4 del GDPR, limita le esigenze di riservatezza e di protezione dei dati, in ragione di superiori esigenze di interesse collettivo o di contrapposte situazioni giuridiche altrettanto rilevanti.

Così, ad esempio, il Garante è intervenuto in maniera sistematica a respingere le richieste di cancellazione dei dati dal registro delle imprese, inoltrate da imprenditori alle Camere di Commercio, ritenendo non illegittima la diffusione dei dati effettuata per le esigenze di pubblicità a cui è preordinato il registro delle imprese: si pensi, tra gli altri, al provv. 3 aprile 2003, doc. *web* n. 1128778, con cui il Garante ha ritenuto legittimo il rifiuto, da parte della Camera di Commercio, di espungere dalla visura camerale storica qualsiasi riferimento al fallimento dell'imprenditore, una volta che questi sia stato dichiarato riabilitato. Si veda anche, sempre a titolo esemplificativo, il provv. del 18 ottobre 2012, doc. *web* n. 2130054, con cui il Garante ha ritenuta legittima l'annotazione dell'esecuzione di pene accessorie a carico di un imprenditore nella visura camerale storica e la successiva annotazione della sentenza di riabilitazione emessa dal tribunale di sorveglianza[103].

3.2. Il principio di solidarietà nelle pronunce della Cassazione in tema di «funzione sociale» e in tema di risarcimento del danno da illecito trattamento di dati personali (ed altre significative sentenze della giurisprudenza di merito)

Anche la Suprema Corte di Cassazione, come s'è già avuto modo di precisare, è intervenuta sul bilanciamento tra il diritto alla protezione dei dati personali e l'interesse generale alla pubblicità delle notizie economicamente rilevanti assicurato dal sistema camerale, respingendo la pretesa dell'imprenditore alla cancellazione dei dati relativi ad un intervenuto fallimento, avanzata a seguito della riabilitazione.

Il Supremo Collegio, con la più volte citata ordinanza del 7 luglio 2015, n. 15096, si è pronunciato nell'ambito di un giudizio introdotto, in primo grado, dall'amministratore unico di una società di costruzioni che aveva ottenuto in appalto l'incarico di costruire un complesso turistico in una nota località, «affermando che le

[102] Significativamente le richiamate Linee guida del Garante, nella citata nota n. 13 relativa al tema della solidarietà quale limite al diritto alla protezione dei dati personali, si fa espressamente rinvio al provvedimento sopra illustrato in tema di segreto bancario (provv. 23 maggio 2001, doc. *web* n. 39821), che tuttavia colloca la solidarietà all'interno del rapporto contrattuale, per far valere le esigenze di protezione dell'interessato alla confidenzialità e alla riservatezza delle proprie operazioni economiche, traducendosi dunque in uno strumento di potenziamento della protezione dei dati personali e, corrispondentemente, come un limite alla circolazione dei dati.

[103] La casistica del Garante qui considerata si trova richiamata anche da Cass., sez. I civ., ord. n. 15096/2015, par. 4.6.6.

unità immobiliari, allo stato di rustico, non trovavano acquirenti, in quanto risultava dal registro delle imprese che (…) era stato l'amministratore unico e il liquidatore (…) [di altra società], il cui fallimento era stato dichiarato nel 1992 e si era chiuso il 10 marzo 1995, con cancellazione, all'esito della liquidazione, della società dal registro della imprese in data 7 luglio 2005»[104], lamentandosi della mancata cancellazione, da parte della Camera di Commercio, dell'informazione a lui pregiudizievole, nonostante la sua esplicita richiesta[105]. Chiedeva dunque che la Camera di Commercio territorialmente competente fosse condannata alla cancellazione o alla trasformazione in forma anonima o al blocco dei dati che ricollegavano il nome del ricorrente al fallimento menzionato nel registro delle imprese, oltre al risarcimento del danno subito.

Il giudice di prime cure accoglieva la domanda, ordinando all'ente camerale la trasformazione in forma anonima dei dati che collegavano l'imprenditore ricorrente al fallimento della società, accordando al contempo un risarcimento per danni non patrimoniali pari a duemila euro. Il Tribunale, in primo grado, aveva motivato le proprie argomentazioni ritenendo prevalente il diritto all'oblio dell'interessato, rilevando – come si legge nella ordinanza della Cassazione – che «è "difficilmente sostenibile la necessità e l'utilità dell'indicazione nominativa dell'amministratore unico della società al tempo del fallimento", per la circostanza che "si tratta di fatti avvenuto oltre un decennio prima e nonostante l'intervenuta cancellazione della società dal Registro delle Imprese da più di due anni", mentre la "memoria storica dell'esistenza della società e delle vicissitudini che l'hanno interessata (…) può essere ampiamente realizzata anche mediante dati anonimi". Ciò in quanto "le iscrizioni che collegano il nominativo di una persona fisica ad una fase patologica della vita dell'impresa (come il fallimento) non possono essere perenni, in mancanza di uno specifico interesse generale alla loro conservazione e divulgazione"; e, non prevedendo il codice civile un tempo massimo d'iscrizione, deve ritenersi che "trascorso un lasso di tempo congruo" dalla definizione del fallimento e cancellata l'impresa dal registro, cade la necessità e l'utilità (…) dell'indicazione nominativa dell'ex amministratore unico al tempo del fallimento, potendo l'interesse pubblico essere soddisfatto dall'indicazione delle vicissitudini della società con dati anonimi quanto alla persona fisica del rappresentante (…)»[106].

Avverso la sentenza di primo grado, però, l'ente camerale proponeva ricorso per Cassazione, nell'ambito di un giudizio nel quale il Supremo Collegio è pervenuto ad opposta soluzione, con l'ordinanza interlocutoria n. 15096 del 2015, cit.

Per la S.C. non assume rilevanza il mero trascorrere del tempo per poter ottenere la cancellazione dei dati personali, occorrendo un'analisi che tenga conto anche di altri importanti elementi valutativi. La Cassazione rimarca la rilevanza del regime di pubblicità camerale, sottolineando che «Costituisce *interesse generale*, tanti più nelle società complesse, che determinati fatti giuridici siano resi conoscibili a

[104] Cass., sez. I civ., ord. n. 15096/2015, cit.
[105] Cass., sez. I civ., ord. n. 15096/2015, cit.
[106] V. la ricostruzione delle motivazioni della pronuncia di primo grado, sottoposta al vaglio della S.C., così come riportata da Cass., sez. I civ., ord. n. 15096/2015, cit.

chiunque: da qui la previsione, in tutti gli ordinamenti moderni, del sistema della *pubblicità*, realizzata attraverso il sistema dei registri»[107]. Questi ultimi, aggiunge la S.C., «hanno enorme importanza, economica e sociale, in quanto producono o fanno circolare delle "speciali forme di sicurezza" circa eventi, che, direttamente o indirettamente, rendono sicuri, o quantomeno più agevoli, i rapporti economici e sociali. Il "cardine" intorno a cui ruotano questi procedimenti è la nozione di certezza: tali strumenti hanno un tratto strutturale e funzionale comune, che consiste nel dar *certezza* di fatti giuridicamente rilevanti»[108]. Si tratta però di *funzione* che può essere assolta in maniera soddisfacente solamente qualora le informazioni siano rese pubbliche in maniera *duratura*[109]. Il servizio di memorizzazione delle informazioni nel registro delle imprese e il servizio di consultazione «costituiscono attività integrante una *pubblica funzione* svolta nell'*interesse generale della certezza del diritto* (…) [dato che] lo scopo esplicito dei registri pubblici, quale il registro delle imprese, consiste nel creare una fonte di informazioni attendibile nei rapporti giuridici e pertanto nel garantire la certezza del diritto necessaria ai fini degli scambi sul mercato»[110].

Tali considerazioni devono essere tenute ben presenti quando ci si trova di fronte ad istanze che intendano far valere il c.d. diritto all'oblio, ovvero del diritto alla cancellazione dei dati soprattutto a fronte di una pretesa perdita di loro attualità: l'interesse generale alla tenuta del registro pubblico delle imprese per la conservazione duratura delle informazioni di carattere economico andrebbe infatti salvaguardato, evitando di sacrificare irreparabilmente i diritti di rango costituzionale e gli interessi generali al cospetto di un solo diritto fondamentale, che altrimenti «diverrebbe "tiranno" nei confronti della altre situazioni giuridiche costituzionalmente riconosciute e protette»[111]. È sull'esigenza di bilanciamento, portato della «*funzione sociale*» predicata nel *considerando* n. 4 del GDPR[112] che entra in gioco il principio

[107] Cass., sez. I civ., ord. n. 15096/2015, cit., par. 4.4.1.

[108] Cass., sez. I civ., ord. n. 15096/2015, cit., par. 4.4.1.

[109] Cass., sez. I civ., ord. n. 15096/2015, cit., par. 4.4.1, ove si trova affermato che «i pubblici registri realizzano lo scopo della sicurezza giuridica (e scongiurano il *far west*). La loro essenziale caratteristica è perciò l'idoneità alla formazione di documenti di cui permettono la conservazione e la facile esibizione in modo duraturo, in quanto interessano un numero indeterminabile di figure soggettive presenti e future».

[110] Cass., sez. I civ., ord. n. 15096/2015, cit., par. 4.4.2.

[111] Cass., sez. I civ., ord. n. 15096/2015, cit., par. 4.4.5, con chiaro riferimento alla "tirannia dei valori" di Carl Schmitt (C. Schmitt, *La tirannia dei valori*, 5ª ed., Milano, 2008).

[112] A. Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, cit., pp. 604 ss., ove viene rimarcato che, «Declinando il diritto alla protezione del soggetto cui si riferiscono le informazioni iscritte nel registro delle imprese alla luce della "funzione sociale", si rivela la necessità di bilanciare la pretesa dell'interessato al controllo sulle informazioni riferite alla sua persona con il diritto dei terzi alla certezza dei rapporti economici e alla trasparenza degli assetti imprenditoriali, reso quest'ultimo effettivo dal regime di pubblicità legale dei registri. In ragione dello scopo sotteso al trattamento delle informazioni iscritte nel registro delle imprese, il diritto alla protezione dei dati personali può quindi subire una restrizione di contenuto che si traduce, a parere di chi scrive, nell'impossibilità di chiedere la cancellazione del dato di natura personale dal registro in ragione del decorso del tempo. In altri termini, la limitazione del diritto alla cancellazione, espressamente riconosciuto dalla legge ed estrinsecazione del diritto all'autodeterminazione informativa, si giustifica per la strumentalità del dato personale al perseguimento di una pubblica funzione».

di solidarietà, esplicitamente richiamato dalla Cassazione nell'ordinanza ora in esame, ove s'è chiarito che «Il bilanciamento degli interessi dell'economia ed il corretto funzionamento del mercato anche con i diritti fondamentali è dunque ammesso ed, anzi, ritenuto doveroso dal giudice italiano delle leggi. Deve richiamarsi il principio di solidarietà secondo cui "il vincolo solidale è destinato a segnare l'agire sociale di ogni componente, sia pubblica, che privata, operando inscindibilmente con il principio di uguaglianza, quel necessario contemperamento tra posizioni idiosincratiche e socialità, attraverso doveri che si impongono per la tutela e la protezione di beni e valori della comunità nel suo complesso"»[113].

La giurisprudenza della Suprema Corte, per la verità, ha mostrato di fare applicazione del principio di solidarietà anche per negare rilevanza a richieste risarcitorie concernenti danni non patrimoniali che, pur derivanti da illeciti effettivamente accertati, siano di lieve entità o siano cagionati da condotte socialmente ritenute non gravi. In tal caso la solidarietà si traduce nella necessità che la vittima sia tollerante rispetto a condotte che, pur formalmente illecite, possano comportare danni sopportabili, in ragione della loro tenuità o dell'assenza di gravità dell'illecito secondo la percezione sociale. Tale indirizzo giurisprudenziale, delineato dalla Corte di Cassazione a Sezione Unite all'interno di motivazioni rese in un caso di malasanità, con Cass., sez. un., sent. 11 novembre 2008, n. 26972, è stato successivamente applicato in maniera sistematica anche con riguardo alla casistica concernente i danni derivanti trattamenti illeciti di dati personali.

Si tratta di orientamento che, seppur autorevolmente sostenuto, non convince affatto e meriterebbe un serio ripensamento, per le ragioni illustrate nel prosieguo. Alle critiche già emerse nell'accordato dibattito dottrinale sollevatosi su tale tema si aggiungono elementi ulteriori desumibili dalla disciplina europea sulla *data protection*, che hanno poi trovato esplicitazione nella recente sentenza della Corte di giustizia dell'UE, già citata, resa il 4 maggio 2023 nella causa C-300/21.

Le Sezioni Unite, nella pronuncia del 2008 poc'anzi richiamata, hanno affermato che «Il risarcimento di pretesi danni esistenziali è stato frequentemente richiesto ai giudici di pace ed ha dato luogo alla proliferazione delle c.d. liti bagatellari. Con tale formula si individuano le cause risarcitorie in cui il danno consequenziale

Cfr. anche ID., *Pubblicità del registro delle imprese e diritto alla protezione dei dati personali. Alcune riflessioni a margine di una recente sentenza di Cassazione, in attesa della decisione della Corte di Giustizia dell'Unione Europea*, in *Giustiziacivile.com*, 2016, 5; nonché A. MANTELERO, *Diritto all'oblio e pubblicità nel registro delle imprese*, in *Giur. it.*, 2015, pp. 2651 ss.
V. altresì CGUE, sez. II, sent. 9 marzo 2017, causa c-398/15, *Camera di commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*.

[113] Cass., sez. I civ., ord. n. 15096/2015, cit., par. 4.4.5, ove si cita anche Cass. 15 luglio 2014, n. 16133, in tema di danno non patrimoniale da violazione del diritto alla protezione dei dati personali e Cass., sez. un., 11 novembre 2008, n. 26972, «laddove ha puntualizzato come il bilanciamento tra i diritti inviolabili della persona ed il *dovere di solidarietà* comporti che non sia risarcibile il danno per lesione di quei diritti che non superi il "livello di tollerabilità" che "ogni persona inserita nel complesso contesto sociale (…) deve accettare in virtù del dovere di d tolleranza che la convivenza impone"), in ragione della "primigenia vocazione sociale dell'uomo" e della "originaria connotazione dell'uomo *uti socius*" (Corte cost. 28 febbraio 1992, n. 75; 17 dicembre 2013, n. 309; v. pure Cass., sez. un., ord. 1° ottobre 2014, n. 20661)».

è futile o irrisorio, ovvero, pur essendo oggettivamente serio, è tuttavia, secondo la coscienza sociale, insignificante o irrilevante per il livello raggiunto. In entrambi i casi deve sussistere la lesione dell'interesse in termini di ingiustizia costituzionalmente qualificata, restando diversamente esclusa in radice (al dei fuori dei casi previsti dalla legge) l'invocabilità dell'art. 2059 c.c. La differenza tra i due casi è data dal fatto che nel primo, nell'ambito dell'area del danno-conseguenza del quale è richiesto il ristoro è allegato un pregiudizio esistenziale futile, non serio (non poter più urlare allo stadio, fumare o bere alcolici), mentre nel secondo è l'offesa arrecata che è priva di gravità, per non essere stato inciso il diritto oltre una soglia minima: come avviene nel caso del graffio superficiale dell'epidermide, del mal di testa per una sola mattinata conseguente ai fumi emessi da una fabbrica, dal disagio di poche ore cagionato dall'impossibilità di uscire di casa per l'esecuzione di lavori stradali di pari durata (in quest'ultimo caso non è leso un diritto inviolabile, non spettando tale rango al diritto alla libera circolazione di cui all'art. 16 Cost., che può essere limitato per varie ragioni)»[114].

Tale argomentazione, tuttavia, finisce per aggiungere requisiti ulteriori rispetto agli elementi essenziali della struttura dell'illecito, nel caso di richieste risarcitorie concernenti danni non patrimoniali (*ex* art. 2059 c.c.): la serietà del danno e la gravità della lesione.

Ciò è ribadito in un ulteriore passaggio della richiamata sentenza della Suprema Corte, nella quale si statuisce espressamente che «La *gravità dell'offesa* costituisce *requisito ulteriore* per l'ammissione a risarcimento dei danni non patrimoniali alla persona conseguenti alla lesione di diritti costituzionali inviolabili. Il diritto deve essere inciso oltre una certa soglia minima, cagionando un *pregiudizio serio*. La lesione deve eccedere una certa soglia di offensività, rendendo il pregiudizio tanto serio da essere meritevole di tutela in un sistema che impone un grado minimo di tolleranza»[115]. È sotto tale profilo che entra in rilievo il *principio di solidarietà*, che imporrebbe alla vittima – per esigenze di convivenza sociale – di soprassedere a richieste risarcitorie per illeciti di tipo bagatellare, che posso essere composti attraverso una solidaristica accettazione di condotte da ritenersi socialmente tollerabili, perché non gravi, o comunque che arrechino pregiudizi non seri e, dunque, contenuti. Il Supremo Collegio rileva infatti che «Il filtro della gravità della lesione e della serietà del danno attua il bilanciamento tra il *principio di solidarietà* verso la vittima, e quello di *tolleranza*, con la conseguenza che il risarcimento del danno non patrimoniale è dovuto solo nel caso in cui sia superato il livello di tollerabilità ed il pregiudizio non sia futile. Pregiudizi connotati da futilità ogni persona inserita nel complesso contesto sociale li deve accettare in virtù del *dovere della tolleranza* che la convivenza impone (art. 2 Cost.). Entrambi i requisiti devono essere accertati dal giudice secondo il parametro costituito dalla coscienza sociale in un determinato momento storico»[116].

[114] Cass., sez. un., sent. 11 novembre 2008, n. 26972, par. 3.10.
[115] Cass., sez. un., sent. 11 novembre 2008, n. 26972, par. 3.11.
[116] Cass., sez. un., sent. 11 novembre 2008, n. 26972, par. 3.11.

Il principio di solidarietà così inteso porta dunque all'introduzione di filtri selettivi che incidono sulla clausola generale dell'«ingiustizia del danno costituzionalmente qualificata», invocata dalle stesse Sezioni Unite, portando ad un arretramento di quelle «mobili frontiere del danno ingiusto» che, proprio ad opera della giurisprudenza, avevano avuto nel tempo un'incredibile *vis* espansiva[117].

Ovviamente l'indirizzo delle Sezioni Unite è stato ripreso dalla giurisprudenza successiva, nonostante le sonore e puntuali critiche sollevate da attenta dottrina[118].

Si pensi in tal senso, tra le altre, anche a Cass., sez. III, 9 aprile 2009, n. 8703, ove s'è ritenuto assente il requisito dell'«ingiustizia costituzionalmente qualificata» del danno qualora quest'ultimo non superi i filtri della serietà del danno e della gravità della lesione, con riguardo ad un'ipotesi di lamentata frustrazione del diritto alla tranquillità individuale. Più precisamente, nella richiamata sentenza la S.C. ha rimarcato che, nella specie sottoposta al suo esame, «non sussiste un'ingiustizia costituzionalmente qualificata, tantomeno si verte in un'ipotesi di danno patrimoniale prevista dal legislatore ordinario, risultando, piuttosto, la ritenuta lesione del "diritto alla tranquillità" insuscettibile di essere monetizzata, siccome inquadrabile in quegli sconvolgimenti [della] quotidianità "consistenti in disagi, fastidi, disappunti, ansie ed in ogni altro di insoddisfazione" (c.d. bagatellari) ritenuti non meritevoli di tutela risarcitoria (pag. 34 della sentenza n. 26972/2008). In conclusione, il (...) ricorso va accolto e (...) la sentenza impugnata va cassata senza rinvio, (...) e – in applicazione dei principi affermati dalle SS.UU. sopra richiamati – la domanda di risarcimento (...) va rigettata»[119].

Significativa è, a tal riguardo, anche la sent. n. 16133 del 15 luglio 2014 con cui la terza sezione della Corte di Cassazione ha deciso relativamente ad una fatti-

[117] Sulle "mobili frontiere del danno ingiusto" memorabili sono le pagine di Francesco Galgano, con riflessioni che si mostrano ancora attuali, a fronte della riapertura del dibattito sulla clausola generale del danno ingiusto, recentemente rilanciato da Contratto e impresa. Si veda, in proposito, F. GALGANO, *Le mobili frontiere del danno ingiusto*, in *Contratto e impresa*, 1985, 1, p. 1 ss., ripubblicato anche nel 2023, 1, p. 3 ss.; G. ALPA, *Responsabilità civile: la frontiera più esposta dell'ordinamento privato alle novità economiche e sociali*, in *Contratto e impresa*, 2023, 1, p. 1 ss.; G. VISINTINI, *Deviazioni dottrinali in tema di danno ingiusto*, in *Contratto e impresa*, 2023, 1, p. 31 ss.

[118] Si veda, ad es., G. PONZANELLI, *Sezioni Unite: il «nuovo statuto» del danno non patrimoniale,* in *Foro it.*, 2009, I, p. 134 ss., spt. par. 3); G. GRISI, *Il danno (di tipo) esistenziale e la nomofilachia «creativa» delle Sezioni Unite*, in *Eur. dir. priv.*, 2009, 2, p. 379 ss., spt. par. 8; P.G. MONATERI, *Il pregiudizio esistenziale come voce del danno non patrimoniale*, in *Resp. civ. e prev*., 2009, 1, p. 56 ss., spt. par. 6; P. ZIVIZ, *Il danno non patrimoniale: istruzioni per l'uso*, in *Resp. civ. e prev*., 2009, 1, p. 94 ss., spt. parr. 7 e 8. *Contra*, cfr. E. NAVARRETTA, *Il valore della persona nei diritti inviolabili e la complessità dei danni non patrimoniali*, in *Resp. civ. e prev*., 2009, 1, p. 63 ss., par. 2.2.1. Si vedano anche D. POLETTI, *La dualità del sistema risarcitorio e l'unicità della categoria dei danni non patrimoniali*, in *Resp. civ. e prev.*, 2009, 1, p. 76 ss., parr. 2 e 3; e C. SCOGNAMIGLIO, *Il sistema del danno non patrimoniale dopo le decisioni delle Sezioni Unite*, in *Resp. civ. e prev.*, 2009. 2, p. 261 ss., par. 2.1.3, i quali tuttavia denunciano le evidenti aporie per i diseguali criteri nel determinare le soglie di risarcibilità tra danni patrimoniali e non patrimoniali.

[119] Nella vicenda sottoposta all'esame della S.C., ci si doleva delle lungaggini dell'iter burocratico affrontato per ottenere lo sgravio di somme non dovute, la cui richiesta era contenuta in una cartella esattoriale di cui era stato ottenuto l'annullamento solo a sei mesi di distanza, dopo numerose richieste e reiterati solleciti, visite allo sportello e ingiustificati rinvii e dinieghi.

specie in cui veniva contestata la violazione del diritto alla riservatezza per illecito trattamento dei dati personali effettuato da una nota università romana, in quanto «risultava possibile, oltre che attraverso l'indirizzo, inserito direttamente in Internet, (...) anche con la sola digitazione del nome e cognome o soltanto il cognome sul motore di ricerca Google, avere accesso al *file excel* (...) recante il nominativo di 3.724 studenti specializzandi e/o *ex* studenti specializzati, tra cui quello dei ricorrenti, con evidenziazione dei relativi dati personali e cioè generalità, codice fiscale, attività di studio, posizione lavorativa e retributiva».

In primo grado il Tribunale di Roma accoglieva le richieste dei ricorrenti, disponendo «la cancellazione dal *web* dei dati personali ed identificativi dei medesimi, contenuti nel predetto *file excel*, inibendone la diffusione all'Università resistente, che condannava, altresì, al risarcimento dei danni non patrimoniali patiti dagli stessi attori, liquidati nella somma di Euro 3.000,00, oltre interessi legali, in favore di ciascuna parte»[120].

In particolare, «Il Tribunale, ritenuto che la divulgazione delle informazioni personali dei ricorrenti risultava sproporzionata rispetto alle finalità proprie del trattamento, escludeva che gli stessi avessero subito un danno patrimoniale, mentre, quanto al danno non patrimoniale, pur essendo stato dedotto "il patema d'animo sofferto per rischio di possibili furti della propria identità, con la necessità di continui controlli", riteneva non dimostrata "tale ultima circostanza", riscontrando, però, a fondamento del liquidato pregiudizio, un "disagio conseguente alla propria (indiscriminata) esposizione personale anche di carattere economico"»[121].

La Cassazione ha tuttavia censurato la sentenza di primo grado, con rinvio ad altro giudice del Tribunale di Roma. Nelle sue motivazioni ha fatto applicazione del *principio di solidarietà*, riconducendo ad esso il dovere di tolleranza nei rapporti sociali. Segnatamente, la S.C. ha sostenuto che, «in una lettura costituzionalmente orientata, l'art. 2059 c.c., nell'affermare la risarcibilità del danno non patrimoniale, è norma di rinvio "ai casi previsti dalla legge" (e quindi ai fatti costituenti reato o agli altri fatti illeciti riconosciuti dal legislatore ordinario produttivi di tale tipo di danno) ovvero ai diritti costituzionali inviolabili presidiati dalla tutela minima risarcitoria, con la precisazione, in quest'ultimo caso, che la rilevanza costituzionale deve riguardare l'interesse leso e non il pregiudizio conseguentemente sofferto e che la risarcibilità del pregiudizio non patrimoniale presuppone, altresì, che la lesione sia grave (e cioè superi la *soglia minima di tollerabilità*, imposta dai *doveri di solidarietà sociale*) e che il danno non sia futile (vale a dire che non consista in meri disagi o fastidi o sia addirittura meramente immaginario)" (ancora la citata Cass. n. 8703 del 2009)»[122].

Ciò che la Cassazione critica, di fronte al ragionamento del giudice di merito, è che nella sentenza impugnata s'è proceduto all'accertamento del danno non patrimoniale da illecito trattamento dei dati personali, poi liquidato ai ricorrenti, facen-

[120] Cfr. Cass., sez. III, 15 luglio 2014, n. 16133, nella parte in cui ricostruisce la vicenda processuale, anche di *prime cure*.
[121] Cass., sez. III, 15 luglio 2014, n. 16133.
[122] Cass., sez. III, 15 luglio 2014, n. 16133.

do tuttavia «riferimento al mero "disagio conseguente alla propria (indiscriminata) esposizione personale anche di carattere economico", mancando, (...) [tuttavia], di rendere pienamente intelligibile lo sviluppo dei criteri che hanno guidato un tale giudizio, il quale, come sopra evidenziato in linea di principio, avrebbe dovuto formarsi all'esito di una verifica in concreto circa la gravità della lesione e la serietà del danno»[123].

Anche altre pronunce utilizzano il *principio di solidarietà* quale *dovere di tolleranza* che, ai sensi dell'art. 2 Cost., imporrebbe di soprassedere rispetto a richieste risarcitorie per illecito trattamento di dati personali di rilevanza marginale. In tal senso si veda, ad es., Cass., sez. III, sent. 3 marzo 2015, n. 4231, relativa ad una fattispecie in cui, in relazione ad un sinistro stradale, l'interessato – quale titolare della polizza assicurativa e quale soggetto in comunione dei beni con la danneggiante, conducente del veicolo – contestata l'uso dei propri dati personali all'interno di una comunicazione indirizzata alla compagnia assicuratrice e all'ISVAP, contenente toni ritenuti dispregiativi, non rispondenti ai principi di limitazione della finalità e minimizzazione dei dati, che governano il trattamento dei dati ai sensi dell'art. 11 del Codice in materia di protezione dei dati personali (ora art. 5 GDPR). Anche in tale sentenza si trova affermato che «Il danno non patrimoniale, risarcibile ai sensi del d.lgs. 30 giugno 2003, n. 196, art. 15 (cosiddetto codice della *privacy*) [ora art. 82 GDPR, *n.d.a.*], pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost., e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), in quanto anche per tale diritto opera il bilanciamento con il *principio di solidarietà ex* art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto, non la mera violazione delle prescrizioni poste dall'art. 11 del codice della *privacy* [ora art. 5 GDPR, *n.d.a.*] ma solo quella che ne offenda in modo sensibile la sua portata effettiva (Cass., 15 luglio 2014, n. 16133)»[124].

Si tratta dunque di indirizzo giurisprudenziale destinato ad incidere in maniera significativa sulla risarcibilità dei danni in tema di illecito trattamento di dati personali, con una casistica che si dimostra piuttosto variegata, riscontrabile nelle decisioni di merito e in quelle di legittimità.

Con sentenza resa il 25 febbraio 2020 dal Tribunale di Reggio Calabria, sez. II, il principio di solidarietà, applicato secondo le scelte nomofilattiche delle Sezioni Unite della Cassazione, ha portato ad escludere la risarcibilità del danno da trattamento dei dati personali lamentato per la pubblicazione della propria immagine su Internet, non oscurata, visibile nell'ambito del noto servizio *Google Street View*, di cui non era stata dimostrata la serietà della lesione, al di là della normale tollerabilità[125]. Argomentazioni analoghe si riscontrano anche in Cass., sez. VI, 20 agosto

[123] Cass., sez. III, 15 luglio 2014, n. 16133.

[124] Cass., sez. III, sent. 3 marzo 2015, n. 4231.

[125] Trib. Reggio Calabria, sez. II, 25 febbraio 2020, in AIDA, 2020, 1, p. 694, secondo cui, in applicazione dei principi espressi dalla Cassazione, «In caso di pubblicazione *online* dell'immagine di

2020, n. 17383, ove il Supremo Collegio ha rigettato il ricorso con cui un'associazione professionale chiedeva la cassazione della sentenza di primo grado, che aveva rigettato le richieste risarcitorie avanzate contro un istituto di credito per violazione del dovere di segretezza delle informazioni bancarie in relazione ad una raccomandata inviata presso lo studio associato, priva di busta e ripiegata su se stessa, contenente la revoca degli affidamenti concessi nel termine di cinque giorni. Anche in questo caso s'è ritenuto esente da censure l'accertamento operato dal giudice di merito, secondo cui non sarebbe stata raggiunta la prova in ordine al danno risarcibile e alla serietà della lesione oltre la soglia minima di tolleranza richiesta in applicazione del principio di solidarietà[126].

Nella stessa direzione si è proiettata anche Cass., sez. I, ord. 31 dicembre 2020, n. 29982, con cui è stata confermata la pronuncia del Tribunale che ha provveduto a respingere la richiesta risarcitoria avanzata da un collaboratore scolastico nei confronti del dirigente amministrativo della scuola ove prestava servizio, per asserito illecito trattamento di dati personali, lamentando che sarebbe stato «indebitamente rivelato alla Polizia giudiziaria che lui era stato in passato destinatario di contestazioni disciplinari e che tale notizia si era diffusa nell'ambito dell'istituto scolastico, così cagionandogli umiliazione, disagio e imbarazzo»[127].

---

una persona senza il suo consenso, il danno non patrimoniale derivante dalla lesione di diritti fondamentali dell'individuo o diritti della personalità, quali il diritto alla riservatezza, all'immagine e alla reputazione, non può essere ritenuto sussistente *in re ipsa*, ma deve essere debitamente allegato e provato, anche mediante presunzioni semplici; occorre inoltre che il danno subito non sia futile, ovvero non consista in meri disagi o fastidi, ma superi la soglia della normale tollerabilità (nella specie: si trattava dell'immagine di una persona acquisita e pubblicata nell'ambito del servizio *Street View di Google*)».

[126] Così Cass., sez. VI, 20 agosto 2020, n. 17383, ove si trova precisato quanto segue: «Il terzo motivo è infondato. Non è esatto che il d.lgs. n. 196 del 2003, artt. 11 e 15 [ora artt. 5 e 82 GDPR, *n.d.a.*], riconoscono il risarcimento *in re ipsa* del danno per il solo fatto del trattamento dei dati personali (p. 10 del ricorso). Ed invero, il danno non patrimoniale risarcibile ai sensi del d.lgs. 30 giugno 2003, n. 196, art. 15 (cosiddetto codice della *privacy*) [ora art. 82 GDPR, *n.d.a.*], pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà *ex* art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della *privacy* [ora art. 5 GDPR, *n.d.a.*] ma solo quella che ne offenda in modo sensibile la sua portata effettiva. Il relativo accertamento di fatto è rimesso al giudice di merito e resta ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale ed al suo essere maturata in un dato contesto temporale e sociale (Cass. 16133/2014; Cass. 20615/2016). E, nel caso di specie, il giudice di merito ha accertato, con motivata valutazione in fatto incensurabile, l'assenza di qualsiasi danno risarcibile».

[127] Cass., sez. I, ord. 31 dicembre 2020, n. 29982, cit., ove si conferma la rilevanza della fattispecie nell'ambito della disciplina in materia di protezione dei dati personali, ma si evidenzia che l'interessato abbia omesso di contestare la serietà e la gravità della lesione, in relazione all'applicazione del principio di solidarietà di cui all'art. 2 Cost., prospettata dal giudice di primo grado nella sentenza impugnata. Segnatamente, dopo aver richiamato l'indirizzo giurisprudenziale della Cassazione sulla "solidarietà sociale" che richiede il rispetto della soglia minima di tolleranza, rendendo risarcibile solo il danno che si dimostri essere grave e di non lieve entità, la S.C. ha ivi precisato che «Non solo

In altri casi i filtri indicati dalla Cassazione, quali nuovi ed addizionali elementi costitutivi dell'illecito non patrimoniale, hanno portato ad un vaglio positivo in ordine alla risarcibilità del danno.

Si registrano così alcune sentenze che utilizzano l'argomentazione relativa al *dovere di tolleranza* quale espressione del *principio di solidarietà* sociale ai sensi dell'art. 2 Cost. per ammettere le richieste risarcitorie: ciò ove il danno subito si palesi di entità e gravità tali da superare la soglia minima di accettazione, secondo una valutazione rapportata al sentire sociale, che il giudice di merito è chiamato ad interpretare ed applicare nella fattispecie concreta. In questa direzione la Suprema Corte ritiene di applicare il principio di solidarietà, come sopra declinato, per confermare la condanna inferta dal giudice di primo grado al risarcimento dei danni non patrimoniali liquidati in via equitativa nella somma di seimila euro, quale conseguenza di una illecita segnalazione alla Centrale Rischi come cattivo pagatore, integrante l'ipotesi di illecito trattamento dei dati personali. Ci si riferisce a Cass., sez. I, 8 gennaio 2019, n. 207, che ha ritenuto provata la serietà del danno, tale da superare la soglia minima di tolleranza a cui la vittima è tenuta ai sensi del principio di solidarietà sociale di cui all'art. 2 Cost.

Ancora, il Tribunale di Monza, sez. IV, con sent. 1° dicembre 2021, n. 2198, ha condannato R.T.I. spa al risarcimento dei danni subiti per violazione del proprio diritto alla riservatezza, alla reputazione e alla *privacy*, per un importo di ventimila euro, in conseguenza della diffusione, in un noto programma televisivo, di informazioni riservate e sensibili dell'interessata, senza le dovute cautele volte a renderla non riconoscibile, nell'ambito di un video registrato e divulgato – in televisione e *online* – senza il consenso dell'interessata. In particolare, la ricorrente affermava di lavorare come meretrice in un locale, all'insaputa dei propri familiari, rendendo una serie di particolari della propria vita privata all'intervistatore – un giornalista che si era mostrato come un cliente intenzionato solamente a "scambiare due chiacchiere" – mandati in onda nell'ambito di un programma giornalistico di larga diffusione, a seguito del quale era stata tuttavia riconosciuta dai propri parenti e conoscenti, benché nel video diffuso televisivamente fosse stata utilizzata una modella con il volto oscurato e fosse stato fatto ricorso ad un nome di fantasia in luogo di quello reale. La riconoscibilità dell'interessata era stata infatti possibile sia perché era stata diffusa la sua voce senza alcun filtro, sia perché le informazioni di carattere personale diramate televisivamente contenevano particolari che la rendevano ben identificabile da parte di chi la conoscesse. Il Tribunale, nella pronuncia testé richiamata, ha affermato che «L'art. 82 del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio prevede espressamente che chiunque subisca un danno materiale o immateriale per effetto della violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento. Quanto al danno causalmente correlabile all'ille-

il ricorrente non affronta la ragione addotta dal Tribunale, che peraltro si risolve in una valutazione di merito insindacabile in sede di legittimità, ma omette anche di farlo nell'unica prospettiva potenzialmente rilevante, stante la mancata censura della *ratio* (…) della serietà e gravità del pregiudizio scaturito dalla trasmissione dell'informazione esclusivamente alla Polizia giudiziaria e al Pubblico Ministero».

cita diffusione di dati personali afferenti alla sfera sessuale dell'interessato, valgono gli ordinari criteri elaborati sul punto da parte della giurisprudenza di legittimità che, a far data dalla nota pronuncia delle Sezioni Unite della Corte di Cassazione n. 26972 del 2008, ha ricondotto alla categoria dei danni non patrimoniali tutti i danni risarcibili non aventi contenuto economico in base al combinato disposto degli artt. 2043 e 2059 c.c., riconoscendo il diritto al risarcimento qualora il fatto illecito abbia violato in modo grave diritti inviolabili della persona, in quanto tali oggetto di tutela costituzionale. Il danno non patrimoniale, determinato dalla lesione di interessi inerenti alla persona non connotati da rilevanza economica, costituisce una categoria unitaria, non suscettibile di divisione in sottocategorie, laddove il riferimento ai vari aspetti del pregiudizio diversamente qualificati (danno morale, danno biologico, danno esistenziale, da perdita del rapporto parentale, etc.) risponde ad esigenze meramente descrittive delle possibili configurazioni che il pregiudizio può assumere senza minarne l'essenza ontologicamente unitaria: costituisce compito del giudice accertare l'effettiva consistenza del pregiudizio dedotto sul piano non patrimoniale individuando, sulla base delle allegazioni svolte, quali ripercussioni negative si siano in concreto verificate sulla persona che assume la lesione, a prescindere dal nome loro attribuito. Su questo assunto si fonda l'affermazione per cui il danno non patrimoniale appartiene alla categoria del danno conseguenza e, come tale, deve essere sempre allegato e provato da chi ne pretende il risarcimento e la prova può essere data con ogni mezzo. La sola circostanza che i dati siano stati utilizzati dal titolare in modo illecito, di conseguenza, non legittima di per sé l'interessato a richiedere il risarcimento del danno non patrimoniale che, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. nonché dall'art. 8 Cedu, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" – intesa quale perdita di natura personale effettivamente patita dall'interessato –, in quanto anche per tale diritto opera il bilanciamento con il *principio di solidarietà*, parimenti tutelato dall'art. 2 Cost., tale per cui le lesioni minime devono essere tollerate»[128].

[128] Così Trib. Monza, sez. IV, sent. 1° dicembre 2021, n. 2198. Ivi si chiarisce, quanto alla dimostrazione del danno e degli elementi relativi alla sua gravità e serietà, che «Nella fattispecie in esame le allegazioni indicate nel ricorso introduttivo sono state accompagnate da specifici elementi di valutazione che consentono di valutare le ripercussioni nella vita privata effettivamente subite dalla (…) [interessata] anche tenuto conto dell'*id quod plerumque accidit*. Le circostanze di fatto allegate dalla ricorrente, unitamente alle deposizioni dei testimoni escussi nell'ambito dell'attività istruttoria, costituiscono infatti argomenti di prova sufficienti a far presumere che il comportamento della società resistente, giudicato illecito per la violazione delle regole deontologiche che regolano l'esercizio dell'attività giornalistica e per il mancato assolvimento dell'onere probatorio in merito alla continenza espositiva e all'essenzialità delle informazioni divulgate, sia stato lesivo del diritto fondamentale della ricorrente alla propria riservatezza, e le abbia cagionato un danno non patrimoniale. La ricorrente ha in conclusione dimostrato sia la sussistenza di una condotta illecita, *sub specie* di illecito trattamento dei suoi dati personali, che l'esistenza di un danno causalmente riconducibile all'illecita violazione dei dati personali di cui precede. Tutti i testimoni escussi hanno infatti riportato che le informazioni diffuse nell'intervista corrispondono a eventi della vita privata della ricorrente e che la voce della (…) [interessata] era riconoscibile per la cadenza, la risata.
Dopo la diffusione del video nell'ambito del programma televisivo (…) e la sua visibilità in rete anche in un momento successivo, d'altronde, amici, conoscenti e parenti della (…) [interessata]

Si tratta però, come più diffusamente illustrato nel prosieguo di discorso, di applicazione non condivisibile del principio di solidarietà, che, in tema di protezione dei dati personali, finisce per cozzare sia con il dettato stesso della costituzione, sia con le superiori norme di diritto europeo formatosi in materia di protezione di dati personali, sia con i tratti connotanti del principio in parola, avuto riguardo alla funzione del diritto nell'ordinamento giuridico italiano ed europeo.

3.3. Riflessioni critiche sulla deriva giurisprudenziale in tema di "solidarietà-tolleranza" e sui filtri selettivi della "gravità della lesione" e della "serietà del danno". Le peculiarità in tema di protezione dei dati personali

L'interpretazione della Cassazione in tema di danni non patrimoniali derivanti da illecito trattamento di dati personali, detto francamente, non pare condivisibile per diverse ragioni, alcune delle quali già ben rimarcate in dottrina con riferimento alle citate sentenze di "San Martino" (Cass., sez. un., nn. 26972, 26973, 26974 e 26975 dell'11 novembre 2008) e per altre ancora che in questa sede si aggiungono.

La motivazione espressa dalle Sezioni Unite nelle richiamate pronunce del 2008 è stata ritenuta troppo «*frettolosa*»[129], incappando in un errore metodologico proprio nel punto in cui richiede, per la risarcibilità del danno non patrimoniale, i requisiti aggiuntivi della serietà del danno e della gravità dell'offesa, che dovrebbero invece «operare come criteri di risarcimento del danno: non già, invece, quali metri di selezione dei danni non patrimoniali»[130].

Sotto altro profilo, il doppio filtro fissato dalla S.C. – s'è rimarcato dagli "anti-esistenzialisti" e dagli "esistenzialisti", perfettamente d'accordo sul punto –, finisce per creare l'evidente paradosso di rendere inaccettabilmente ammissibile la "violabilità dei diritti inviolabili", seppur all'interno della soglia minima individuata giurisprudenzialmente[131].

---

hanno appreso della professione svolta dalla stessa e, trattandosi di un piccolo Comune, la notizia è circolata velocemente anche al bar frequentato abitualmente dalla ricorrente e ove la stessa aveva lavorato. Il tempo durante il quale il servizio è rimasto in onda – d'altronde – ha fatto sì che anche chi non aveva visto il video potesse vederlo dopo che la sua diffusione era stata resa nota all'interno del Comune.

Le ricadute negative sulla reputazione e sull'identità personale della ricorrente, in conclusione, vengono presunte, sulla base dell'oggettiva portata diffamatoria delle informazioni divulgate, considerato che lo svolgimento dell'attività di prostituzione, peraltro vietato in Italia, è connotato da un profondo disvalore sociale».

[129] G. PONZANELLI, *op. cit.*, par. 4.

[130] *Ibidem*. L'A. ha qui ben colto, con efficace sintesi, un aspetto di grande rilievo ai fini di un più corretto inquadramento dei termini del discorso, ricollocando i criteri della serietà del danno e della gravità della lesione sul piano delle valutazioni relative al *quantum* e non all'*an* del risarcimento.

[131] Tra gli "anti-esistenzialisti" v. in particolare PONZANELLI, *op. cit.*, par. 4, il quale apertamente rimarca che «A mio modo di vedere, i diritti inviolabili, se sono tali, devono essere sempre risarciti (anche con un piccolo risarcimento nel caso si trattasse di un danno non serio)». Tra gli "esistenzialisti" si veda, invece, ZIVIZ, *op. cit.*, par. 7, nella parte in cui rimarca che «I due parametri selettivi proposti dalle Sezioni Unite appaiono – in verità – alquanto discutibili. Per quanto riguarda la regola della gravità dell'offesa, si tratta di un criterio che non gode di alcun riscontro normativo; nessuna indica-

Ciò basterebbe a portare al di fuori del perimetro costituzionale i criteri selettivi del danno proposti dalla Cassazione (utilizzabili invece per la quantificazione). Si noti, il discorso non cambia neanche qualora si volesse addurre, in senso contrario, la tesi del contemperamento proporzionale dei contrapposti interessi, perché «Vero è che l'art. 2 Cost. pone sullo stesso piano e con eguale dignità, garanzia dei diritti inviolabili dell'uomo e doveri di solidarietà, ma l'esigenza di bilanciamento degli interessi che allora emerge non può autorizzare lo snaturamento dei caratteri propri dell'inviolabilità; caratteri che – le S.U. avrebbero dovuto rammentarlo – riflettono la dimensione "di un diritto che, essendo intangibile nel suo contenuto di valore, può essere unicamente disciplinato da leggi generali che possono limitarlo soltanto al fine di realizzare altri interessi costituzionali altrettanto fondamentali e generali" (così, testualmente, Corte cost. 3-3-1988 n. 235, *Foro it.*, 1988, I, 1801)»[132].

L'attrito con la Costituzione, invero, è rilevabile sotto diversi profili. Non solo per la preminenza che finirebbe per avere la risarcibilità del danno patrimoniale sul danno alla persona, in contrasto con il principio personalistico evincibile dalla lettura della Carta costituzionale[133], ma anche per via del contrasto con il diritto di difesa di cui all'art. 24 Cost., che le Sezioni Unite vorrebbero scalfire proprio innanzi alle richieste risarcitorie di danni non patrimoniali per lesione di diritti fondamentali, rendendolo invece privo di soglie risarcitorie al cospetto di richieste di risarcimento, anche minimo, per danni di carattere patrimoniale[134].

Siamo qui di fronte ad "aporie" che, invero, scontano il problema della compatibilità anche con l'art. 3 Cost., nella parte in cui l'applicazione dei filtri limitativi delle richieste risarcitorie, fissate per i soli danni non patrimoniali, finiscono irragionevolmente per creare evidenti disparità di trattamento, se non vere e proprie

---

zione in tal senso, in particolare, può essere distillata in via ermeneutica all'interno delle ipotesi di espressa risarcibilità del danno non patrimoniale. Ponendosi altresì come criterio limitativo ulteriore in materia di tutela dei solo diritti inviolabili, tale regola si colloca in aperto contrasto con la logica costituzionale di primazia della persona sul patrimonio, in quanto essa dà vita al paradosso della "violabilità dei diritti inviolabili": per questi ultimi sarebbe infatti richiesto – entro una certa soglia – di dover tollerare le relative aggressioni, mentre in campo patrimoniale anche la minima lesione giustificherebbe l'attivazione della salvaguardia aquiliana».
Nello stesso senso si veda anche G. Grisi, *op. cit*., par. 8, per il quale, con riguardo all'art. 2 Cost., «L'impedimento opposto alla possibilità di accesso alla tutela risarcitoria quando la lesione incida su "diritti costituzionalmente inviolabili" della persona e presenti i caratteri dell'illecito – si è notato – ben difficilmente conciliabile con il riconoscimento e la garanzia dei diritti inviolabili dell'uomo che, proprio in virtù di detta disposizione, devono essere assistiti da una tutela cui ognuno, senza restrizioni, può attingere in modo incondizionato». Così anche P.G. Monateri, *op. cit.*, par. 6, là dove afferma che «Siamo per ammissione delle stesse Sezioni di fronte a ipotesi di violazione di diritti inviolabili».

[132] G. Grisi, *op cit.*, par. 8, il quale ha modo di precisare che «Non c'è legge (…) richiamabile nel nostro caso, né questo vuoto può essere validamente colmato dal pronunciamento – ancorché autorevole – della S.C.: la critica alla linea tracciata dalle S.U. e all'apprezzamento operato della solidarietà riceve, dunque, conferma».

[133] Si veda, ancora una volta, quanto richiamato nella nota precedente.

[134] Il rilevo è di G. Grisi, *op cit.,* par. 8. Questi, sul punto, ben chiarisce che «allo stato, se l'art. 24 Cost. sancisce che essendo in gioco la tutela di diritti soggettivi l'azione in giudizio è nella disponibilità di tutti i titolari, evidentemente è per consentire ad essi – previi gli accertamenti del caso – di ottenere tutela piena e non per far sì che alcuni se la vedano negata».

"discriminazioni", rispetto a chi lamenti il pregiudizio al patrimonio, risarcibile illimitatamente, senza i predetti filtri[135].

Il discorso va poi riconsiderato anche alla luce di un inquadramento sistematico di più ampia portata. Osservando la tesi della Cassazione alla luce dell'ordinamento europeo, nei cui confronti quello italiano deve essere ricondotto a sistema, emergono ulteriori rilievi critici, non adeguatamente emersi nel dibattito dottrinale. In questo senso la disciplina in materia di protezione dei dati personali offre argomentazioni decisive.

Il regime risarcitorio dei danni, patrimoniali e non patrimoniali, in materia di protezione dei dati personali è da rapportare anche al tenore di cui all'art. 82 GDPR, che è norma contenuta in un regolamento eurounitario (Reg. UE 679/2016) volto ad assicurare regole uniformi in tutti gli Stati dell'UE, incluse quelle sulla risarcibilità dei danni derivanti da trattamenti di dati personali[136]. Si tratta, com'è noto, di norme non derogabili in sede nazionale, né da parte del legislatore italiano, né da parte della giurisprudenza "creativa" della Suprema Corte nazionale, la cui funzione nomofilattica deve pur arrestarsi di fronte alla supremazia del diritto unionale e all'unitarietà dei criteri risarcitori voluti dal legislatore europeo.

È chiaro che le esigenze di uniforme applicazione del dritto europeo – in particolare quelle in tema di risarcimento dei danni patrimoniali e non patrimoniali da trattamenti di dati personali di cui all'art. 82 GDPR, in connessione con il diritto alla

[135] C. SCOGNAMIGLIO, *op. cit*., par. 2.2.1, parla a tal riguardo, di «aporie tutt'altro che trascurabili» e di dubbi in ordine all'«effettiva coerenza sistematica, pure all'interno di una scelta ordinamentale di fondo che voglia restare correttamente agganciata al sistema bipolare», giacché, «portando fino alle sue estreme conseguenze il ragionamento imperniato sul dovere di tolleranza, v'è da chiedersi se, allo stesso modo in cui ciascun consociato è chiamato a sopportare un pregiudizio non patrimoniale "insignificante o irrilevante per il livello raggiunto" (secondo l'esemplificazione delle Sezioni Unite, il graffio superficiale dell'epidermide o il mal di testa per un sola mattinata dipendente dalla inalazione dei fumi di una fabbrica), analoga soluzione non finirebbe per doversi imporre quando al pregiudizio patrimoniale bagatellare (la "strisciatina" sulla propria autovettura in un parcheggio, la lacerazione del proprio vestito che un urto accidentale sull'autobus può determinare). Nel caso di pregiudizio non matrimoniale irrilevante o insignificante prospettati dalla Corte non può soccorrere, come criterio selettivo, quello del diritto della persona costituzionalmente garantito (la salute lo è, ovviamente), cosicché, a meno di non voler ritenere (ciò che, in prospettiva, potrebbe anche costituire uno scenario condivisibile) che pure il danno patrimoniale bagatellare debba essere sopportato da chi lo subisce, si creerebbe una discriminazione tra danno patrimoniale e danno non patrimoniale, che anche il criterio selettivo dell'art. 2059 c.c. non pare automaticamente giustificare». Un rilievo analogo è rinvenibile anche nelle argomentazioni di D. POLETTI, *op. cit.*, che parla di «irragionevole disparità di trattamento», che, secondo l'A., potrebbe essere eventualmente rimossa tentando in via interpretativa il recupero di un fondamento di unitarietà, generalizzando la portata applicativa, sia per i danni patrimoniali che per i danni non patrimoniali, dei filtri limitativi della gravità dell'offesa e della serietà del danno, al fine di espungere in ogni caso dall'area della risarcibilità i c.d. danni bagatellari. Si tratta però di operazione che poggia pur sempre sul ricorso a criteri selettivi introdotti in via giurisprudenziale, non sul piano normativo, e che presentano problemi di raccordo non solo con il principio di uguaglianza, ma anche con altre garanzie costituzionali e con i principi dell'ordinamento europeo.

[136] F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 383 ss.

protezione dei dati personali riconosciuto quale diritto fondamentale ai sensi dell'art. 8 della Carta dei diritti fondamentali dell'UE – non consentono l'interpretazione riduttiva sui limiti alla risarcibilità dei danni non patrimoniali, voluti dalle Sezioni Unite della Cassazione. Sarebbe altrimenti invocabile l'intervento della Corte di giustizia dell'UE, con una pronuncia interpretativa volta a verificare la compatibilità con l'ordinamento europeo dei criteri selettivi introdotti nel nostro sistema giuridico per la risarcibilità del danno non patrimoniale, se non un'apertura della procedura di infrazione per violazione delle disposizioni in materia di risarcibilità del danno da illecito trattamento dei dati personali di cui agli artt. 82 GDPR e 8 Carta dei diritti fondamentali dell'UE[137]. Il regime europeo di responsabilità da illecito trattamento dei dati personali, infatti, finirebbe per essere (inammissibilmente) disapplicato dai giudici italiani, nel caso in cui il danno non patrimoniale riportato dall'interessato sia accertato al di sotto della soglia di rilevanza definita dalle Sezioni Unite della Cassazione[138].

[137] Il rischio di una procedura di infrazione e la necessità di richiedere quantomeno una pronuncia interpretativa della Corte di giustizia dell'UE, per l'unitaria applicazione del diritto europeo, senza possibilità di applicazione delle soglie di gravità del danno, erano stati evidenziati in F. Bravo, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, cit., p. 430.

[138] La questione potrebbe porsi anche per altre materie. P.G. Monateri, *op. cit.*, par. 6, ricorda ad esempio l'evidente contraddizione tra l'indirizzo delle Sezioni Unite, che negano soddisfazione risarcitoria ai «pregiudizi consistenti in disagi, fastidi, disappunti, ansie ed in ogni altro tipo di insoddisfazione…», mentre tale tutela è pacificamente ammessa, a titolo esemplificativo, in caso di «sconvolgimento della vita famigliare di fronte a violazioni dell'art. 8, comma 1, l. n. 848 del 1955 di ratifica della Convenzione europea per la salvaguardia dell'uomo e delle libertà fondamentali. Orbene in un caso analogo di violazione dell'art. 8, ritardo dei servizi sociali nell'assegnazione di una casa adeguata ad un disabile, affrontato dall'arcigna *Queen's Bench Division* della *High Court*, Mr. Justice Sullivan ha affermato con riferimento alla giurisprudenza della Corte di Strasburgo, e con riferimento al Report dell'ancor più arcigno Lord Woolf, *Master of the Rolls*, che in questi casi le categorie di danno (*categories of loss*) che devono venir risarcite includono: "*ditress, frustration, inconvenience, humiliation and anxiety*". (…) Nel diritto comparato è raro che si possano trovare due proposizioni identiche ma di segno assolutamente contrario come queste. Il giudice inglese, e il *Master of Rolls* (!), ritengono palese che in tali casi si debbano risarcire quei danni che i giudici italiani ritengono *palesemente* non meritevoli della tutela risarcitoria (!)».
V'è chi, diversamente argomentando, ha notato che l'indirizzo delle Sezioni Unite finisce illogicamente per far degradare la pretesa risarcitoria in una sorta di indennità, al cospetto di lesione dei diritti inviolabili, che reclamerebbero invece ben altro trattamento. Si veda A. di Maio, *Danno esistenziale o di tipo esistenziale: quale l'esito?*, in *Corriere giur.*, 2009, p. 414, il quale sottolinea che l'orientamento delle Sezioni Unite finisce per fissare una regola simile a quella introdotta nell'ordinamento tedesco, ove si associa al danno non patrimoniale una «equa riparazione in danno» e non «il risarcimento *stricto sensu*». Il tema è ripreso anche da G. Grisi, *op. cit.*, par. 7, il quale nega che nel nostro ordinamento possa avere ingresso un istituto analogo a quello che si registra «in Germania soprattutto in forza del richiamo al c.d. *Bereicherungsverbot*», in cui è vigente «un regime che, affidando valore selettivo al giudizio che dalla coscienza sociale promana, introduca limitazioni alla risarcibilità dei danni non patrimoniali volte ad impedire l'accesso alla tutela alle liti cc.dd. bagattellari. (…) Le S.U. (…), senza rilevarlo, hanno finito in pratica per attrarre il risarcimento dei danni non patrimoniali nella logica indennitaria, ma il percorso seguito e l'esito raggiunto (…) non convincono. La verità è che l'ancoraggio a quella logica presuppone lo svincolo del risarcimento dalla razionalità risarcitoria, cosa che da noi, nell'attuale quadro normativo, è assai complicata, per non dire impossibile, da configurare».

Altre considerazioni riguardano gli aspetti ontologici e funzionali del principio di solidarietà, nell'attuale quadro normativo nazionale ed europeo. Non si può fare a meno di notare, sotto tale profilo, che la forza normativa del principio di solidarietà – volto a dare "concretezza", nell'ordinamento giuridico, all'"utopia necessaria" predicata da Stefano Rodotà[139] –, risulta del tutto ridimensionata dalla "deriva" giurisprudenziale in tema di risarcibilità dei danni non patrimoniali di cui s'è dato conto ora, che finisce per piegare tale principio normativo ad esigenze non sempre aderenti al tessuto valoriale che ad esso si ricollega. Tale giurisprudenza, infatti, finisce per degradare la solidarietà, colorandola di sfumature dai connotati intrinsecamente contradditori rispetto alla sua stessa essenza.

Invero, quando ci si pone di fronte alla portata applicativa del principio normativo di solidarietà, non si può separare l'analisi del dato normativo testuale dalla cornice assiologica in cui esso si colloca, come precisato da Guido Alpa nelle sue pagine dedicate a tale tema, giacché l'analisi del dato normativo non può che rappresentare solamente il punto di avvio della ricerca in ordine ai suoi confini semantici, che però «si deve spingere a considerare i valori che il termine racchiude (...)»[140].

Mi pare tuttavia che l'indagine sul significato assunto dal principio di solidarietà in sede giurisprudenziale mostri il tentativo malcelato di spostare l'asse valoriale della solidarietà verso esigenze ulteriori e addirittura contrapposte a quelle che la stessa solidarietà, quale principio normativo, dovrebbe esprimere nelle relazioni intersoggettive, secondo il nostro ordinamento giuridico, nazionale ed europeo.

La solidarietà è espressione, nella sua matrice, di "fratellanza" e "coesione" sociale[141] e nei rapporti di diritto privato dovrebbe tradursi nell'applicazione delle clausole generali, soprattutto in quelle di buona fede e di correttezza[142], che nella particolare materia della protezione dei dati personali assurgono anch'esse a principio normativo, declinato esplicitamente nell'art. 5, par. 1, lett. *a)*, GDPR[143].

La migliore dottrina, che ha indagato la solidarietà anche nei rapporti contrattuali, ha messo in risalto proprio la connessione di quest'ultima con la clausola di buona fede e correttezza (enucleata sia nell'art. 1175 c.c., sia negli artt. 1366 e 1375 c.c.): si tratta di una clausola utilizzata da una storica pronuncia della Corte di Cassazione per argomentare l'applicazione del principio di solidarietà di cui all'art. 2 Cost. anche nei rapporti contrattuali, ma qui, si noti, la *solidarietà* ha il significato inequivocabile del *dovere di salvaguardare l'altrui interesse* nei limiti in cui ciò non comporta un apprezzabile sacrificio dell'interesse proprio[144].

---

[139] S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit.

[140] G. ALPA, *Solidarietà. Un principio normativo*, cit., p. 82.

[141] Significativa è l'espressione scelta per il titolo scelto da Eligio Resta per la sua opera monografica dedicata proprio al «diritto fraterno» (E. RESTA, *Il diritto fraterno*, Roma-Bari, 2005). Su «fraternità e solidarietà» si veda anche S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., p. 20 ss., nonché G. ALPA, *Solidarietà. Un principio normativo*, cit., p. 20 ss., 33 ss., 71 ss., 108 ss. e 178.

[142] G. ALPA, *Solidarietà. Un principio normativo*, cit., p. 232 ss. e, spt., 235 ss.

[143] F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 101 ss.

[144] Cfr. G. ALPA, *Solidarietà. Un principio normativo*, cit., p. 237 s., il quale rimarca la significatività di Cass., sent. 20 marzo 1994, n. 3775, in *Foro it.*, I, 1995, c. 1296, sul noto "caso Fiuggi", nelle cui

La clausola di buona fede e correttezza, ovviamente, è applicabile nello stesso senso non solo nei rapporti contrattuali, ma anche negli ulteriori rapporti obbligatori delineati *ex lege*, come ben si evince sia dalla collocazione sistematica dell'art. 1175 c.c., sia dall'affermazione esplicita del principio di correttezza nei rapporti relativi a fattispecie di trattamento di dati personali: è menzionata nell'art. 5, par. 1, lett. *a)*, GDPR, che trova ovviamente applicazione anche là dove tra titolare e interessato non sussistano relazioni di tipo contrattuale[145].

Il nuovo orientamento della Cassazione – che dal 2008 ad oggi ha riscritto la portata precettiva del principio di solidarietà di cui all'art. 2 Cost. in materia di risarcimento dei danni non patrimoniali, incluso quelli da illecito trattamento dei dati personali – è però approdato in tutt'altra direzione, annichilendo il senso e la funzione della solidarietà, che risulta ora piegata ad esigenze ultronee.

Non mi pare, infatti, che sia la logica della solidarietà a sorreggere le argomentazioni del citato indirizzo giurisprudenziale, bensì la *logica deflattiva del carico pendente innanzi all'autorità giudiziaria*, che è tutt'altra cosa. È in base ad essa – e non alla solidarietà – che si pretende di imporre la rinuncia a far valere (la tutela risarcitoria del danno non patrimoniale derivante dalla violazione dei) propri diritti, se modestamente lesi, ad irragionevole beneficio di chi agisce comunque illecitamente, seppur in ragione di un vantaggio nella gestione collettiva dei contenziosi[146]. Non è

motivazioni si legge che nei rapporti contrattuali il dovere di correttezza di cui all'art. 1175 c.c. deve portare a far sì che «l'ossequio alla legalità formale non si traduca in sacrificio della giustizia sostanziale e non risulti, quindi, disatteso quel dovere (inderogabile) di solidarietà, ormai costituzionalizzato (art. 2 Cost.), che, applicato ai contratti, ne determina integrativamente il contenuto o gli effetti (art. 1374 c.c.) e deve, ad un tempo, orientarne l'interpretazione (art. 1366 c.c.) e l'esecuzione (art. 1375), nel rispetto del noto principio secondo cui ciascuno dei contraenti è tenuto a salvaguardare l'interesse dell'altro, se ciò non comporti un apprezzabile sacrificio dell'interesse proprio».

[145] Sulla fattispecie di trattamento di dati personali e sui rapporti generati a fronte di essa cfr. F. Bravo, *Il "diritto" al trattamento dei dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 42 ss.; sulle obbligazioni *ex lege* in materia di protezione di dati personali si veda S. Faillace, *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di* privacy by design *e di* privacy by default, in *Contratto e impresa*, 2022, 4, p. 1123 ss.

[146] In analoga direzione, con riguardo ai problemi relativi al contenimento dei costi per la collettività, a cui non è accostabile il concetto di solidarietà di cui all'art. 2 Cost., si veda anche chi ha affermato che «Le S.U. fanno timidamente cenno al nesso con l'art. 2 Cost. ma, a prescindere da ciò, per nulla certo è che il dovere citato [di tolleranza, *n.d.a.*] costituisca realmente espressione della solidarietà imposta da detta disposizione. La sentenza in esame [Cass., sez. un., 11 novembre 2008, n. 26972, *n.d.a.*] identifica "la vittima" quale termine soggettivo di riferimento della solidarietà, avvalorando così l'idea che quest'ultima si trovi proiettata in una dimensione individualistica; ma – a ben vedere – sulla vittima, nel caso di specie, nessun effetto benefico si irradia in forza della solidarietà, essendovi qui un danneggiato che – al contrario – è costretto, suo malgrado, a sopportare il pregiudizio senza poter invocare tutela. Dunque, delle due l'una: o si ammette che la solidarietà qui invocata gioca a vantaggio dell'autore della lesione o è da rivedere l'idea che la solidarietà sia correlata alla soddisfazione di istanze particolari di protezione. E se – come pare – la sola via percorribile è la seconda, è d'uopo concludere che, qui, la solidarietà è al servizio di interessi sociali (giudicati) preminenti e risponde alla ragion pubblica che, in certe fasi critiche, rende imperativo sacrificare prerogative private sull'altare dell'economia dei costi gravanti sulla collettività. Questo, in definitiva, è il reale significato del richiamo, dalle S.U. operato, al "dovere della tolleranza che la convivenza impone (art. 2 Cost.)"». Così Grisi, *op. cit.*, par. 8, il quale, tuttavia, critica tale impostazione dell'orientamento delle Sezioni Unite per via dell'incoerenza stessa di tale accezione di solidarietà

però questo il concetto di solidarietà che l'ordinamento dovrebbe accogliere *ex* art. 2 Cost.

Che la solidarietà sia stata invocata malamente, per sorreggere un intendo deflattivo, volto ad assicurare il coinvolgimento dell'autorità giudiziaria solamente per questioni ritenute di maggior "spessore", è percepibile proprio nel testo argomentativo della sentenza da ultimo richiamata, là dove la Cassazione mette in relazione il principio di solidarietà con quello «che icasticamente viene indicato come il principio *de minimis non curat praetor* [che] guida la Corte Europea dei diritti dell'uomo nella delibazione di ricevibilità dei ricorsi, ai sensi dell'art. 35, p. 2 b), della Convenzione, alla stregua del criterio del "pregiudizio significativo", che porta a verificare, in concreto, se la violazione di un diritto abbia raggiunto "una soglia minima di gravità per giustificare l'esame da parte di una *giurisdizione internazionale*" (cosi, da ultimo, Corte EDU, sentenza Cusan e Fazzo c. Italia, n. 77/07, 7 gennaio 2014)»[147].

Nella giurisdizione nazionale, tuttavia, il legislatore ha inteso strutturare un'articolazione differenziata, governata dai criteri di competenza per valore e per materia, al fine di garantire una tutela anche alle questioni di minore gravità. La generalizzazione dell'indirizzo espresso dalla Corte europea dei diritti dell'uomo, infatti, non coglie nel segno, perché quest'ultimo non mira a negare rilevanza assoluta alle richieste di giustizia per violazione di minor gravità, ma mira a risolverle nell'ambito della giurisdizione interna agli Stati, riservando alla «*giurisdizione internazionale*» solamente i casi in cui la violazione del diritto superi la soglia minima di gravità.

L'operazione ermeneutica della Cassazione non convince affatto anche sotto un altro aspetto: la necessità di realizzare un intento deflattivo del carico pendente innanzi all'autorità giudiziaria non può passare attraverso l'utilizzo strumentale del principio normativo della solidarietà ad opera della giurisprudenza. Semmai questa potrebbe essere una linea di politica del diritto – volta a realizzare non esigenze di solidarietà, ma il contenimento del carico giudiziario – la cui adozione dovrebbe però fare ingresso nel nostro ordinamento per via legislativa (e non giurisprudenziale).

(la solidarietà-tolleranza) con il principio stesso di solidarietà di cui all'art. 2 Cost., per il quale, in ogni caso, andrebbe effettuata in via legislativa (e non giurisprudenziale) la definizione dell'ambito di operatività del dovere costituzionale di solidarietà incidente su diritti inviolabili, anch'essi costituzionalmente rilevanti, senza che il rispetto del dovere di solidarietà sociale possa tradursi nell'annichilimento del diritto inviolabile.

[147] *Ibidem*. Si legge ancora, in Cass. 16133 del 2014 cit., che «quel che più preme porre in rilievo è che alla radice delle ragioni giustificative della "soglia di risarcibilità" opera il principio di solidarietà, di cui quello di tolleranza è intrinseco precipitato, il quale, nella sua portata etica, è immanente nello stesso concetto di *societas* umana e la cui trasposizione in norma giuridica costitutiva si è avuta, nel nostro ordinamento, con l'art. 2 Cost., ponendosi esso, insieme ai diritti inviolabili, tra i valori fondanti dell'ordinamento giuridico stesso, "come base della convivenza sociale normativamente prefigurata dal Costituente" (Corte costituzionale, sentenza n. 75 del 1992). (…) Il principio di solidarietà costituisce allora il punto di mediazione che consente al sistema ordinamentale di salvaguardare il diritto del singolo nell'ambito della collettività; esso, pertanto, non giustifica in sé la necessità di un apparato di tutela dei diritti inviolabili, ma, tuttavia, ne sorregge l'effettività, rendendolo sostenibile come sistema operante all'interno di una concreta comunità di persone che deve affrontare i costi di una esistenza collettiva».

Le scelte del legislatore nazionale e di quello europeo mi pare siano però andate in direzione contraria.

Il legislatore nazionale, infatti, ha mostrato di voler accordare ai danni bagatellari, in via generale, una tutela, seppur differenziale quanto all'iter processuale per snellire il contenzioso innanzi ai giudici togati, devolvendo al giudice di pace le controversie di minor valore, riservando però alla competenza del tribunale, *ratione materiae*, diverse questioni, tra cui quelle relative alla protezione dei dati personali, in ragione della particolare natura dell'interesse protetto dall'ordinamento, con impugnazione diretta innanzi alla Corte di Cassazione[148]. È dunque illogico che in via giurisprudenziale si inseriscano criteri selettivi extralegislativi per impedire l'accesso alla tutela risarcitoria in sede giudiziale, a maggior ragione per il contenzioso in materia di protezione dei dati personali, ove la competenza del tribunale (e quella della Cassazione in sede di impugnazione) sono definiti in via legislativa *ratione materiae* a prescindere dall'entità di quanto forma oggetto della domanda[149].

Anche il legislatore europeo, come già precisato, s'è mosso in direzione inversa rispetto alle scelte di "politica del diritto" sulla gestione dei contenziosi operate dalla Cassazione in tema di risarcimento dei danni non patrimoniali: il citato art. 82 del Reg. UE 679/2016 (GDPR) ha introdotto un regime *ad hoc* per tutta l'UE sulla risarcibilità dei danni – patrimoniali e non patrimoniali – da illecito trattamento di dati personali, senza prevedere alcuna soglia selettiva. Eppure il legislatore europeo, così come quello nazionale in sede di recepimento, non hanno avuto remore, in altre materie, a introdurre criteri selettivi sulle soglie di risarcibilità, com'è avvenuto in tema di risarcimento del danno cagionato al consumatore da prodotti difettosi, con riferimento al quale è stata fissata una soglia selettiva per la definizione della rilevanza del danno a cose, che nell'art. 123, comma 2, c. cons. «è risarcibile solo nella misura che ecceda la somma di euro trecentottantasette», mentre non è prevista alcuna

[148] L'art. 152 del Codice in materia di protezione dei dati personali, infatti, riserva all'autorità giudiziaria ordinaria «le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento [Reg. UE 679/2016, n.*d.a.*] e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo regolamento (…)», richiamando espressamente l'art. 10 del d.lgs. n. 150 del 2011, che, per un verso, prevede l'applicabilità del rito del lavoro e la competenza del tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero del tribunale del luogo di residenza dell'interessato, e, per altro verso, stabilisce la non appellabilità della sentenza che definisce il giudizio, ferma restando la proponibilità del ricorso per cassazione.

[149] Acuta è a tal riguardo l'osservazione di P.G. Monateri*, op. cit.*, par. 6, ove rimarca che le Sezioni Unite della Cassazione, con l'impianto delineato con il «lungo e accorato (…) medaglione sui danni bagatellari (…), dimenticano le posizioni che la Suprema Corte assume rispetto alle liquidazioni effettuate dai giudici di pace. Proprio in un caso recente di malaugurato danno da *shock* televisivo è stata la Cassazione a dire che siccome il giudice di pace giudica secondo equità essa non può rivederne le conclusioni. Se si lascia mano libera ai giudici di pace codesto medaglione fa la figura d'una grida manzoniana». Sicché per i danni non patrimoniali di modesta entità liquidati dal giudice di pace secondo equità il filtro selettivo della Cassazione rischia di non operare, mentre per i danni non patrimoniali "bagatellari" che *ratione materiae* approdano direttamente alla magistratura togata il filtro selettivo impedisce la risarcibilità dei danni cagionata da modesta violazione dei diritti inviolabili, qual è il diritto alla protezione dei dati personali, con riferimento al quale le controversie sono devolute al tribunale ordinario.

soglia minima di risarcibilità per il danno non patrimoniale alla persona, ai sensi del comma 1, lett. *a)*, del medesimo articolo.

Anche alla luce di tali considerazioni, che assumono rilievo di carattere sistematico, possiamo certamente ribadire che i predetti criteri selettivi di matrice giurisprudenziale, individuati nella serietà del danno e nella gravità della lesione, non possono trovare ingresso nel nostro ordinamento, tanto più in tema di violazione di diritti fondamentali della persona.

Ulteriore conferma si ha dall'intersezione dell'art. 8 della Carta dei diritti fondamentali dell'UE, relativo al diritto alla protezione dei dati personali, con l'art. 52, dedicato alla portata e all'interpretazione dei diritti e dei principi: in quest'ultima disposizione normativa si trova stabilito, al par. 1, che «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà (...)».

La Cassazione, nell'indirizzo relativo ai criteri selettivi volti a negare rilevanza al risarcimento dei danni non patrimoniali da lesione di diritti inviolabili, ha disatteso sia la riserva di legge, sia la preservazione del contenuto essenziale del diritto inviolabile, nei casi in cui venga leso in maniera modesta.

Tra l'altro, la Cassazione opera evidenti forzature anche sotto il profilo metodologico, là dove usa la solidarietà come antitesi, essa stessa, del diritto fondamentale da proteggere, nella valutazione concernente il bilanciamento proporzionale dei contrapposti interessi: la Cassazione cioè finisce per individuare nella solidarietà, intesa come dovere di tolleranza verso l'illecito nei cui confronti si intende reclamare la protezione, il controvalore oggetto di bilanciamento al cui cospetto sacrificare il diritto fondamentale modestamente leso[150]. Il ragionamento, apparentemente cor-

[150] Cfr., ancora una volta, Cass., sez. III, 15 luglio 2014, n. 16133, ove, all'esito del percorso argomentativo ivi tracciato, viene sostenuto che «Conclusivamente può, quindi, essere enunciato il seguente principio di diritto: "il danno non patrimoniale risarcibile ai sensi del d.lgs. 30 giugno 2003, n. 196, art. 15, (c.d. codice della *privacy*) [ora art. 82 GDPR, *n.d.a.*] non si sottrae alla verifica di "gravità della lesione" (concernente il diritto fondamentale alla protezione dei dati personali, quale intimamente legato ai diritti ed alle libertà indicate dall'art. 2 del codice, convergenti tutti funzionalmente alla tutela piena della persona umana e della sua dignità) e di "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), che, in linea generale, si richiede in applicazione dell'art. 2059 c.c., nelle ipotesi di pregiudizio inferto ai diritti inviolabili previsti in Costituzione. Ciò in quanto, anche nella fattispecie di danno non patrimoniale di cui al citato art. 15 [ora art. 82 GDPR, *n.d.a.*], opera il bilanciamento (siccome pienamente consentito all'interprete dal modo in cui si è realizzata nello specifico l'*interpositio legislatoris*) del diritto tutelato da detta disposizione con il principio di solidarietà – di cui il principio di tolleranza è intrinseco precipitato –, il quale, nella sua immanente configurazione, costituisce il punto di mediazione che permette all'ordinamento di salvaguardare il diritto del singolo nell'ambito di una concreta comunità di persone che deve affrontare i costi di una esistenza collettiva. L'accertamento di fatto rimesso, a tal fine, al giudice del merito, in forza di previe allegazioni e di coerenti istanze istruttorie di parte, dovrà essere ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale ed al suo essere maturata in un dato contesto temporale e sociale, dovendo l'indagine, illuminata dal bilanciamento anzidetto, proiettarsi sugli aspetti contingenti dell'offesa e sulla singolarità delle perdite personali verificatesi. Un siffatto accertamento – che, ove l'offesa non superi la soglia di minima tollerabilità o il danno sia futile, può condurre anche ad escludere la possibilità di somministrare il risarcimento del danno – è come tale sottratto al sindacato di legittimità se congruamente motivato"». La Cassazione, così, finisce per assegnare alla solidarietà il significato opposto a quello che le è proprio, ossia di

retto, si rivela fallace perché non pone in contrapposizione due valori o "interessi" positivamente connotati e protetti dall'ordinamento, siano essi rilevanti sul piano individuale (ad es. un diritto fondamentale) o collettivo (ad es. un interesse generale, come potrebbe essere quello alla sicurezza pubblica o alla salute pubblica, che costituiscono comunque un vantaggio anche per l'individuo titolare del diritto di cui si chiede il sacrificio): al contrario, il ragionamento della Corte di Cassazione contrappone, nell'operazione di bilanciamento, un valore o "interesse" positivamente connotato, rilevante sul piano individuale (il diritto fondamentale alla protezione dei dati personali), con un "dovere", come tale non direttamente riconducibile nell'alveo dell'interesse individuale o generale. In altre parole il diritto fondamentale viene ad essere sacrificato non per l'esigenza di far salvo un ulteriore diritto fondamentale, né per l'esigenza di far salvo un interesse generale, di cui beneficerebbe anche il soggetto titolare del diritto sacrificato, ma viene bilanciato con una situazione giuridica soggettiva passiva, non idonea alla diretta individuazione dell'interesse oggetto di bilanciamento proporzionale, il che rende del tutto fittizia l'operazione di bilanciamento sul piano metodologico. È lo stesso art. 52, par. 1, ult. parte, della Carta dei diritti fondamentali dell'UE che precisa in maniera inequivoca che «Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

Non può neanche sostenersi che il "dovere di solidarietà", inteso quale "dovere di tolleranza", possa essere in realtà considerato nella tecnica del bilanciamento degli interessi traducendosi in un interesse generale al contenimento dei costi collettivi che deriverebbero dall'incremento dei contenziosi – o altro analogo ragionamento – perché, così facendo, non si pone il dovere di solidarietà o di tolleranza quale contropartita nell'operazione di bilanciamento, ma l'ulteriore esigenza (appunto, il contenimento dei costi collettivi). È l'esigenza ulteriore che viene in realtà a costituire l'estremo opposto da considerare nella tecnica del bilanciamento proporzionale e non il dovere di solidarietà e di tolleranza *ex se* considerati. In questo modo, però, il richiamo costituzionale operato dall'art. 2 al dovere di solidarietà porterebbe a bilanciare con le più varie esigenze, indefinite sia a livello costituzionale che a livello di legge ordinaria, il diritto fondamentale che si pretende di comprimere. Cioè, il principio di solidarietà-tolleranza, così inteso, finirebbe per essere il "cavallo di Troia" utilizzato per permettere l'ingresso di qualsivoglia esigenza, nell'operazione tecnica di bilanciamento di interessi costituzionalmente rilevanti, anche qualora tale esigenza non abbia in realtà un'effettiva copertura costituzionale, né sia stata determinata dal legislatore. Per poter limitare proporzionalmente il diritto fondamentale (così come la tutela risarcitoria in caso di sua lesione) occorre però che l'esigenza da far valere nell'operazione di bilanciamento, come precisato anche nell'art. 52 cit., sia individuata *ex lege* e che non porti a sacrificare il contenuto essenziale del diritto sottoposto ad operazione di bilanciamento. In ogni caso non è il "dovere" in sé ad

cura "fraterna" (o "solidale") dell'altrui interesse, meritevole di protezione secondo l'ordinamento giuridico.

essere oggetto dell'operazione di bilanciamento, ma, semmai, l'interesse ulteriore, positivamente determinato, che a quel dovere è riconducibile.

Ma v'è di più. S'è già rimarcato che il principio di solidarietà-tolleranza, affermato dalle Sezioni Unite, colloca la solidarietà in un'accezione assai diversa rispetto a quella, tipica, che impone di tutelare gli interessi del soggetto con cui socialmente ci si relaziona: l'annotazione, però, assume rilevanza non solo sul piano del "*contenuto*" da assegnare al principio normativo di solidarietà, ma anche sul piano "*funzionale*", soprattutto con riguardo alle fattispecie in tema di trattamento di dati personali.

La prospettiva funzionale consente di individuare altre aporie nel ragionamento portato avanti dalla Cassazione in tema di irrisarcibilità di quei danni non patrimoniali che risultino incapaci di superare i filtri selettivi individuati in via giurisprudenziale in base al principio di solidarietà-tolleranza: sembra si faccia un'applicazione "stravagante" del principio normativo di solidarietà *ex* art. 2 Cost., a tal punto da imporre un sacrificio di un diritto fondamentale, ancorché modestamente leso, a vantaggio di un soggetto che non vanta un'analoga contrapposta pretesa giuridica, ma che, al contrario, ha compiuto un illecito e che, pertanto, avrebbe un dovere di protezione e di riparazione. Non siamo dunque nell'ottica del bilanciamento tra posizioni giuridiche soggettive di pari rango. Anzi, il soggetto autore dell'illecito trattamento dei dati personali (il titolare del trattamento) sarebbe tenuto – proprio in applicazione del principio di solidarietà – ad attivarsi per tutelare gli interessi della vittima (il *data subject*, a cui i dati personali si riferiscono). Paradossalmente, invece, il ragionamento portato innanzi dalla Cassazione, là dove reclama l'applicazione del principio di solidarietà imponendo la tolleranza dell'illecito di modesta entità o connotato da condotte illecite socialmente tollerabili, impone di favorire (in base ad un preteso senso di solidarietà) la posizione di chi rifiuta la cura solidale degli interessi altrui, ancorché afferenti ai diritti fondamentali.

Si snatura così il senso e la funzione della solidarietà.

Va altresì tenuto presente che nei rapporti socio-economici, le violazioni di lieve entità, di cui si impone l'accettazione supina, possono essere sistematicamente perpetrate in contesti imprenditoriali legati alla fornitura di servizi (soprattutto telematici), portando a generare cospicui vantaggi, anche di carattere economico, per il titolare del trattamento che sia autore di illeciti "bagatellari" sistematicamente reiterati. Il problema si pone in maniera prorompente nel settore del trattamento dei dati di fronte al fenomeno dei *big data*, che costituiscono oggetto di rilevanti operazioni di commercializzazione, nonché di fronte ai servizi telematici forniti su larga scala, basati sull'utilizzo in ambito economico dei dati. L'indirizzo giurisprudenziale sostenuto dalla Suprema Corte finirebbe per ritagliare sacche di impunità, a fronte della sostenuta irrilevanza di trattamenti illeciti di dati personali, considerati di lieve entità o percepiti socialmente come non gravosi se considerati nella relazione micro-economica, ma di grande impatto nella prospettiva macro-economica, proprio perché commessi su larga scala.

Mi pare tuttavia necessario riconsegnare la solidarietà alla dimensione della cura dell'interesse altrui, evitando invece di impregnarla con il concetto di "tolleranza" verso altrui condotte illecite – ancorché modeste, se apprezzate individualmente secondo logiche "micro-economiche" –, le quali esigerebbero una ben diversa

considerazione, essendo portatrici in sé di un disvalore che l'ordinamento dovrebbe scoraggiare o impedire e che va colto anche in considerazione delle logiche "macroeconomiche", a cui s'è appena fatto riferimento o, se si vuole, in relazione al loro impatto sociale, sulla collettività.

In altre parole, mutuando il linguaggio dal diritto delle obbligazioni, la solidarietà non va tradotta nel dovere di "tolleranza" benevola del creditore (interessato) verso comportamenti illeciti del debitore (titolare del trattamento), ancorché di modesta rilevanza, ma, semmai, nel dovere del debitore (titolare del trattamento) di attivarsi per la protezione degli interessi meritevoli di tutela del creditore (interessato) e, tutt'al più, nell'obbligo di cooperazione del creditore medesimo affinché il debitore possa realizzare appieno il comportamento dovuto in ossequio all'obbligazione assunta volontariamente o *ex lege*. Mi pare invece che la Cassazione, nell'insistere sulla dimensione del dovere di solidarietà *ex* art. 2 Cost., inteso quale dovere di tolleranza verso le altrui condotte illecite, finisca per tradire il senso della disposizione costituzionale e la sua stessa *ratio*, che va colta ricollocandola all'interno di una corretta cornice valoriale di riferimento, che non si traduca nella «tirannia dei valori» di Schmittiana memoria, ma si raccordi alla funzione ultima del diritto, quale sistema improntato all'ordinata convivenza sociale.

Come magistralmente rimarcato da Francesco Galgano, «Secondo la generale (...) funzione del diritto, che è la soluzione non violenta dei conflitti fra gli uomini, ogni norma giuridica dispone in ordine ad un possibile conflitto di interessi. Essa stabilisce quale fra gli interessi in conflitto sia degno di protezione e debba prevalere e quale, invece, non sia degno di protezione e debba soccombere: prescrive obblighi o divieti per impedire la realizzazione di interessi valutati come non degni di tutela e per consentire la realizzazione di interessi valutati come degni di tutela»[151].

Ebbene, sotto tale profilo, l'orientamento della Cassazione va ridiscusso in relazione alla funzione del diritto, che reclama di vedere quale sia l'interesse meritevole di protezione e quale invece il confliggente interesse destino a soccombere. In tali logiche, di carattere funzionale, la scelta nomofilattica delle Sezioni Unite lascia aperto un interrogativo a cui l'interprete non può sottrarsi: perché si pretende il dovere di "solidarietà-tolleranza" a carico del danneggiato e non si pretende, invece, il dovere di "solidarietà-fratellanza" (ovvero, il dovere di "solidarietà-correttezza", che implica il dovere di protezione per la cura dell'altrui interesse) a carico del danneggiante?

Nella specifica materia qui in esame, si noti, gli obblighi di protezione sono scolpiti nel dettato normativo di matrice europea – con riferimento tanto all'art. 8 della Carta dei diritti fondamentali dell'UE, che ha esplicitato il diritto alla protezione dei dati personali, quanto al Reg. UE 679/2016 –, così come in quella internazionale (Convenzione 108+ e art. 8 CEDU). Non si tratta, dunque, di un percorso interpretativo rivolto all'applicazione della controversa categoria degli "obblighi di protezione", che *in subiecta materia* sono invero già specificamente disciplinati *ex*

[151] F. Galgano, *Trattato di diritto civile*, Milano, 2014, vol. I, 3ª ed. aggiornata a cura di N. Zorzi Galgano, p. 24. Si veda anche, *ivi*, p. 3.

lege[152]. Si tratta, invece, di rimanere entro una più soddisfacente interpretazione costituzionalmente orientata del principio di solidarietà sociale di cui all'art. 2 Cost., di cui il principio di correttezza – previsto espressamente anche nell'art. 5, par. 1, lett. *a)*, del GDPR –, costituisce la sua più significativa espressione.

3.4. La sentenza della Corte di giustizia dell'UE del 4 maggio 2023 (C-300/21) sull'inammissibilità di soglie minime di risarcibilità del danno non patrimoniale relative alla gravità del danno (ed alla serietà della lesione) in materia di protezione dei dati personali e il parziale *revirement* della Corte di Cassazione

La questione è stata più recentemente affrontata anche dalla Corte di giustizia dell'UE con sent. 4 maggio 2023, resa nella causa C-300/21, con la quale, in riferimento all'art. 82 GDPR, ha avuto modo di chiarire diversi aspetti controversi in materia di risarcimento del danno da illecito trattamento di dati personali.

Dapprima ha ribadito che tale danno non può ritenersi *in re ipsa*, quale automatica conseguenza della violazione di una norma del Reg. UE 679/2016, ma di esso occorre sempre fornire adeguata prova, sicché «la mera violazione delle disposizioni di tale regolamento non è sufficiente per conferire un diritto al risarcimento»[153]. Ciò esclude, dunque, la possibilità di ricondurre l'art. 82 GDPR ad un regime di responsabilità civile per il quale vi sia prevista *ex lege* la possibilità di liquidazione di danni punitivi, come invece proposto da parte della dottrina[154].

La Corte ha poi precisato che la liquidazione del danno, con il concorso delle norme dell'ordinamento nazionale, va effettuata secondo criteri di effettività e di equivalenza[155], il che esclude, ancora una volta, la possibilità di danni punitivi con riferimento alla liquidazione dei danni da illecito trattamento di dati personali. L'applicazione delle norme del diritto interno, sulla determinazione dell'entità del risar-

[152] Sulle *obbligazioni ex lege* nella disciplina in materia di protezione di dati personali cfr. F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 776 ss.; nonché S. FAILLACE, *op. cit.*, p. 1123 ss.

[153] CGUE, sent. 4 maggio 2023, causa C-300/21 (n. 1 del dispositivo). La Corte ha precisato che la violazione del regolamento è una condizione necessaria ma non sufficiente ai fini del conseguimento del diritto al risarcimento del danno da illecito trattamento di dati personali, occorrendo anche, quali ulteriori condizioni, l'esistenza stessa del danno, che deve essere oggetto di autonoma considerazione (anche sul piano probatorio) e, da ultimo, l'esistenza del «nesso di causalità tra tale trattamento illecito e tale danno».

[154] V., ad es., E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo*, in *Contratto e impresa*, 2020, 3, pp. 1115 ss., il quale ha ritenuto ammissibile, in tale materia, la risarcibilità del danno *in re ipsa*, con funzione sanzionatoria, in applicazione dell'indirizzo giurisprudenziale ribadito in Cass. civ., sez. III, 11 novembre 2019, n. 28989.

[155] CGUE, sent. 4 maggio 2023, causa C-300/21, n. 3 del dispositivo, ove si afferma che «ai fini della determinazione dell'importo del risarcimento dovuto in base al diritto al risarcimento sancito da tale articolo [82 GDPR, *n.d.a.*], i giudici nazionali devono applicare le norme interne di ciascuno Stato membro relative all'entità del risarcimento pecuniario, purché siano rispettati i principi di equivalenza e di effettività del diritto dell'Unione.

cimento, deve dunque rispettare siffatti criteri e «A tal riguardo, tenuto conto della funzione compensativa del diritto al risarcimento previsto all'art. 82 GDPR (…), un risarcimento pecuniario fondato su tale disposizione deve essere considerato "pieno ed effettivo" se consente di compensare integralmente il danno concretamente subito a causa della violazione di tale regolamento, senza che sia necessario, ai fini di una siffatta compensazione integrale, imporre il versamento di un risarcimento punitivo»[156].

La Corte di giustizia si pronuncia, inoltre, anche ai filtri selettivi relative alla gravità del danno subito, affermando che l'art. 82 GDPR è incompatibile con la previsione, nel diritto nazionale, di soglie minime di risarcibilità del danno non patrimoniale derivante dal trattamento illecito di dati personali. Più esplicitamente, la Corte di giustizia, nella sentenza cit., ha stabilito che «L'art. 82, par. 1, del Reg. 2016/679 deve essere interpretato nel senso che esso osta a una norma o a una prassi nazionale che subordina il risarcimento di un danno immateriale, ai sensi di tale disposizione, alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità».

La questione era sorta nell'ordinamento austriaco, che contiene una norma che esclude espressamente la risarcibilità dei danni immateriali qualora non superino una certa soglia di gravità: il che aveva indotto l'*Oberlandesgericht Wien* (Tribunale superiore del Land, Vienna, Austria) a confermare la sentenza di primo grado con cui era stata negata risarcibilità ai sentimenti negativi patiti dell'interessato avverso il trattamento dei dati personali con cui gli era stata attribuita un'affinità con un determinato partito politico[157].

Si noti che, disattendendo le conclusioni dell'avvocato generale, la Corte di giustizia ha ritenuto incompatibile con l'ordinamento europeo non solo, come nel caso austriaco, una «norma» di diritto interno volta ad escludere espressamente la

[156] CGUE, sent. 4 maggio 2023, causa C-300/21, par. 58.

[157] Come si legge nei parr. 11 ss. della cit. sent. 4 maggio 2023 della CGUE, causa C-300/21, «A partire dal 2017, la Österreichische Post, società di diritto austriaco che pratica la vendita di indirizzi, ha raccolto informazioni sulle affinità politiche della popolazione austriaca. Con l'ausilio di un algoritmo che tiene conto di diversi criteri sociali e demografici, essa ha definito "indirizzi di gruppi destinatari". I dati così generati sono stati venduti a diverse organizzazioni per consentire loro di effettuare invii pubblicitari mirati.
Nell'ambito della sua attività, la Österreichische Post ha trattato dati che, per estrapolazione statistica, l'hanno indotta a dedurre un'elevata affinità del ricorrente nel procedimento principale con un determinato partito politico austriaco. Tali elementi non sono stati trasmessi a terzi, ma il ricorrente nel procedimento principale, che non aveva acconsentito al trattamento dei suoi dati personali, si è sentito offeso dal fatto che gli era stata attribuita un'affinità con il partito in questione. La circostanza che, all'interno di tale società, siano stati conservati dati relativi alle sue presunte opinioni politiche avrebbe suscitato in lui una grave contrarietà, una perdita di fiducia, nonché un sentimento di umiliazione. Dalla decisione di rinvio risulta che non è stato accertato alcun danno diverso da tali afflizioni di carattere temporaneo e di ordine emotivo». Di fronte alla richiesta inibitoria della condotta illecita e risarcitoria del danno subito, quantificato in euro 1.000, il giudice di prime cure e quello di appello hanno ritenuto di accogliere la prima richiesta e di rigettare la seconda, applicando la norma del diritto austriaco secondo cui la risarcibilità del danno non patrimoniale è da escludere ove non raggiunga una certa «soglia di gravità». Il caso giungeva innanzi alla Suprema Corte austriaca (l'*Oberster Gerichtshof*), che ha ritenuto di investire la Corte di giustizia.

risarcibilità dei danni immateriali qualora non superino una certa «soglia di gravità», ma una «prassi» adottata in sede «applicativa» che, come nell'esperienza italiana, mira a raggiungere tale risultato. In altre parole, non sono conformi al Reg. UE 679/2016 i filtri selettivi volti a precludere il risarcimento del danno non patrimoniale perché ritenuto non grave.

Com'è noto, le sentenze interpretative della Corte di giustizia hanno efficacia *erga omnes* in tutta l'UE, sicché la pronuncia è destinata a mutare radicalmente l'indirizzo giurisprudenziale difforme assestatosi in alcuni Paesi membri, come l'Austria e l'Italia e, segnatamente, la prassi applicativa nostrana con cui, invocando (malamente) il principio di solidarietà, è stata negata dignità risarcitoria ai danni non patrimoniali di lieve entità.

La vincolatività della pronuncia interpretativa della Corte di giustizia dell'UE, dunque, ha ridelineato la portata applicativa del "principio di solidarietà" in materia di risarcimento del danno non patrimoniale derivante da illecito trattamento di dati personali e, di conseguenza, a tutte le ulteriori ipotesi di risarcimento del danno non patrimoniale, precludendo che possa essere inteso nel senso di imporre il sacrificio della vittima di fronte a danni immateriali accertati, ma ritenuti modesti nella loro consistenza.

Gli effetti della citata sent. 4 maggio 2023 della CGUE hanno iniziato a manifestarsi negli orientamenti della nostra S.C., come avvenuto con Cass. civ., sez. I, ord. 12 maggio 2023, n. 13704, in cui – a distanza di solamente otto giorni dalla sentenza della Corte di giustizia – viene rivista solo parzialmente l'argomentazione sui filtri selettivi ai fini del risarcimento del danno non patrimoniale, con un risultato segnato però da una certa contraddittorietà.

Per un verso, infatti, In un passaggio delle motivazioni di tale sentenza, la Corte di Cassazione non rinuncia ad affermare che, a fronte dell'adeguamento del nostro ordinamento alle norme del GDPR, «il diritto al risarcimento non si sottrae alla verifica della gravità della lesione e della serietà del danno. Questo perché anche per tale diritto opera il bilanciamento con il principio di solidarietà ex Cost, art. 2, di cui quello di tolleranza della lezione minima è un precipitato».

Tuttavia ora la Corte ammette la risarcibilità anche dei danni bagatellari, ricordando che, ai sensi dell'art. 82 Reg. UE 679/2016, «il soggetto danneggiato a seguito di un trattamento dei suoi dati in violazione delle norme del GDPR e di quelle nazionale di recepimento (cfr. il D.Lgs. n. 101 del 2018 di aggiornamento del codice privacy) può ottenere il *risarcimento di qualunque danno* occorsogli, *anche se la lesione sia marginale*». Al contempo però, argomentando sul requisito di effettività del danno, e ricordando che esso non può considerarsi sussistente il *re ipsa*, ribadisce comunque la necessità che sia fornita «la prova della *serietà della lesione* conseguente al trattamento», precisando che «ciò vuol dire che può non determinare il danno la mera violazione delle prescrizioni formali in tema di trattamento del dato, mentre induce sempre al risarcimento quella violazione che *concretamente offenda la portata effettiva del diritto* alla riservatezza».

La prova della *serietà della lesione*, dunque, sembra coincidere – nell'interpretazione della S.C. – con la prova dell'esistenza stessa di un danno *effettivo*, in difetto della quale il risarcimento verrebbe negato dalla prassi applicativa della S.C.,

nel nostro ordinamento[158]. La dimostrazione della *serietà* della lesione, tuttavia, non può portare ad escludere *tout court* la risarcibilità del danno *marginale* (o bagatellare), perché si avrebbe altrimenti una prassi applicativa, nel nostro diritto interno, contrastante con la richiamata pronuncia della Corte di giustizia, che àncora il requisito di *effettività* al risarcimento, più che al danno. In altre parole, qualora venga provata l'esistenza di un danno da illecito trattamento di dati personali, anche di modesta entità, occorre che l'ordinamento nazionale assicuri un risarcimento «pieno ed effettivo», anche al cospetto di danni marginali, a fronte dei quali non può essere negato il diritto al risarcimento. La Corte europea, nella sent. cit., par. 58, evidenzia infatti che il «*risarcimento* (…) deve essere considerato "pieno ed *effettivo*" se consente di compensare integralmente il danno concretamente subito a causa della violazione» delle norme in materia di protezione dei dati personali. L'indagine sul grado di serietà e gravità della lesione e del danno vanno apprezzate, dunque, non sul piano dell'*an* del risarcimento, ma sul piano del *quantum*. L'*an* invece è conseguente alla valutazione positiva dell'onere probatorio concerne l'esistenza del danno da illecito trattamento dei dati personali, in ordine alla quale non può essere chiamato in causa il principio di "solidarietà-tolleranza".

[158] Nel caso di specie, culminato con ord. 13073/2023, cit., resa dalla Sez. I della C. Cass., è stata confermata la condanna al risarcimento del danno da illecito trattamento di dati personali prevista dal giudice del merito. La richiesta risarcitoria era stata avanzata da una dipendente di un Comune dopo che quest'ultimo aveva pubblicato sul proprio sito istituzionale una propria determina relativa al pignoramento del quinto dello stipendio della predetta dipendente a favore della società creditrice pignorante. Nella determina era stata omessa la pubblicazione dei dati della dipendente-debitrice, che rimanevano comunque apprensibili dalla nota contabile ad essa allegata, seppur per poco più di un giorno, nell'albo pretorio *online* del Comune. Il danno subito è stato ritenuto conseguente all'ostensione di tali dati in violazione dei principi di necessità e minimizzazione previsti dal GDPR.

Finito di stampare anno 2023
presso le Industrie Grafiche della Pacini Editore S.r.l.
Via A. Gherardesca • 56121 Pisa
Tel. 050 313011 • Fax 050 3130300
www.pacinieditore.it

€ 70,00