Information Technology Law 03

Series Editors Fabio Bravo *and* Angelo Giuseppe Orofino

Tutela e valorizzazione dei dati nei mercati digitali

Il contratto, la concorrenza e i nuovi soggetti tutelati

Giuseppe Proietti

Wolters Kluwer

INFORMATION TECHNOLOGY LAW

The volumes published in this Series
have been subject to a double-blind peer review procedure

Information Technology Law 03

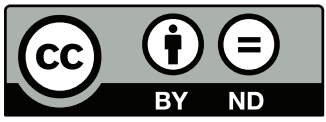
Series Editors Fabio Bravo *and* Angelo Giuseppe Orofino

Tutela e valorizzazione dei dati nei mercati digitali

Il contratto, la concorrenza e i nuovi soggetti tutelati

Giuseppe Proietti

Wolters Kluwer



Printed by
GECA - Divisione Libri di CISCRA S.p.A., Via Belvedere, 42 - 20862 Arcore (MB)

INDICE SOMMARIO

Introduzione e obiettivi XI

CAPITOLO I

LA CIRCOLAZIONE DEI DATI NEI MERCATI DIGITALI EUROPEI

1. Premessa 2
2. «Privacy»: riservatezza e trattamento dei dati personali 7
3. La definizione di dato personale 10
4. La concezione di dato personale nella recente giurisprudenza europea 12
5. I principi di *accountability*, privacy *by default* e *by design* nel Regolamento generale sulla protezione dei dati (Reg. UE 2016/679 – GDPR) 16
6. I principi di limitazione delle finalità, proporzionalità, minimizzazione, esattezza e trasparenza nel trattamento dei dati personali nel GDPR 19
7. Il diritto alla portabilità dei dati personali ai sensi dell'art. 20 GDPR 24
8. Le basi giuridiche per il trattamento dei dati personali 28
9. La base giuridica del consenso (art. 6, par. 1, lett. a, GDPR) 29
10. La prima teoria sul consenso: la visione negoziale 31
11. La seconda teoria sul consenso: la visione autorizzatoria 32
12. Il consenso in senso unitario o duale 33
13. La base giuridica del legittimo interesse (art. 6, par. 1, lett. f, GDPR) 36
14. Ancora sulla base giuridica del legittimo interesse del titolare del trattamento (o di un terzo). Le recenti linee guida dell'EDPB 42
15. L'applicazione del legittimo interesse nel contesto del *marketing* diretto (secondo le linee guida EDPB) 50
16. Il legittimo interesse nella recente decisione IAB Europe (CGUE - C-604/2022) 54

17. La teoria patrimonialistica e personalistica sul trattamento dei dati personali 56
18. Il trattamento dei dati come condizione necessaria per accedere al servizio digitale: le operazioni di *tying* 64
19. Le prescrizioni concernenti i contratti di fornitura di contenuto digitale o dei servizi digitali tra operatori economici e consumatori (la direttiva UE 2019/770) 69
20. L'utilizzo secondario dei dati personali e il principio di limitazione della finalità del trattamento 76
21. Le operazioni di «profilazione» dell'utente e il processo decisionale automatizzato (art. 22 GDPR) 79
22. Il fenomeno del *Black Box* e l'impatto sul principio di trasparenza 84

CAPITOLO II

LA CIRCOLAZIONE DEI DATI PERSONALI VERSO STATI TERZI

1. Il quadro giuridico europeo in materia di trasferimento dei dati personali verso Stati terzi o organizzazioni internazionali 89
2. La nozione di «trasferimento» dei dati personali 94
3. Il *Privacy Shield* e il trasferimento dei dati personali verso gli Stati Uniti d'America 96
4. I principi europei alla base della sentenza della Corte di Giustizia *Schrems II* 99
5. I criteri di valutazione previsti dall'art. 46 del GDPR e il ruolo delle Autorità di controllo secondo la sentenza *Schrems* II 101
6. Conseguenze pratiche dopo la sentenza *Schrems* II 103
7. La fase transitoria dopo la sentenza *Schrems* II per i trasferimenti dei dati personali verso gli Stati Uniti d'America 106
8. Il nuovo quadro giuridico con il *Trans-Atlantic Data Privacy Framework* (DPF) 109
   8.1 I poteri delle agenzie di *intelligence* secondo il nuovo accordo 112
   8.2 La supervisione delle attività di *intelligence* 113
9. Il parere dell'EDPB sul *Trans-Atlantic Data Privacy Framework* 114
10. Il Report dell'EDPB sulla prima revisione della Commissione europea sul *Data Privacy Framework* 117
11. Le conseguenze derivanti dal *Trans-Atlantic Data Privacy Framework* 118
12. Il trasferimento dei dati personali verso il Regno Unito dopo Brexit 126

13. Le altre basi giuridiche previste dal GDPR per i trasferimenti all'estero: la deroga dell'art. 49, lett. a), GDPR 132
14. Le norme vincolanti d'impresa (*Binding Corporate Rules*) 134
15. Le *standard contractual clauses* (SCC) 137
16. Trasferimenti o comunicazioni non autorizzati dal diritto dell'Unione (art. 48 GDPR) 141
17. Trasferimento e accesso internazionale ai dati ai sensi del *Data Governance Act* e *del Data Act* 142

Capitolo III

LA PROTEZIONE DEI DATI E IL DIRITTO DELLA CONCORRENZA NEI MERCATI DIGITALI

1. I risvolti anticoncorrenziali della circolazione dei dati personali nei mercati digitali 145
2. I *big data* plasmano i mercati 150
3. I "nuovi" poteri privati nei mercati digitali 153
4. L'abuso di posizione dominante (art. 3 L. n. 287/1990 - art. 102 TFUE) 157
   4.1 Abusi di sfruttamento e abusi escludenti 166
   4.2 La pratica dei prezzi dinamici o personalizzati 170
   4.3 I potenziali e nuovi orizzonti delle pratiche di *self-preferencing* per il tramite degli assistenti vocali 173
5. Il trattamento dei dati personali e la sua rilevanza antitrust 174
6. L'intervento chiarificatore della Corte di Giustizia europea sul collegamento tra normativa antitrust e normativa in materia di dati personali: la sentenza CGUE C-252/21 180
7. Il recente caso Apple sull'adozione di politiche di privacy differenziate 183
8. Il caso Google - Weople sulla portabilità dei dati personali 186
9. Il caso del *Norwegian Consumer Council* 190

Capitolo IV

IL NUOVO QUADRO REGOLATORIO EUROPEO IN TEMA DI MERCATI DIGITALI E LA VALORIZZAZIONE DEI DATI

1. Il regolamento europeo *Platform-to-Business* (P2B - Reg. UE 2019/1150) e gli altri interventi normativi che regolano i mercati digitali 198
2. Il *Digital Markets Act* (DMA - Reg. UE 2022/1925) 200

3. Il *ne bis in idem*. La necessità di coordinare la disciplina antitrust tradizionale e il DMA 204
4. I *gatekeeper* secondo il *Digital Markets Act* 206
5. Le pratiche sleali o limitative della contendibilità (artt. 5 - 7 DMA): gli obblighi e i divieti 209
6. I poteri della Commissione europea 215
7. I primi casi applicativi del DMA 217
8. Il *Digital Services Act* (DSA – Reg. UE 2022/2065) 219
9. Scopo e applicazione del *Digital Services Act* 222
10. Il quadro di esenzione da responsabilità dei prestatori di servizi intermediari 225
11. Gli obblighi per i prestatori di servizi intermediari nel DSA 229
11.1 Obblighi applicabili a tutti i prestatori 230
11.2 Obblighi applicabili ai prestatori di servizi di memorizzazione di informazioni 231
11.3 I poteri dei fornitori di piattaforme online e i relativi obblighi 232
11.4 Obblighi supplementari per i fornitori di piattaforme online (VLOP) e di motori di ricerca online di dimensioni molto grandi (VLOSE) 235
12. I primi casi applicativi del DSA 239
13. La nuova figura di «utente commerciale» e di «operatore commerciale» nei mercati digitali 243
14. La creazione dei servizi di intermediazione nella strategia europea per i dati con il *Data Governance Act* (DGA – Reg. UE 2022/868) 246
15. La circolazione dei dati nel sistema dell'*Internet of Things* con il *Data Act* (Reg. UE 2023/2854) 250

CAPITOLO V

LE NUOVE SFIDE NEL CONTESTO NORMATIVO DEI MERCATI DIGITALI

1. Il dedalo normativo nel settore dei mercati digitali. La (già) impellente necessità di delineare un quadro sistematico 257
2. La ricostruzione del dibattito sull'incidenza della normativa privacy nelle dinamiche antitrust 260
3. Il consenso al trattamento dei dati per l'erogazione del servizio o prodotto digitale «gratuito» in sostituzione del «corrispettivo» 262
4. Gli elementi di una (complessa) indagine antitrust per i servizi o prodotti digitali: la valutazione del mercato rilevante nel

«mercato a due versanti» richiede un approccio differente rispetto ai mercati tradizionali 265
5. La perdurante centralità del consenso che non produce un trasferimento di un diritto dominicale in favore del titolare del trattamento 270
6. Il dibattito sul *pay or consent* 273
7. Gli standard del trattamento dei dati personali come parametro per la qualità del prodotto digitale a tutela di una libera scelta dell'utente consapevole 274
8. Il nuovo quadro normativo europeo dei dati e dei mercati digitali introduce novità e consolida fattispecie previgenti 279
9. L'utilizzo dell'algoritmo nel trattamento dei dati personali. Il caso *Mevaluate* 282
9.1 Il caso "Schufa" (CGUE C-634/21). Ancora sullo *scoring* algoritmico, anche alla luce del regolamento europeo sull'intelligenza artificiale 284
9.2 Il diritto di accesso ai dati personali e la nozione di informazioni significative sulla "logica utilizzata" nell'ambito di un processo decisionale automatizzato. Il caso "Dun & Bradstreet" (CGUE C-203/2022) 289

Bibliografia 295

Introduzione e obiettivi

Gli ultimi tre lustri si sono caratterizzati per l'affermazione di un'economia digitale sempre più pervasiva ed emersa grazie al dirompente sviluppo della tecnica. Si è presto passati a un'economia digitale che fa il paio con una economia dei dati in considerazione del ruolo sempre più pregnante dei dati nel funzionamento dei sistemi tecnologici più o meno "intelligenti". Tutto questo ha avuto inevitabili effetti sia nei confronti dei singoli, intesi come consumatori o utenti, sia nei confronti della collettività, intesa anche in termini di "mercato".

Il presente lavoro si fonda su un approccio giuridico non solo dogmatico-ricostruttivo, ma con una prospettiva critica e sistematica. Il metodo adottato mira, da un lato, a ricostruire in maniera organica il complesso quadro normativo europeo e nazionale in materia di dati e mercati digitali, attraverso l'analisi delle principali fonti primarie che lo riguardano (regolamenti, direttive, legislazione interna); dall'altro, a esaminare i nodi interpretativi e applicativi emersi in dottrina e giurisprudenza. L'indagine si avvale inoltre di un approccio comparatistico e interdisciplinare che mette in relazione le discipline della protezione dei dati personali, della concorrenza e del diritto contrattuale, al fine di evidenziare le tensioni sistemiche e proporre chiavi interpretative idonee a valorizzare i dati in un'ottica di equilibrio tra la tutela dei diritti fondamentali e le dinamiche di mercato.

Invero, le evoluzioni della tecnica hanno richiamato l'attenzione di economisti, di giuristi e del legislatore. Quest'ultimo, in specie quello europeo, negli ultimi anni si è dimostrato particolarmente produttivo adottando una serie di direttive e regolamenti che incidono sui settori della tecnologia, dei dati personali, dei consumatori e della concorren-

za, risaltando la necessità di un coordinamento tra questi settori, sempre più connessi, e mettendo a dura prova la certezza del diritto e le abilità ermeneutiche dei giuristi.

Basti pensare, infatti, agli atti legislativi più recenti, al di là dell'ovvio riferimento al GDPR (*General Data Protection Regulation*) che conserva ancora un ruolo centrale in materia, ossia:

il regolamento *Platform-to-Business* (Regolamento UE 2019/1150); la direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale (direttiva UE 2019/790); il *Data Governance Act* (Regolamento UE 2022/868); il *Data Act* (Regolamento UE 2023/2854); il *Digital Markets Act* (Regolamento UE 2022/1925); il *Digital Services Act* (Regolamento UE 2022/2065); la direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (direttiva UE 2019/770); la direttiva relativa a determinati aspetti dei contratti di vendita di beni (direttiva UE 2019/771); la direttiva *Open Data* (direttiva UE 2019/1024); la direttiva per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori (direttiva UE 2019/2161); il Regolamento sull'intelligenza artificiale (*Artificial Intelligence Act,* Regolamento UE 2024/1689); la nuova direttiva sulla responsabilità per danno da prodotti difettosi (direttiva UE 2024/2853).

Ebbene, l'obiettivo che si tenta di perseguire con questo scritto è di inquadrare gli aspetti normativi dei mercati digitali in virtù di quegli sviluppi sopra descritti per sommi capi. Infatti, ciò che si va a formare in questi anni è un vero e proprio diritto digitale, inteso come materia di carattere culturale.

In particolare, gli sforzi si incentrano sull'analisi dell'impianto giuridico, sempre più connesso e interdipendente, inerente alla normativa in materia di dati personali e alle sue dinamiche concorrenziali. L'illecito antitrust su cui ci si focalizza è l'abuso di posizione dominante, fino ad arrivare all'analisi della più recente normativa europea che disciplina *ex ante* le vicende dei mercati digitali.

Perciò, partendo dall'analisi della normativa in materia di protezione dei dati personali, ci si concentra non solo sulla tutela, ma anche sulla funzione circolatoria dei dati personali nell'ambito dei mercati di-

gitali europei; ciò viene effettuato partendo da necessarie premesse che consentono di chiarire gli elementi di base come la differenza con il concetto di riservatezza, passando per l'analisi dei principi e degli elementi fondamentali dettati dal GDPR, senza trascurare i più rilevanti interventi giurisprudenziali in materia. L'analisi coinvolge, in modo particolare, la base giuridica dell'interesse legittimo e il meccanismo del *pay or consent*.

La funzione circolatoria dei dati personali, nel suo complesso, non può essere compresa se non si considera – in un sistema globale iperconnesso – anche la circolazione dei dati verso Stati terzi rispetto ai confini dello spazio economico europeo. Per questo, è necessario dedicarsi anche alla disciplina dei trasferimenti dei dati personali oltre i confini dello spazio economico europeo, ponendo l'accento sulle vicende che negli ultimi anni hanno riguardato l'Unione europea e gli Stati Uniti d'America, anche per il fatto che le principali *big tech*, le cc.dd. GAFAM[1], hanno la propria sede (principale) negli U.S.A. Un altro Stato che, per note vicende geopolitiche, si è guadagnato un'attenzione particolare, anche in tema di dati personali, è il Regno Unito.

Il tema dei mercati digitali, che si lega a doppio filo con questioni inerenti ai dati personali, interessa varie questioni e solo alcune di esse verranno esaminate nei cinque capitoli che compongono lo scritto. Ci si concentrerà infatti su quei temi in cui i mercati digitali hanno già dato vita a sfide pregnanti come il settore della concorrenza, alcuni aspetti relativi al settore contrattuale, così come temi strettamente attinenti al trattamento dei dati (si pensi al trattamento automatizzato) e ai nuovi soggetti giuridici che reclamano una nuova forma di tutela dovuta ai mutamenti delle dinamiche dei mercati provocati dalla tecnica (gli utenti commerciali).

Il quarto capitolo è dedicato a un'altra parte della recente normativa europea che, benché abbia trovato una esigua e concreta applicazione, ha già creato malcontenti in seno a grandi imprese che hanno

[1] Acronimo che indica le principali aziende tecnologiche (occidentali): Google, Apple, Facebook, Amazon e Microsoft.

adito le autorità giurisdizionali europee. Dunque, l'analisi normativa riguarda, oltre al regolamento *Platform-to-Business* (P2B), la disciplina regolatoria del *Digital Markets Act,* del *Digital Services Act* del *Data Governace Act* e del *Data Act*. Queste costituiscono normative con un impianto regolamentare incentrato sui mercati digitali che si presentano in gran parte complementari, seppur con ambiti e scopi, per altra parte, differenti. L'intero e articolato quadro, quindi, si conclude con riflessioni di natura contrattuale - anche in virtù della fallace gratuità che viene spesso richiamata nel settore digitale - e di revisione del profilo concorrenziale in un'ottica di mercati a due versanti oltre a una armonizzazione con la disciplina che tende a tutelare nuovi soggetti, ossia gli utenti commerciali, in una ottica *ex ante*.

Va da sé che i mercati digitali, per le loro caratteristiche, schiudono un copioso numero di temi e questioni che verranno analizzate solo in riferimento ad alcuni profili. La complessità e varietà dei temi è divenuta tale anche per l'ipertrofia normativa a cui si assiste nelle latitudini europee che, già oggi, richiede una seria rivisitazione.

Capitolo I

LA CIRCOLAZIONE DEI DATI NEI MERCATI DIGITALI EUROPEI

Sommario: 1. Premessa – 2. «Privacy»: riservatezza e trattamento dei dati personali – 3. La definizione di dato personale – 4. La concezione di dato personale nella recente giurisprudenza europea – 5. I principi di *accountability*, privacy *by default* e *by design* nel Regolamento generale sulla protezione dei dati (Reg. UE 2016/679 – GDPR) – 6. I principi di limitazione delle finalità, proporzionalità, minimizzazione, esattezza e trasparenza nel trattamento dei dati personali nel GDPR – 7. Il diritto alla portabilità dei dati personali ai sensi dell'art. 20 GDPR – 8. Le basi giuridiche per il trattamento dei dati personali – 9. La base giuridica del consenso (art. 6, par. 1, lett. a, GDPR) – 10. La prima teoria sul consenso: la visione negoziale – 11. La seconda teoria sul consenso: la visione autorizzatoria – 12. Il consenso in senso unitario o duale – 13. La base giuridica del legittimo interesse (art. 6, par. 1, lett. f, GDPR) – 14. Ancora sulla base giuridica del legittimo interesse del titolare del trattamento (o di un terzo). Le recenti linee guida dell'EDPB – 15. L'applicazione del legittimo interesse nel contesto del *marketing* diretto (secondo le linee guida EDPB) – 16. Il legittimo interesse nella recente decisione IAB Europe (CGUE - C-604/2022) – 17. La teoria patrimonialistica e personalistica sul trattamento dei dati personali – 18. Il trattamento dei dati come condizione necessaria per accedere al servizio digitale: le operazioni di *tying* – 19. Le prescrizioni concernenti i contratti di fornitura di contenuto digitale o dei servizi digitali tra operatori economici e consumatori (la direttiva UE 2019/770) – 20. L'utilizzo secondario dei dati personali e il principio di limitazione della finalità del trattamento – 21. Le operazioni di «profilazione» dell'utente e il processo decisionale automatizzato (art. 22 GDPR) – 22. Il fenomeno del *Black Box* e l'impatto sul principio di trasparenza

1. *Premessa*

Si può sostenere che il concetto di *privacy,* negli ultimi decenni, ha subìto una trasformazione dovuta non solo a interventi legislativi (uno su tutti il GDPR entrato in vigore nel 2018) ma anche al parallelo sviluppo di nuove tecnologie che richiedono un differente approccio [1]. I procedimenti delle Autorità preposte alla tutela dei dati personali si sono moltiplicati e i dibattiti dottrinali hanno assunto nuova linfa.

In questi ultimi è ricorrente il riferimento a un processo di disumanizzazione dovuta alla simbiosi tra dati personali e capitalismo digitale [2].

---

[1] Le nuove tecnologie della comunicazione, combinate con la pervasiva circolazione dei dati personali di cui si servono generano fenomeni sociali ed economici di cui si dibatte sempre con maggior vigore. Il fenomeno ha finanche condotto ad una scarsa sensibilità da parte degli interessati sul reale valore dei dati personali. La distrazione o il disinteresse dell'utente nella manifestazione del consenso al trattamento dei dati personali è ormai una caratteristica sociale diffusa. In questo senso, D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza italiana,* n. 12, 2019, 2785. In letteratura alcuni sottolineano come le tecnologie di IA tendano a radicalizzare tale automatismo. Si veda a tal proposito G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *federalismi.it*, n. 16, 2020, 282; M.L. JONES, E. KAUFMAN, E. EDENBERG, *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy*, vol. 16, n. 3/2018, 64 ss.; numerosi studi sul comportamento degli utenti mettono in risalto come questi prestino consenso al trattamento dei dati quasi nella totalità dei casi e senza prendere contezza dell'informativa privacy. A tal proposito si veda G. SIMEONE, *Machine learning e tutela della Privacy alla luce del GDPR*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, Pacini, 2020, 291.

[2] A. ESPOSITO, *Dove sono i miei dati? Privacy e reificazione nell'era digitale*, in *Etica & Politica / Ethics & Politics*, vol 23, n. 1, 2021, 496, spec. 498, dove l'A. illustrando l'elemento della "privazione" rileva come oggi «la sfera privata è infatti divenuta privazione dei rapporti umani all'interno di un orizzonte spersonalizzante. In quanto dato personale, il privato penetra la dimensione pubblica come un qualcosa di alienato rispetto all'utente stesso, divenendo oggetto di processi economici mirati al profitto. Il dato personale rappresenta insomma quell'oggetto nel quale l'intimità della persona viene sradicata e posta sul piano pubblico». In relazione all'elemento

Il tema della protezione dei dati personali non si esaurisce a un suo ambito ristretto, ma deve estendersi alla complessità dei rapporti socioeconomici di oggi e dev'essere letto in un rapporto sinergico con altri settori e discipline, tra cui quella antitrust e quella consumeristica [3].

---

della burocratizzazione l'A., pag. 499, la lega alla mancanza di controllo da parte del soggetto interessato sui meccanismi che conducono alla privazione e che ne permettono il propagarsi. La disumanizzazione dell'uomo collimerebbe, quindi, con la burocratizzazione del sistema interno al mondo del digitale e al mercato dei dati personali. Per quanto riguarda l'ultimo elemento, la reificazione, p. 503, si pone in evidenza come gli «esseri umani sarebbero ridotti a puri rapporti tra oggetti esterni, tra merci. Il dato personale rappresenta solo l'ultimo dei modi attraverso i quali i rapporti umani si reificano. In esso il singolo individuo trasforma il proprio rapporto con gli altri individui in un rapporto tra pure raccolte di dati, frammentarie e totalmente esterne rispetto alla soggettività che le produrrebbe. (...) Nell'intricata e caotica dimensione del web tali oggetti, tali merci, divengono protagonisti di meccanismi e leggi di scambio che sono ben lungi dall'essere oggetto della coscienza dell'essere umano. I dati personali e i meccanismi di sottrazione rappresentano l'oggetto della contemplazione dell'utente medio che, sebbene si illuda di partecipare attivamente alla strutturazione del proprio profilo, vede continuamente, al contrario, l'alienazione della propria intimità all'interno di processi di profilazione, di raccolta dati e di profitto privato». L'A. conclude riprendendo un contributo di S. Sevignani, *The Problem of Privacy in Capitalism and Alternative Social Media: The Case of Diaspora*, in C. Fuchs, V. Mosco (eds.), *Marx in the Age of Digital Capitalism*, Brill, Leiden/Boston, 2015, 435, evidenziando la necessità di collocare l'individuo nell'ambito della sua libertà affinché possa creare la propria dimensione digitale, sottraendosi a quel meccanismo che lo vede semplice spettatore del mondo digitale nel quale vive. Viene quindi riportato, nell'ambito dei *social network*, l'esempio della poco conosciuta piattaforma 'Diaspora*'.

[3] Mentre la disciplina del GDPR regola il mercato dei dati personali stabilendo se e quando il loro scambio è ammesso, quella riguardante i consumatori regola invece le modalità di siffatto scambio garantendo la trasparenza e prevedendo rimedi a favore dei consumatori, a prescindere dalla liceità dello scambio. In tal senso si veda S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media laws*, n. 3, 2019, 146; sul rapporto tra disciplina dei dati personali e disciplina consumeristica si veda S. Pagliantini, *L'interferenza ascosa tra GDPR e diritto dei consumatori: appunti per una tassonomia*, in *Giurisprudenza italiana*, n. 10, 2023, 2212. Sulla figura e tutela del consumatore nell'era digitale si veda L. Ammannati,

Si discute se sia necessaria un'applicazione separata delle normative citate oppure se occorra una impostazione che le adatti ad ambiti diversi rispetto alla loro naturale collocazione in un'ottica di complementarità [4]. Si tenterà, nelle pagine e nei capitoli che seguono, di porre l'accento su questo necessario rapporto di complementarità tra le discipline, in particolare tra quella concorrenziale, contrattuale e quella strettamente afferente alla protezione dei dati personali. Tra le varie questioni che nel tempo sono state poste emergono anche quelle riguardanti la possibilità di identificare casi di abuso dominante derivanti dalla violazione della normativa sui dati personali [5].

I fenomeni che sono stati sommariamente descritti attribuiscono un immenso potere ai principali attori del mercato digitale sino all'effetto estremo di produrre un fallimento di mercato a danno di utenti o consumatori [6].

Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?, in *Rivista Trimestrale di diritto dell'economia*, n. 1, 2019, 8 ss.

[4] S. PELLERITI, *La tutela dell'utente ai tempi di Facebook*, in L. AMMANNATI, A. CANEPA, G. GRECO, U. MINNECI (a cura di), *Algoritmi, Big Data, piattaforme digitali*, Torino, Giappichelli, 2021, 73. Successivamente, 77-78, l'A., analizzate alcune decisioni adottate dalle autorità indipendenti in materia antitrust, si esprime a favore di quella proposta del legislatore europeo denominata *Digital Markets Act* (DMA) - ormai definitivamente approvata e confluita nel regolamento (UE) 20221925 (che verrà meglio illustrato nei successivi capitoli) - che all'articolo 5, par. 1, lett. a), censura la condotta dei *gatekeeper* che con la quale vengono combinati i dati provenienti dalla propria piattaforma con quelli provenienti da siti terzi senza alcuna opzione per l'utente.

[5] Si veda sul punto M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in *Diritto dell'informazione e dell'informatica.*, vol. 37, n. 2, 2021, 111 ss. Sia consentito un rinvio anche a quanto esposto in G. PROIETTI, *La pubblicità nell'era delle nuove tecnologie*, in *Diritto e intelligenza artificiale,* cit., 161 ss. Per un'analisi della pubblicità mirata sotto differenti prospettive disciplinari si veda F. GALLI, *La pubblicità mirata al tempo dell'intelligenza artificiale: quali regole a tutela dei consumatori?*, in *Contratto e Impresa*, vol. 38, n. 3, 2022, 919.

[6] N, ECONOMIDES, I. LIANOS*, Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective*, in *Journal of Competition Law and Economics*, vol. 17, n. 4, 2021, 765-847. Il fallimento di mercato sarebbe una conseguenza del-

I benefici a favore delle piattaforme digitali consisterebbero nella possibilità di combinare i dati raccolti con quelli acquistati da terze parti e costruire così un più dettagliato profilo dell'utente. Tale raccolta massiva di dati, favorendo il miglioramento della qualità del servizio che viene offerto, rafforzerebbe una loro posizione dominante.

Il processo a cui si fa riferimento avviene per mezzo di una profilazione dell'utente che consente il suo inserimento nell'ambito di una determinata categoria a seconda di quelli che sono i suoi interessi, le sue preferenze, i suoi comportamenti o gli ulteriori e particolari elementi che lo caratterizzano.

A seconda della categoria nella quale l'interessato viene inserito ne potrebbe derivare l'assunzione di una decisione algoritmica (o automatizzata), ad esempio, una su tutte, la pubblicità personalizzata[7].

---

l'imposizione propria di queste piattaforme che impongono un prendere o lasciare nell'erogazione del servizio grazie alla loro posizione dominante.

[7] Sussistono dubbi sulla possibilità di considerare la pubblicità come una decisione, considerato che non produce alcun vincolo, sebbene sia stato rilevato come una attività massiva di tal genere potrebbe essere idonea a generare una significativa incidenza sull'interessato come sancito nell'art. 22 GDPR, limitando infatti la libertà di scelta degli utenti, e rinchiudendo gli stessi in una bolla poiché ricevono solo informazioni conformi alle proprie idee. In ordine al primo aspetto si veda G. Mobilio, *L'intelligenza artificiale e le regole giuridiche alla prova*, cit., 286-288, per il secondo aspetto, E. Pariser, *The filter bubble: What the internet is hiding from you*, London, Penguin Books Ltd, 2011; K. Shaffer, *Data versus Democracy: How big data Algorithms Shape Opinions and Alter the Course of History*, Colorado, 2019. In merito alla corretta applicazione del citato art. 22 GPDR, inoltre, si veda la recentissima sentenza (7 dicembre 2023, C-634/21) CGUE sul caso Schufa, consultabile al sito curia.europa.eu. Nelle sedi istituzionali europee si è aperto il dibattito inerente al trattamento dei dati personali anche in riferimento alle questioni relative alla pubblicità mirata. Il riferimento è al nuovo regolamento europeo denominato *Digital Services Act*. Quest'ultimo si inserisce nell'insieme di quelle proposte che compongono le regole europee della *data economy*. Al *Digital Services Act* si affianca il già citato *Digital Markets Act,* volto a regolare la competizione delle imprese con le *big tech*, il *Data Governance Act,* che si pone l'obiettivo di agevolare lo scambio di dati tra pubblico e privato, il *Data Act,* che si pone lo scopo di conferire maggior controllo sui propri dati ai cittadini, soprattutto attraverso una estensione e un rafforzamento della portabilità dei dati e l'*AI Act,* dedicato alla disciplina concernente più propriamente i sistemi di

Questa finalità, principalmente incentrata su esigenze commerciali, viene stimolata sia da piattaforme digitali come i *social network*, sia da terzi mediante l'incoraggiamento al compimento di attività di condivisione online o comunque di altre attività utili a una costante produzione di dati [8]. L'acquisizione di tali dati e il loro trattamento vanno classificati come beni fondamentali per determinate finalità; essi, grazie a operazioni di carattere predittivo, finiscono per ridurre gli atti degli uomini in dati calcolabili [9]. Per alcuni operatori del settore digitale, l'utente non viene più considerato 'soggetto', così come non è neppure più il 'prodotto' della loro attività. Infatti, il prodotto sarebbe rappresentato da quelle previsioni ottenibili dai comportamenti degli utenti vendute poi ad altri soggetti [10].

---

intelligenza artificiale. In riferimento a quest'ultima proposta legislativa, sia consentito il rinvio a G. PROIETTI, *Una normativa per l'intelligenza artificiale. La proposta di regolamento europeo*, in *Responsabilità d'impresa e autoriciclaggio*, n. 2, 2021, 198 ss. Per un primo commento sul *Digital Services Act* e sul *Digital Markets Act* si veda D. D'ALBERTI, *Google e le nuove autorità private: la metamorfosi dal fatto al diritto*, in *Rivista di diritto civile*, vol. 67, n. 4, 2021, 770.

[8] A. R. POPOLI, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *Diritto dell'informazione e dell'informatica*, vol. 34, n. 6, 2019, 1311. L'A. definisce con il termine *datafication* o datizzazione quella abilità «delle piattaforme network di trasformare in dati molti aspetti del mondo in cui viviamo, che non erano mai stati quantificati precedentemente: non solamente dati demografici o di profilazione forniti dai consumatori, ad esempio tramite sondaggi online, ma altresì, metadata - quali marche temporali, geolocalizzazione - automaticamente derivati dagli smart phone».

[9] B. ROMANO, *Civiltà dei dati libertà giuridica e violenza*, Torino, Giappichelli, 2020, 45. L'A. aggiunge, 49-50, che «trattare i naviganti nella rete come freddi dati spersonalizzati si concretizza nel manipolarli come cose, merci, ovvero nel situarli in un processo di reificazione, che esaurisce gli esseri umani nello stesso statuto degli oggetti, privi di personalità originale, capace di concepire e realizzare dei progetti, trasformativi del mondo mediante l'attività, storica e creativa del lavoro».

[10] S. ZUBOFF, *Il capitalismo della sorveglianza*, Roma, Luiss Press, 2019, 105.

2. *«Privacy»: riservatezza e trattamento dei dati personali*

Per analizzare la normativa in materia di trattamento dei dati personali e le sue varie sfaccettature non si può prescindere da una precisazione terminologica e sostanziale che spesso provoca fraintendimenti di non poco conto. Il riferimento è alla distinzione tra *privacy* intesa come riservatezza e *privacy* intesa come protezione dei dati personali.

Infatti, è molto frequente che riservatezza e trattamento dei dati personali vengano ricompresi nella stessa categoria giuridica di *privacy*. I due concetti, tuttavia, devono essere distinti tra loro perché, sebbene possano sorgere casi in cui si frappongono, sono ontologicamente differenti [11].

La nozione di *privacy* si confronta con una nuova realtà rappresentata dalla tecnologia informatica, capace di mutare radicalmente la prospettiva e di determinare un radicale mutamento di significato della locuzione che continua a «essere usata come eponima» della normativa [12].

La genesi del diritto alla riservatezza viene di norma rintracciata in altre latitudini, ossia, a cavallo tra il 1800 e il 1900, negli Stati Uniti a seguito di un celebre saggio di Samuel D. Warren e Louis D. Bran-

---

[11] Molti autori in dottrina si sono soffermati sulla distinzione tra le due figure. Tra i vari, V. Ricciuto, *L'equivoco della privacy*, Napoli, Edizioni scientifiche italiane, 2022; M. Franzoni, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in *Jus civile*, n. 1, 2021, 4-20; A. Mantelero, *Privacy*, in *Contratto e impresa*, vol. 24, n. 3, 2008, 758; M. Giuliano, *Dati personali, consenso e privacy nell'era digitale: sfide legali e implicazioni negoziali*, in *giustiziacivile.com*, n. 5, 2023; G.B. Ferri, *Persona e privacy*, in *Persona e formalismo giuridico*, Rimini, Maggioli, 1987, 276; V. Cuffaro, *Il diritto europeo sul trattamento dei dati*, in *Contratto e impresa*, vol. 34, n. 3, 2018, 1098; S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, Il Mulino, 1973, 130; J. Kokott, C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, vol. 3, n. 4, 2013, 222.

[12] V. Cuffaro, *Il diritto europeo sul trattamento dei dati,* cit., 1100.

deis,[13] benché nel sistema italiano l'influenza maggiore sia pervenuta dalla tradizione germanica[14].

Il diritto a un corretto trattamento dei dati personali, invece, è un diritto di "nuova generazione" che ha una caratteristica partecipativa[15]. In altri termini, sebbene entrambi i diritti vengano ricompresi all'interno della locuzione di *privacy*[16], il primo presuppone un atteggiamento *passivo* dell'interessato, mentre il secondo presuppone un atteggiamento *attivo*, perciò partecipativo.

Con riservatezza si intende una situazione giuridica soggettiva con una funzione in negativo, ossia una protezione dalle altrui intromissioni nella sfera privata. Con *privacy,* intesa come trattamento dei dati personali, invece, si ha una funzione in senso positivo, configurando uno strumento di realizzazione della personalità nella dimensione individuale[17]. Da tale evoluzione verso un diritto a mantenere il controllo sulle proprie informazioni sorge la configurazione di un nuovo interesse consistente nella "autodeterminazione informativa"[18].

---

[13] S. WARREN, L. BRANDEIS, *The right to privacy,* in *Harvard Law Review*, vol. 4, n. 5, 1890, 193-220. Fu solo nel 1903 che a New York venne emanata una normativa titolata "Law of Privacy" che proibì l'uso del nome di una persona, immagine e simili per pubblicità o altri scopi commerciali senza il consenso dell'interessato. Cfr. A. CZUBIK, *"The right to Privacy" by S. Warren and L. Brandeis – The story of a Scientific Article in the United States*, *Journal of American Studies,* n. 17, 2016, 211-219; A.A. MERSACK, *Right of Privacy – Civil Rights Law*, in *St. John's Law Review*, vol 9, n. 1, 2014, 159.

[14] A. MANTELERO, *Privacy,* cit., 763-764. Dopo aver segnalato come era la situazione americana prima del saggio di Warren (*privacy* intesa in base al luogo) e quella successiva al saggio (in cui subentra un diritto della personalità a prescindere dal luogo), effettua una ricostruzione dell'origine del diritto in Italia, in cui da fine anni '30, così come nei decenni successivi, l'influenza era germanica piuttosto che americana.

[15] M. FRANZONI, *Lesione dei diritti della persona,* cit., 5.

[16] A. MANTELERO, *Privacy,* cit., 757. L'A. rileva come anche in scritti giuridici accade di riscontrare l'accostamento del saggio di Warren e Brandeis con la vigente normativa sui dati personali, suggerendo la forviante idea di una ricezione di categorie concettuali che non si è in realtà avuta.

[17] V. RICCIUTO, *L'equivoco della privacy*, cit., 21.

[18] *Ivi*, 22-24. La differenza tra riservatezza e tutela dei dati personali da un punto

Quindi, per la realizzazione della *privacy* intesa come corretto trattamento dei dati personali non viene richiesta una astensione da parte di terzi, come accade per la riservatezza, bensì una determinata condotta in conformità a determinate modalità. In altri termini, l'interessato è consapevole di aver comunicato informazioni qualificate, e ha diritto a un uso corretto nella loro acquisizione, conservazione, divulgazione o cancellazione [19]. Quest'ultimo concetto di *privacy*, come diritto di nuova generazione, è legato a un sistema che presuppone un modello di relazione sociale in cui lo scambio di informazioni è costante in ogni rapporto interpersonale [20]. Nell'epoca della *infosfera* [21] si ha costantemente l'intermediazione di un terzo in cui entra in gioco l'identità digitale dell'interessato; una intermediazione che spesso avviene per mezzo di un algoritmo che entra in possesso di informazioni della persona senza le quali non potrebbe essere accettato come utente [22].

Dunque, la tutela dei dati personali è una categoria piuttosto recen-

---

di vista testuale e normativo viene rintracciata nell'art. 5 GDPR, là dove la riservatezza viene in considerazione come una modalità tecnica e organizzativa per garantire un'adeguata sicurezza dei dati personali, senza che essa riceva formale, esplicita e solenne consacrazione come diritto ispiratore della disciplina. Perciò, non si deve cadere nell'equivoco di ritenere che la protezione dei dati si identifichi con la riservatezza.

[19] M. Franzoni, *Lesione dei diritti della persona,* cit.*,* 5. L'A. precisa, quindi, che «il tradizionale diritto alla riservatezza protegge il segreto di certe informazioni relative alla persona, lasciando così intendere che la persona può vivere anche nel silenzio e con un isolamento che diventa, quindi, meritevole di tutela per il diritto. Quella particolare riservatezza che è parte della tutela del dato personale presuppone invece, che certe informazioni debbano essere necessariamente comunicate a coloro con i quali si viene in contatto e al sistema che lo consente. Presuppone in altri termini che la vita della persona sia necessariamente sociale, quindi che qualcosa di sé debba costantemente esser condiviso con gli altri».

[20] *Ibidem*.

[21] L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione,* Torino, Giappichelli, 2009.

[22] M. Franzoni, *Lesione dei diritti della persona*, cit.*,* 6. Lo strumento tecnologico per poter dialogare richiede lo scambio e la condivisione di dati. Nella nostra socie-

te che in Europa ha visto la propria origine con la direttiva del 1995. Oggi, i dati personali sono un tema oggetto di ricerca, non solo da parte della scienza giuridica, bensì anche nell'ambito più propriamente economico [23].

Mentre l'approccio europeo si ispira a un principio etico, generalista e centralizzato, l'approccio statunitense, invece, si ispira a principi di carattere utilitaristico, settoriale ed è decentrato. Tuttavia, nonostante queste differenze, gli scopi sarebbero gli stessi, ossia quelli di salvaguardare la *privacy* dell'individuo senza danneggiare i flussi di informazione che costituiscono il cuore di ogni economia avanzata [24].

Nel sistema europeo si è così giunti al GDPR del 2016 il quale, al suo art. 1, non menziona più il diritto alla vita privata, volendo così distinguere il concetto di protezione dei dati rispetto alla vita privata, indice del «sopravvento della dimensione economica dei dati, oggetto di sempre crescente mercificazione» [25]. Rispetto al passato, l'impianto normativo del GDPR, nel suo complesso, si incentra in modo molto più netto sulla disciplina della circolazione dei dati personali [26].

Chiarita la differenza esistente tra *privacy* intesa in senso tradizionale e *privacy* come diritto di nuova generazione, occorre rilevare come il dibattito ha riguardato anche la natura e la definizione di dato personale.

3. *La definizione di dato personale*

Per le successive questioni che verranno analizzate è opportuno ripercorrere, seppur sommariamente, il dibattito che riguarda la defini-

---

tà, l'alternativa sarebbe l'isolamento della persona, che concretamente si può immaginare solamente in astratto.

[23] A. ACQUISTI, *l'economia della privacy*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007, 906-907.

[24] V. RICCIUTO, *L'equivoco della privacy,* cit., 68.

[25] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, Giappichelli, 2021, 37.

[26] *Ivi*, 38; cfr. anche G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, Edizioni scientifiche italiane, 2020.

zione di dato personale. Sulla base del diritto dell'Unione Europea, così come della *soft law* europea, può ritenersi «dato personale» qualsiasi informazione, purché sia riferito a una persona identificata o identificabile [27].

Secondo la Corte di giustizia europea, per determinare se una persona fisica sia identificabile, direttamente o indirettamente, è opportuno considerare l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da un'altra persona per identificare l'interessato, senza tuttavia richiedere che tutte le informazioni che consentono di identificare tale persona siano nelle mani di un unico soggetto [28].

In particolare, però, il dibattito ha riguardato la possibilità di ricomprendere il dato personale nell'ambito dei beni giuridici ai sensi dell'art. 810 c.c. o, comunque, nei cc.dd. «nuovi» beni [29].

Spesso la risposta affermativa al quesito viene fornita da chi sostiene una tesi patrimonialistica del dato personale per giustificarne, quindi, la sua libera circolazione. Il dato personale potrebbe essere ricompreso nella nozione di bene giuridico art. 810 c.c. rifacendosi a quella dottrina che intende il riferimento ai "diritti" di cui alla norma codicistica in un'accezione che trascende il diritto di proprietà. Si può ammettere l'esistenza di entità che possono ritenersi beni giuridici pur senza assurgere a oggetto del diritto di proprietà [30]. Invero, se, come si vedrà, è configurabile un diritto di natura patrimoniale allo sfruttamento economico dei dati personali, tali dati possono essere conside-

---

[27] G. Felici, *La tutela dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo: brevi riflessioni introduttive,* in F. Rossi Dal Pozzo (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, *Eurojus*, fasc. sp., 2020, 56.

[28] CGUE, 09 novembre 2023, n. 319, eurlex.eu.

[29] Per una ampia ricostruzione del tema che riguarda le nuove proprietà o nuovi beni, nell'ottica dell'informazione, si veda il saggio di A. Zoppini, *L'informazione come bene,* in M. D'Auria (a cura di)*, I problemi dell'informazione nel diritto civile, oggi*, Roma-Tre-Press, 2022, 79 e ss.

[30] V. Ricciuto, *L'equivoco della privacy,* cit. 66; l'A. cita dottrina come P. Perlingieri, *L'informazione come bene giuridico*, in *Rassegna di diritto civile*, n. 2, 1990, 327.

rati come beni [31]. Trattandosi di *informazione*, essa è suscettibile di trasferimenti plurimi, con conseguente possibilità di trattamenti molteplici, ciascuno dei quali non esclude gli altri [32].

Secondo questo orizzonte interpretativo, il GDPR disciplina il mercato dei dati personali attribuendogli un valore di uso e un valore di scambio, così da considerarli beni economici e, quindi, beni giuridici, disponendoli in questo modo alla contrattualizzazione [33].

Una tesi opposta, invece, ritiene che i dati personali non possano rientrare nella categoria di beni di cui all'art. 810 c.c. e, anche qualora si volessero considerare come tali, essi non vengono «tutelati in sé e per sé, in quanto tali, ma in via mediata, per essere in loro riconosciuta la qualità di elementi rappresentativi degli individui», ossia come aspetti della persona idonei a identificarla [34].

Le opinioni e le teorie su questo tema dipendono in particolar modo da quale tesi viene sposata sul valore da attribuire ai dati personali, come si vedrà di seguito. Può essere utile qui anticipare che, benché non si intravedano specifici motivi ostativi a ritenere i dati personali all'interno della nozione di bene, tale dibattito perde parte della sua rilevanza pratica se ci si concentra sull'operazione del trattamento dei dati personali piuttosto che sul dato personale in sé.

4. *La concezione di dato personale nella recente giurisprudenza europea*

Con una recente decisione della Corte di Giustizia europea sul caso IAB Europe, tra i profili trattati emerge anche quello della definizione

---

[31] P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Rivista di diritto civile*, n. 6, 2022, 1064.

[32] *Ibidem*.

[33] R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, vol. 36, n. 2, 2020, 765.

[34] C. IRTI, *Consenso "negoziato"*, cit., 45, che si rifà a G. ALPA, *la proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati: riflessioni sul GDPR*, in *Le monografie di Contratto e impresa*, Cedam, vol. 175, n. 5, 2019, 9 ss.

di dato personale e della sua estensione in termini di "identificabilità" dell'interessato. Una seconda questione su cui si è pronunciata ha riguardato invece il concetto di contitolarità del trattamento [35].

Il contesto nel quale sono stati elaborati i principi è quello del trattamento dei dati personali per finalità di *marketing*. In modo specifico, nel contesto del *Real Time Bidding* (RTB), ossia, un vero e proprio mercato all'interno del quale le imprese - *broker* di dati e piattaforme pubblicitarie - presentano offerte in tempo reale per acquisire (con una tempistica quasi istantanea) un determinato spazio pubblicitario attraverso un sistema di asta [36].

IAB Europe è una associazione rappresentante di imprese del settore dell'industria della pubblicità e del *marketing* digitale che ha elaborato un quadro di norme (specifiche tecniche, istruzioni, obblighi contrattuali e protocolli) in grado di consentire al fornitore di un sito web, o ad altri operatori di quel mercato, di trattare i dati di un utente conformemente alla normativa europea [37].

Questo quadro di norme prevede una preventiva acquisizione del consenso dell'interessato attraverso il *Consent Management Platform* e la registrazione delle preferenze degli utenti, codificate in una stringa di codice composta da lettere e caratteri (*Trasparency and Consent String*), la quale viene condivisa con i *broker* di dati e le piattaforme pubblicitarie che partecipano al RTB. Il sistema si avvale anche di un *cookie* installato sul dispositivo dell'utente e, quindi, quest'ultimo, insieme alla stringa di codice, può essere correlato all'indirizzo IP dell'interessato [38].

La Corte di giustizia, quindi, si è occupata anche della definizione di dato personale e ha premesso che con l'espressione "qualsiasi infor-

---

[35] CGUE, 7 marzo 2024, C-604/2022, *IAB Europe*.

[36] La struttura del sistema di *Real-time bidding* è descritto dettagliatamente nel provvedimento sanzionatorio dell'Autorità per la protezione dei dati personali belga, cfr. p. 7.

[37] Il quadro in questione è denominato *Trasparency & Consent Framework*.

[38] cfr. Sent. CGUE, *IAB Europe*, § 25.

mazione" contemplata nella definizione di dato personale del GDPR l'intento legislativo sia di considerare il dato in un'accezione ampia [39] che include ogni tipo di informazione, sia oggettiva quanto soggettiva [40]. Sicché, la Corte ha stabilito che la stringa contenente le preferenze degli utenti costituisce, ai sensi dell'art. 4, n. 1, GDPR, un dato personale «qualora essa possa essere associata, con mezzi ragionevoli, ad un identificativo, quale in particolare l'indirizzo IP del dispositivo di detto utente» identificando l'interessato [41].

La sentenza specifica che la circostanza secondo cui una organizzazione detentrice della stringa non sarebbe in grado di accedere ai

---

[39] La Corte è in linea con il ragionamento espresso nel provvedimento sanzionatorio dell'Autorità belga che al § B.1.1., al punto da 290 a 292, ripercorre l'ampia accezione che in Europa si è avuto in riferimento al concetto di "dato personale". Cfr. *Autorité de protection des données Gegevenschermingsautoriteit*, *Decision on the merits 21/2022 of 2 February 2022*, n. DOS-2019-01377.

[40] Al § 43 la Corte ha rilevato che «anche se una *TC String*, di per sé, non contenesse elementi che consentano l'identificazione diretta dell'interessato, rimarrebbe comunque il fatto, in primo luogo, che essa contiene le preferenze individuali di un utente specifico per quanto riguarda il suo consenso al trattamento dei dati personali che lo riguardano, nella misura in cui tale informazione» riguarda una persona fisica ex art. 4, n. 1, GDPR. Nel successivo punto, poi, sottolinea che «quando le informazioni contenute in una TC String sono associate a un identificativo, come in particolare l'indirizzo IP del dispositivo di tale utente, esse possono consentire di creare un profilo di detto utente e di identificare effettivamente la persona specificamente interessata da tali informazioni». La Corte di giustizia si era già espressa sul concetto di informazioni che qualificano il dato personale e sui criteri per l'identificabilità in CGUE C-434/2016, 20 dicembre 2017, *Nowak t. Data Protection Commissioner*, § 45.

[41] In tal senso la CGUE - *IAB Europe* § 51. La Corte giunge a tale conclusione anche in forza del considerando n. 30 GDPR. Nel provvedimento dell'Autorità austriaca, da cui origina la pronuncia della CGUE, al § 309 e 310, 66, viene enfatizzata una contraddizione in termini della politica utilizzata dal ricorrente che sarebbe volta proprio a identificare l'interessato per determinare le sue preferenze per poi ritenere che gli individui non sono identificabili. Tuttavia, la tesi del ricorrente si concentrava sul fatto che una sola organizzazione non potesse di per sé identificare un individuo senza la cooperazione di altri soggetti. Tesi, quest'ultima, in ogni caso respinta dalla Corte di giustizia.

dati trattati dai suoi membri senza un contributo esterno, né di combinare la stringa con altri elementi, non può incidere sulla qualifica di dato personale [42]. Dunque, la concezione di "dato personale" elaborata dalla Corte è molto ampia e consente di chiarirne il perimetro.

Tuttavia, la stessa Corte di giustizia ha recentemente adottato una decisione storica che pone la valutazione sulla identificabilità del dato personale sottoposto a procedura di pseudonimizzazione su un piano concreto e rimesso a una valutazione delle circostanze del caso di specie: l'analisi sulla re-identificabilità dell'interessato è un'analisi del rischio che deve tenere conto di profili concreti [43]. Il caso oggetto della decisione verteva sul tema della definizione di dato personale quando viene attuata una sua pseudonimizzazione e il dato trasferito a un terzo destinatario. Stando a tale pronuncia il contesto concreto in cui viene operato il trasferimento del dato è fondamentale. In altri termini, i dati pseudonimizzati non possono considerarsi, in tutti i casi e per ogni persona, dati personali ai fini del regolamento UE 2018/1725 [44]. Il processo di pseudonimizzazione può, a seconda delle circo-

---

[42] *Ibidem*. La Corte giunge a tale ultima conclusione in virtù del considerando n. 26 del GDPR e del precedente giurisprudenziale della stessa Corte di Giustizia, 19 ottobre 2016, Breyer, C-582/2014, § 45. Infatti, il considerando sopra citato prevede che, per stabilire «l'identificabilità» di una persona, sia 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». Tale formulazione suggerisce che, affinché un dato possa essere qualificato come «dato personale», ai sensi dell'art. 4, n. 1, GDPR, non si richiede che tutte le informazioni idonee a identificare la persona interessata si trovino in possesso di una sola persona. In questo senso il § 40 della CGUE - *IAB Europe*.

[43] CGUE, 4 settembre 2025, C-413/23, *EDPS v SRB*, curia.europa.eu. Decisione già identificati da alcuni come sentenza Deloitte.

[44] Al §86 la CGUE ha statuito che «(...) contrariamente a quanto sostiene il GEPD, non si deve ritenere che i dati pseudonimizzati costituiscano, in ogni caso e per qualsiasi persona, dati personali ai fini dell'applicazione del regolamento 2018/1725, in quanto la pseudonimizzazione può, a seconda delle circostanze del caso di specie, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato in modo tale che, per esse, quest'ultimo non sia o non sia

stanze del caso concreto, impedire di fatto a persone diverse dal responsabile del trattamento di identificare la persona interessata in modo tale che, per loro, la persona interessata non sia o non sia più identificabile [45]. In altre parole, i dati potranno considerarsi anonimi se per il terzo non è possibile materialmente o giuridicamente re-identificare l'interessato, oppure allorquando il rischio che ciò avvenga sia insignificante [46].

Analizzata l'accezione di dato personale è ora doverosa l'analisi di quei principi e di quelle regole fondamentali di *data protection* utili per affrontare i profili che interessano questo volume.

5. *I principi di accountability, privacy by default* e *by design nel Regolamento generale sulla protezione dei dati (Reg. UE 2016/679 - GDPR)*

Il Regolamento (UE) generale sulla protezione dei dati n. 679/2016 (di seguito anche "GDPR"), si fonda sul principio di *accountability* che consente di delineare un sistema fondato sulla responsabilizzazione del titolare del trattamento piuttosto che prevedere un impianto di regole precise e cogenti da osservare a pena di sanzione [47].

Il principio si estrinseca su due livelli. Il primo, si concentra sulla

più identificabile». La disciplina del GDPR, sul punto, è identica a quella del Reg. UE 2018/1725.

[45] Al §100 la CGUE ha statuito che «(...) la prospettiva pertinente per valutare l'identificabilità dell'interessato dipende essenzialmente dalle circostanze che caratterizzano il trattamento dei dati in ciascun caso particolare».

[46] La Corte riprende anche la giurisprudenza relativa a CGUE, 7 marzo 2024, C-479/22, *OC/Commissione*, curia.europa.eu

[47] G. FINOCCHIARO, *Il principio di accountability*, in *Giurisprudenza italiana*, n. 12, 2019, 2778. L'A. rileva come il principio costituisca il cardine dell'approccio basato sulla gestione del rischio cui si fonda il regolamento europeo, il quale non è quindi sancito in un'unica disposizione di quest'ultimo. Si veda altresì V. RICCIUTO, *L'equivoco della privacy,* cit., 128; C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali,* Bari, Cacucci Editore, 2022, 48; M. PEREL, N. ELKIN-KOREN, *Accountability in Algorithmic Copyright Enforcement.* in *Tech. L. Rev.*, Vol 19, 2016, 473.

necessità che il titolare del trattamento adotti misure appropriate e specifiche affinché sia attuata una effettiva protezione dei dati personali. Il secondo livello, invece, riguarda un secondo aspetto, sempre a carico del titolare del trattamento. Quest'ultimo deve essere in grado di dimostrare che le misure adottate siano efficaci e appropriate allo scopo di una effettiva protezione dei dati personali [48].

L'*accountability* trova una chiara attuazione anche per la scelta della base giuridica del trattamento [49]. Il precedente sistema si fondava su una preventiva valutazione da parte dell'Autorità della preminenza di un interesse, oggi è invece il titolare del trattamento che, sulla base della gestione del rischio, è responsabile nell'individuazione di «un equilibrio tra interessi contrapposti, con piena autonomia di giudizio» [50].

L'art. 25 del GDPR, stabilisce ulteriori principi che afferiscono all'innovativo approccio che caratterizza il sistema regolatorio. Si tratta dei principi di *data protection by design e by default* [51]. Il primo (art. 25,

---

[48] Si veda il Parere n. 3/2020 del Gruppo di lavoro ex Articolo 29.

[49] È utile precisare che con «trattamento» si intende 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, par. 1, n. 2, GDPR).

[50] G. Finocchiaro, *il principio di accountability,* cit., 2780-2781. L'A. prosegue specificando che nell'ambito dei sistemi di IA, «il principio di accountability può costituire un approccio quanto mai appropriato al problema, dal momento che alloca il rischio presso il soggetto, cioè il titolare del trattamento dei dati, che meglio è in grado di esaminare il contesto e di valutare come affrontarlo e che sarà chiamato a dimostrare l'adeguatezza delle scelte adottate».

[51] Sul tema 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*, vol. 38, n. 4, 2022, 1123; A. Principato, *Verso nuovi approcci alla tutela della privacy: privacy* by design *e privacy* by default settings, in *Contratto e impresa Europa*, vol. 20, n. 1, 2015, 197.

par.1, GDPR) stabilisce che il titolare del trattamento è tenuto ad attuare misure tecniche e organizzative adeguate a realizzare in modo efficace i principi di protezione dei dati.

Il paragrafo successivo, invece, sancisce il secondo principio, imponendo al titolare del trattamento l'adozione di misure tecniche e organizzative volte a garantire che siano trattati, per impostazione predefinita, solo quei dati personali necessari per ogni specifica finalità del trattamento [52]. Questo concetto di protezione, per una sua impostazione predefinita, si concentra sul controllo dei dati oggetto di trattamento, richiedendo che siano oggetto di "filtro" per l'intero ciclo di vita del trattamento attraverso accorgimenti tecnici e organizzativo-procedurali [53].

In dottrina si fa notare che la *privacy by design* sembrerebbe individuare una metodologia piuttosto che una specifica prescrizione [54], mentre, per converso, la *privacy by default*, poiché riguarda anche la progettazione dei trattamenti e degli apparati utilizzati già prima che abbiano concretamente avvio, retroagisce anche sulla progettazione degli strumenti e delle applicazioni finalizzate a trattare i dati personali. La *privacy by default*, quindi, soprattutto se letta alla luce del considerando 78 GDPR, trascende i titolari dei trattamenti in senso proprio e si estende anche all'attività di programmazione delle macchine, comprese quelle i cui algoritmi consentono capacità autonome di autoapprendimento [55].

---

[52] Ciò costituisce una previsione di utilità strategica laddove considera la possibile inerzia dell'interessato nell'ambito della gestione delle impostazioni che, in ordine al trattamento dei dati personali, il servizio prevede. La norma «sembrerebbe quasi far proprie le teorie dell'economia comportamentale sul nudge e in ottica proattiva porre rimedio a quell'inconsapevole inerzia dell'interessato che potrebbe arrecargli danno». In tal senso si veda G. D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. il caso dell'uso secondario di big data*, in *Diritto dell'informazione e dell'informatica*, vol. 39, n. 6, 2018, 968.

[53] S. FAILLACE, *La natura e la disciplina delle obbligazioni*, cit., 1136.

[54] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 116.

[55] *Ivi*, 114.

Le due tecniche di protezione sono tra loro complementari. Le tecnologie ideate in fase di progettazione per la tutela della *privacy* devono essere poi impostate di *default* affinché il trattamento sia ristretto ai soli dati necessari per conseguire gli obiettivi originari [56].

Quindi, con il diverso approccio di politica del diritto adottato dal legislatore europeo, non è più quest'ultimo che segue l'evoluzione delle nuove tecnologie, ma sono queste ultime ad essere, sin dall'origine della fase di progettazione, conformi al dettato normativo [57].

Come si vedrà di seguito, l'edificio normativo in materia di dati personali è proteso verso obiettivi di incentivo alla libera circolazione dei dati personali, anche – seppur con i suoi limiti - al di fuori dell'UE [58]. È per questo che si deve necessariamente analizzare il flusso dei dati personali anche in un'ottica transfrontaliera, esaminando la disciplina che sorregge il fenomeno. Una tutela dei dati personali a livello puramente europeo sarebbe del tutto monca senza una adeguata disciplina della circolazione dei dati a livello extra UE.

Tuttavia, prima di esplorare i limiti e le problematiche sulla circolazione dei dati personali, è necessario procedere preliminarmente con un'analisi di ulteriori principi generali che caratterizzano il Regolamento europeo di cui si discute.

6. *I principi di limitazione delle finalità, proporzionalità, minimizzazione, esattezza e trasparenza nel trattamento dei dati personali nel GDPR*

L'art. 5 del GDPR stabilisce, al di là della liceità, correttezza e trasparenza, altri principi generali applicabili al trattamento di dati personali.

---

[56] S. Faillace, *La natura e la disciplina delle obbligazioni,* cit., 1137.

[57] G. Simeone, *Machine learning e tutela della Privacy,* cit., 288.

[58] S. Sica, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy,* Wolters Kluwer-Cedam, Assago, 2016, 5.

Il titolare del trattamento deve precisare l'ambito degli interessi che intende realizzare, indicandoli in modo diretto o segnalando i criteri in forza dei quali individuarli in modo univoco. Tale perimetro consentirebbe la misurazione delle varie operazioni del trattamento coerentemente a quel principio di minimizzazione dei dati stabilito nello stesso articolo [59]. La determinazione della finalità del trattamento – benché vi possano essere casi di informazioni inferite dai dati - costituisce un parametro di valutazione della legittimità del trattamento [60].

Il principio di limitazione delle finalità fa sì che il trattamento oltre ad essere lecito, venga vagliato nella sua necessità e, una volta che sia stata superata in senso positivo tale accertamento, soggiace a un esame di proporzionalità. Con quest'ultima valutazione occorre accertare il grado di tollerabilità della sua effettiva incidenza sui diritti dell'interessato [61].

La proporzionalità richiede perciò una valutazione sulla congruità del trattamento rispetto alle finalità perseguite, considerando il contesto, la natura dei dati, i soggetti interessati e l'eventuale presenza o la possibile applicazione di misure meno invasive in forza di un costante bilanciamento degli interessi in gioco [62].

Il principio di minimizzazione richiede che il titolare compia le proprie attività di trattamento dei dati in modo da ridurre al minimo

---

[59] 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, Giappichelli, 2019, 207.

[60] G. FINOCCHIARO, *Considerazioni su intelligenza artificiale e protezione dei dati personali*, in U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, Giappichelli, 2021, 337, secondo cui «non mancano casi in cui, pur essendo individuati i dati da trattarsi, le finalità non possono essere determinate. Come nel caso di (...) informazioni inferite dai dati, ove la finalità del trattamento non è chiara fin dal principio, ma si va definendo con il trattamento stesso e dunque, non essendo nota, non può essere comunicata all'interessato».

[61] D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza italiana*, n. 12, 2019, 2784.

[62] L. GRECO, A. MANTELERO, *Industria 4.0, robotica e privacy by design*, in *Diritto dell'informazione e dell'informatica*, vol. 34, n. 6, 2018, 875.

le possibili interferenze con l'interessato affinché vi sia una corrispondenza del contenuto dei dati in suo possesso rispetto a quella rappresentata dai soggetti interessati [63].

La lett. d) dell'art. 5 GDPR stabilisce il principio di esattezza. È previsto che i dati oggetto di trattamento 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». Il principio di esattezza e di aggiornamento, è stato sottolineato, comporta un impedimento nell'utilizzo delle tecniche *big data* «come se si facesse una sorta di "pesca a strascico", senza, cioè, aver chiari né gli scopi perseguiti né la correttezza ed esattezza dei dati utilizzati» [64].

Dai predetti principi ne deriva l'obbligo di assicurare che il periodo di conservazione dei dati sia limitato al minimo necessario (principio della limitazione della conservazione, art. 5, par. 1, lett. e, GDPR) [65].

---

[63] M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali,* cit., 210. Non manca in letteratura chi ha segnalato come il principio appaia incompatibile con quelle tecniche di *big data analytics* e di *machine learning* che esigono una copiosa quantità di dati da raccogliere. In questo senso A. Stazi, F. Corrado, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Diritto dell'informazione e dell'informatica*, vol. 35, n. 2, 2019, 442; M. Stucke, A. Grunes, *Big Data and Competition Policy*, in *Oxford University Press*, 2016, 16; M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in *Cambridge University Press*, 2019, 24; T. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 2017, vol. 47, n. 4, 2017, 995. La Corte di giustizia europea, con una importante e recente pronuncia, ha stabilito che il principio di minimizzazione dei dati impedisce a che tutti i dati che un responsabile del trattamento (nel caso di specie si tratta del *social media* Facebook) ha ottenuto dall'interessato o da terzi siano aggregati, analizzati ed elaborati ai fini della pubblicità mirata, senza alcuna limitazione temporale e senza una distinzione che si fondi sulla natura di tali dati: CGUE, C-446-21, *Schrems* c. *Meta Platforms Ireland Ltd*, 4 ottobre 2024, eurlex.eu. La lettura di tale sentenza della CGUE è utile anche perché ha stabilito un rilevante principio sul trattamento dei dati personali particolari.

[64] F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione,* cit., 61.

[65] Deve essere considerata lecita un'ulteriore conservazione dei dati personali (rispetto a quanto consentito in virtù delle finalità del trattamento) qualora ciò sia

Il principio di *explicability*, invece, è ancora protagonista di serrati dibattiti. Questo principio trova il suo spazio naturale soprattutto negli ambiti in cui vi sono sistemi tecnologici particolarmente sofisticati la cui azione merita di essere spiegata. Sebbene la sua efficacia sia stata criticata da alcuni [66], sul piano sistematico si potrebbe ricavare una sua esistenza dal GDPR. In altri termini, questo diritto consisterebbe nella facoltà dell'interessato di comprendere le caratteristiche e l'architettura del processo decisionale a cui viene sottoposto, nonché i criteri utilizzati e le ragioni sottese [67]. Secondo alcuni commentatori, il diritto (a una spiegazione *ex post*) potrebbe essere ricavato da una interpretazione combinata degli artt. 12, 13, 14, 15 e 22 del GDPR [68].

---

necessario per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

[66] L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, 2017, 18-84. «*Firstly, the law is restrictive, unclear, or even paradoxical concerning when any explanation-related right can be triggered. Secondly, even navigating this, the legal conception of explanations as "meaningful information about the logic of processing" may not be provided by the kind of ML "explanations" computer scientists have developed, partially in response. ML explanations are restricted both by the type of explanation sought, the dimensionality of the domain and the type of user seeking an explanation. However, "subject-centric" explanations (SCEs) focussing on particular regions of a model around a query show promise for interactive exploration, as do explanation systems based on learning a model from outside rather than taking it apart (pedagogical versus decompositional explanations) in dodging developers' worries of intellectual property or trade secrets disclosure. Based on our analysis, we fear that the search for a "right to an explanation" in the GDPR may be at best distracting, and at worst nurture a new kind of "transparency fallacy." But all is not lost. We argue that other parts of the GDPR related (i) to the right to erasure ("right to be forgotten") and the right to data portability; and (ii) to privacy by design, Data Protection Impact Assessments and certification and privacy seals, may have the seeds we can use to make algorithms more responsible, explicable, and human-centered*».

[67] G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova*, cit., 289.

[68] B. GOODMAN, S. FLAXMAN, *European Union Regulations on algorithmic decision-making and a "right to explanation"*, in *AI Magazine*, vol 38, n. 3, 2017, 6.

Secondo altra parte della dottrina, esisterebbe un diritto ad essere informati *ex ante* sulla impostazione di un processo decisionale automatizzato e sulla logica utilizzata, ma non esisterebbe una spiegazione *ex post*[69]. La tesi a favore di un diritto a una spiegazione, in particolar modo a fronte di decisioni automatiche, include anche il riferimento al considerando n. 71 del GDPR[70].

Dunque, queste riflessioni e le ultime disposizioni citate impongono di annoverare anche il principio di trasparenza a cui la normativa europea dedica l'art. 12 del GDPR e gli articoli successivi per le sue declinazioni.

Secondo il "Gruppo di lavoro ex art. 29" il principio di trasparenza comporta che «(...) l'interessato dovrebbe esser in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano. (...) In particolare, per il trattamento di dati in casi complessi, tecnici o inattesi, la posizione del Gruppo è che, oltre a fornire le informazioni prescritte agli articoli 13 e 14, il titolare del trattamento debba dichiarare in una sede distinta, in un linguaggio privo di ambiguità, quali saranno le principali conseguenze del trattamento, in altre parole, quale tipo di effetto sull'interessato» avrà concretamente quello specifico trattamento[71]. Il principio di trasparenza, come si vedrà successivamente,

---

[69] S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law*, vol. 7, n. 2, 2017, 76-99.

[70] Piuttosto favorevole a un riconoscimento di tale diritto di spiegazione C. Tabarrini, *Comprendere la "big mind": il gdpr sana il divario di intelligibilità uomo-macchina?*, in *Diritto dell'informazione e dell'informatica*, vol. 35, n. 2, 2019, 565; G. Malgieri, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 7, n. 4, 2017, 243–265.

[71] In questo senso le linee guida sulla trasparenza ai sensi del regolamento 2016/679, WP 206 rev. 01, del 29 novembre 2017, così come emendate il 11 aprile 2018, 6-7.

gioca un ruolo fondamentale anche per le "ragionevoli aspettative" dell'interessato e, quindi, sulla base giuridica utilizzabile.

Prima di addentrarsi nell'analisi di altri elementi centrali del GDPR è utile analizzare il diritto alla portabilità dei dati personali, il quale – in tema di circolazione dei dati e per i suoi riflessi in materia antitrust – riveste un ruolo centrale.

7. *Il diritto alla portabilità dei dati personali ai sensi dell'art. 20 GDPR*

Il diritto alla portabilità dei dati è disciplinato nel GDPR all'art. 20, nel capo III, dedicato ai diritti fondamentali dell'interessato [72]. Con questo diritto, il legislatore europeo ha voluto rafforzare il potere contrattuale degli individui, dotandoli di un più esteso controllo sui loro dati [73]. A tale obiettivo si affianca però, il perseguimento di uno scopo pro-

---

[72] L'art. 20 GDPR prevede testualmente: «1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica 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.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui».

[73] O. BORGOGNO, *Regimi di condivisione dei dati e interoperabilità: il ruolo e la disciplina delle A.P.I.*, in *diritto dell'informazione e dell'informatica*, vol. 36, n. 3, 2019, 695. Peraltro, secondo la più recente giurisprudenza, l'esercizio dei diritti di cui agli artt. 15-22 GDPR, in caso di decesso dell'interessato, si trasmette ai suoi eredi: Tribunale Milano, Sez. I, Ordinanza del 10 febbraio 2021, in *Famiglia e Diritto*, n. 6, 2021, 622,

competitivo, rappresentando (il diritto alla portabilità dei dati) un utile mezzo per il rinvigorimento della concorrenza nei mercati digitali [74].

Invero, questo diritto non ha una valenza puramente circoscritta a un maggior controllo sui propri dati da parte dell'interessato, ma riveste un ruolo cruciale anche in un'ottica di competitività tra le imprese nel mercato dei dati. In altri termini, è un diritto che consente di rendere più contendibili le informazioni detenute da quei grandi attori che operano nei mercati digitali [75].

Per il contenuto del diritto, si può affermare che esso comprende tre pretese, tra loro astrattamente distinguibili [76]. In particolare, l'art. 20 riconosce al soggetto interessato, in presenza di specifiche condizioni, il diritto di ricevere dal titolare del trattamento i dati personali che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico. A questo si affianca il diritto di trasmettere i dati a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti. Infine, l'interessato avrà diritto, purché tecnicamente fattibile, di ottenere che il trasferimento avvenga direttamente dal vecchio al nuovo titolare [77].

Tale diritto può però essere esercitato a condizione che il trattamento si basi sul consenso o sull'esecuzione di un contratto di cui è parte l'interessato, e sia effettuato con mezzi automatizzati [78]. Esso,

---

nota di Mastroberardino; Tribunale Bologna, Sez. I, Ordinanza del 25 novembre 2021, in *Famiglia e Diritto*, n. 7, 2022,710, nota di Vignotto.

[74] O. Lynskey, *Aligning data protection right with competition law remedies? The GDPR right to data potability,* in *European Law Review*, vol 42, n. 6, 2017, 793-803.

[75] A. Manganelli, *La condivisione dei dati fra rimedi antitrust, privacy e regolazione pro-concorrenziale: un bilanciamento dinamico e cooperativo*, in *Concorrenza e mercato*, n. 1, 2022, 94, spec. 115.

[76] L. Somaini, *The right to data portability and user control: ambitions e limitations*, in *Rivista del diritto dei Media*, n. 3, 2018, 164.

[77] S. Troiano, *Il diritto alla portabilità dei dati personali*, in N. Zorzi Galgano (a cura di) *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Wolters Kluwer, n. 5, 2019, 199.

[78] M. Mirone, M. Martorana, *I diritti dell'interessato*, in M. Martorana (a cura di), *GDPR e decreto legislativo 101/2018*, Milano, Wolters Kluwer, n. 2, 2019, 24.

inoltre, può essere fatto valere esclusivamente per quei dati personali che riguardano l'interessato e da esso forniti. Alla prima di tali condizioni consegue l'inapplicabilità del diritto ai dati anonimi.

Rispetto alla seconda condizione, invece, sono intervenute le linee guida del Gruppo di lavoro art. 29 a fare chiarezza [79], le quali precisano che con l'espressione "forniti da" ci si riferisce ai dati personali relativi alle attività compiute dall'interessato o derivanti dall'osservazione del comportamento dello stesso, con l'esclusione quindi, dei dati derivanti dalla successiva analisi di tale comportamento [80].

In virtù del secondo paragrafo dell'art. 20 GDPR, affinché l'ultima delle tre facoltà possa essere esercitata, la diretta trasmissione dei dati personali da un titolare ad un altro deve essere «tecnicamente fattibile». Tale facoltà diviene così eventuale [81], essendo la sua operatività condizionata *ex ante* alla sussistenza di tale requisito [82].

Il diritto alla portabilità è inoltre escluso ogniqualvolta il trattamento sia 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» [83]. Come si legge nel considerando n. 68, infatti, per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei soggetti che trattano dati personali nell'esercizio delle loro funzioni pubbliche [84]. Nel par. 4, infine, l'art. 20 GDPR sottolinea un ulteriore limite a cui il diritto è condizionato, ossia non devono es-

---

[79] Linee-guida sul diritto alla "portabilità dei dati", adottate dal Gruppo di lavoro art. 29 il 13 dicembre 2016, versione emendata e adottata il 5 aprile 2017.

[80] A.G. MONTELEONE, *Il diritto alla portabilità dei dati. Tra diritti della personalità e diritti del mercato*, in *Luiss Law Review*, n. 2, 2017, 208.

[81] F. CATALANO, *Il diritto alla portabilità de dati tra interessi individuali e prospettiva concorrenziale*, in *Europa e diritto privato*, n. 3, 2019, 841.

[82] G.M. RICCIO, F. PEZZA, *Portabilità dei dati e interoperabilità*, in *I dati personali nel diritto europeo,* cit., 401.

[83] M. GIORGIANNI, *Art. 20 – diritto alla portabilità dei dati*, in *Commentario del codice civile*, Milano, Utet giuridica, 2019, 425.

[84] I. GRAEF, M. HUSOVEC, N. PURTOVA, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law,* in *German Law Journal,* vol. 19, n. 6, 2019, 1359.

sere lesi i diritti e le libertà altrui. Nella prassi può infatti accadere che i dati personali di un soggetto siano strettamente connessi a quelli di altri interessati con cui lo stesso entra in contatto. Pertanto, il *dataset* per il quale il titolare esercita la portabilità potrebbe ricomprendere inevitabilmente informazioni personali riferibili ad altri soggetti. Perciò, si ritiene che in questo caso il *discrimen* in base al quale accertare se possa sussistere in concreto il rischio di ledere i diritti di tali soggetti sia la finalità perseguita nel trattamento [85].

L'art. 20 GDPR definisce, inoltre, il modo in cui l'interessato deve ricevere i dati dal titolare del trattamento. Il paragrafo 1, stabilisce che il titolare deve fornire all'interessato una copia dei dati «in un formato strutturato, di uso comune e leggibile da un dispositivo automatico». Secondo il considerando n. 68, tale formato deve essere interoperabile. Per interoperabilità si intende la possibilità di trasferire dati e informazioni in generale da un sistema, un'applicazione o un dispositivo a un altro, potendoli utilizzare su ciascuno di essi. Questo concetto si salda con quello di portabilità, andando a formare l'obbligo, in capo al titolare, di utilizzare formati che permettano il riutilizzo dei dati da parte degli operatori [86].

Come si è accennato, con questo diritto vengono finanche perseguite finalità in materia di concorrenza. La portabilità agevola il passaggio da un servizio all'altro, permettendo una riduzione dei costi di *switching* [87]. Essa, inoltre, rafforza la facoltà di scegliere tra servizi concorrenti, stimolando il *multi-homing*, ossia l'impiego simultaneo dei pro-

---

[85] Ad esempio, il trattamento è lecito nel caso di un conto corrente contenente i dati di altri soggetti purché essi siano utilizzati, pur se da un altro titolare, per le medesime finalità. Se invece tali informazioni siano utilizzate per finalità diverse, come ad esempio per attività di *marketing*, la condotta sarà ritenuta illecita. F. Catalano, *Il diritto alla portabilità de dati tra interessi individuali e prospettiva concorrenziale*, in *Europa e diritto privato*, n. 3, 2019, 841, spec. 495.

[86] M. Borghi, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, n. 2, 2018, 232.

[87] A. Iuliani, *Note minime in tema di trattamento dei dati personali*, in *Europa e diritto privato*, n. 1, 2018, 308.

pri dati su servizi diversi. È grazie alla portabilità che viene stimolato il riutilizzo dei dati, rimuovendo gli ostacoli allo sviluppo di nuovi servizi e applicazioni.

Pertanto, l'art. 20 si configura come un rimedio concorrenziale a priori in grado di prevenire a monte situazioni di *lock-in* dovute a ingiustificati costi di *switching*, e di ridurre le barriere all'entrata [88]. Su questo tema si tornerà anche nel successivo capitolo III.

Questo diritto lo si ritrova sancito anche nel recente *Digital Markets Act* (DMA). In quest'ultimo, viene imposto ai *gatekeeper* di offrire gratuitamente gli strumenti per facilitare l'effettivo esercizio della portabilità, raccomandando l'utilizzo di interfacce di programmazione delle applicazioni (API) di elevata qualità; questa specifica è invece assente nel GDPR che non fornisce una guida su come assicurare i meccanismi di portabilità tra diversi soggetti [89].

Come si vedrà nel capitolo IV, la portabilità costituisce anche il fulcro della logica sottesa al nuovo regolamento del *Data Governance Act*.

8. *Le basi giuridiche per il trattamento dei dati personali*

L'art. 5, lett. a), del GDPR stabilisce che il trattamento dei dati personali deve essere lecito, corretto e trasparente. Il primo requisito viene precisato nel successivo art. 6 dove sono elencate le condizioni di liceità. È sufficiente che ricorra una sola di queste condizioni perché possa dirsi lecito il trattamento dei dati personali.

Tali condizioni costituiscono le «basi giuridiche» su cui si può fondare un determinato trattamento di dati personali. Esse sono: la manifestazione del consenso da parte dell'interessato, la necessità di un trattamento per l'esecuzione di un contratto, la necessità di adempiere ad un obbligo legale, la necessità di salvaguardare gli interessi vitali dell'interessato o altra persona fisica, la necessità di eseguire un com-

---

[88] M. BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, cit., 226.

[89] A. MANGANELLI, *La condivisione dei dati fra rimedi antitrust*, cit., 121.

pito di interesse pubblico, l'ipotesi del legittimo interesse del titolare del trattamento.

Quest'ultima, probabilmente costituisce la base giuridica più delicata e per questo "abusata" per alcune operazioni. Si tratta dell'ipotesi in cui il trattamento è necessario per il perseguimento di un 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.

Nei paragrafi che seguono si analizzeranno le due basi giuridiche più rilevanti ai fini del presente scritto, ossia il consenso dell'interessato e l'interesse legittimo del titolare del trattamento.

9. *La base giuridica del consenso (art. 6, par. 1, lett. a, GDPR)*

Le condizioni di liceità dettate dal GDPR - secondo una precisa impostazione dottrinale - producono la rimozione di un limite o di un ostacolo che l'ordinamento pone al preesistente potere privatistico o pubblicistico del titolare del trattamento, espandendo quindi questo potere per la realizzazione di interessi conformi all'ordinamento [90]. Ciò vale anche per la base giuridica probabilmente più utilizzata, vale a dire il consenso, [91] ancorché questo sembri aver subito una decentralizzazione con l'entrata in vigore del GDPR rispetto al previgente impianto della direttiva 95/46/CE [92].

Il consenso richiesto in tema di trattamento dei dati personali va

---

[90] F. Bravo, *Lo scambio dei dati personali nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e Impresa*, vol. 30, n. 1, 2019, 34.

[91] Per un'analisi dei profili tecnici dell'istituto del consenso si veda G. Versaci, *Consenso al trattamento dei dati personali e* dark patterns *tra opzionalità e condizionalità*, in *Le nuove leggi civili commentate*, vol. 45, n. 5, 2022, 1130.

[92] F. Caggia, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Rivista di diritto commerciale*, vol. 117, n. 3, 2019, 405.

distinto dal consenso richiesto in via generalizzata in campo negoziale; infatti, si tratta di un consenso informato, e quindi rafforzato, richiesto allorché siano in gioco interessi fondamentali come l'autodeterminazione della persona con obblighi di informazione a carico della parte più *forte*[93]. Come si vedrà, quindi, si discute ampiamente su quale sia la natura del consenso, ovvero se debba essere inteso in senso *negoziale* o *autorizzatorio*[94].

Quando la base giuridica è costituita dal consenso, occorre considerare anche l'elemento della granularità che ricorre nel caso di perseguimento di più finalità. Quest'ultimo risulta in alcuni casi carente, ad esempio nell'ambito dei *social network* dove l'attività di accettazione del contratto e il consenso al trattamento dei dati viene spesso concentrata in un'unica azione e, sebbene vi sia un riferimento a più finalità, ad esse non corrispondono distinti consensi[95]. Sarebbe necessaria, quindi, l'indicazione della finalità dell'attività di trattamento in forma specifica, esplicita e legittima, benché la mancata soddisfazione del requisito della specificità insita nelle formule generiche come "migliorare l'esperienza degli utenti", "finalità di marketing", "finalità di sicurezza informatica" o "ricerca futura" rappresenta una prassi quasi consolidata[96].

In ogni caso, sul consenso si sono sviluppate due principali teorie: negoziale e autorizzatoria.

---

[93] A. MORACE PINELLI, *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova giurisprudenza civile commentata*, n. 6, 2022, 1327.

[94] Si veda in proposito la ricostruzione ad opera di A. PURPURA, *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data*, in *Jus civile*, n. 4, 2022, 905; si veda altresì la puntuale illustrazione delle due tesi dottrinali in F. CAGGIA, *Il consenso al trattamento dei dati personali nel diritto europeo,* cit., 410-413.

[95] A.R. POPOLI, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato,* cit., 1289 ss.

[96] *Ibidem*.

10. *La prima teoria sul consenso: la visione negoziale*

Come accennato, si sono sviluppate due teorie dottrinali sulla base giuridica del consenso, la prima su una visione "negoziale" e la seconda, invece, "autorizzatoria".

Secondo la prima teoria, la manifestazione del consenso non andrebbe a ledere l'autodeterminazione dell'interessato, ma favorirebbe la logica circolatoria dei dati personali [97]. Inteso in questo senso, il consenso avrebbe una funzione di tipo dispositivo dei dati personali, considerati come bene e, in quanto elementi che orbitano nella sfera del soggetto, cedibili e trasferibili come merce di scambio per la fornitura di un determinato servizio [98].

Non si produce o trasferisce un titolo di proprietà, ma si fa riferimento a un concetto di *appartenenza* [99] poiché l'interessato non potrebbe compiere un atto traslativo, non potrebbe trasmettere la titolarità del dato personale. Gli effetti di un consenso all'ingerenza altrui nella propria sfera giuridica possono manifestarsi in obblighi di

---

[97] A. Purpura, *Il consenso nel mercato dei dati personali,* cit., 905.

[98] *Ivi*, 905-906. L'A. sostiene che «la lettura negoziale rifletta meglio l'autodeterminazione individuale all'atto di adesione al contratto per la prestazione del servizio. Un'adesione, si è riferito, in definitiva analoga a quella di utenti e consumatori al cospetto della predisposizione di contratti di massa uniformi. (...). Si aggiunga che l'inclusione dei dati personali nel perimetro dell'oggetto contrattuale, fungendo sostanzialmente da controprestazione, assume ampio risalto, specie dinanzi a quelle operazioni contrattuali che (...) riguardano trattamenti massivi di dati personali. Come vicenda negoziale il consenso non soltanto può dunque vestire i panni sia di una manifestazione di volontà pura e semplice, atto di determinazione non piegato alla logica dello scambio, ma può giustificarsi in vista della (contro)prestazione di un servizio»; si veda a tal proposito anche V. Zeno-Zencovich, *Una lettura comparatistica della L. 675/96 sul trattamento dei dati personali*, in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffré, 1998, 159 ss.

[99] G. Oppo, *Sul consenso dell'interessato*, in, *Trattamento dei dati e tutela della persona*, cit., 124.

comportamento in capo all'interessato e in capo al titolare del trattamento [100].

La visione negoziale viene abbracciata anche da chi sostiene che vi sia stata una evoluzione a seguito del recepimento della recente direttiva 2019/770/UE nel codice del consumo in cui viene regolato lo scambio contenuto digitale – dati personali. Nel prestare il consenso a che altri soggetti utilizzino gli attributi della persona, ne viene fuori una negozialità che conferisce un godimento il quale, poiché concesso ad altri, non è più (temporaneamente) esclusivo [101].

11. *La seconda teoria sul consenso: la visione autorizzatoria*

Una differente teoria, invece, benché con differenti sfumature, inquadra il consenso nella sua funzione autorizzatoria, ossia come un elemento che elide l'antigiuridicità della condotta, la quale si va ad esprimere attraverso il trattamento dei dati personali [102].

Il consenso avrebbe una funzione autorizzatoria di tipo integrativo, e non costitutivo. Non potrebbe essere ritenuto avente una funzione di scriminante, tanto da giustificare comportamenti altrimenti illeciti, ma rimuove un ostacolo che l'ordinamento pone in funzione di protezione dell'interessato allo svolgimento di un'attività di per sé non illecita [103].

---

[100] S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di diritto civile*, n. 6, 2001, 633.

[101] S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies – 135 vicies ter c.cons.*, in *Le nuove leggi civili commentate*, n. 6, 2022, 1510.

[102] G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *diritto dell'informazione e dell'informatica*, 1993, 313 ss.; R. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Rivista critica diritto privato*, 1998, 339 ss., spec. 350; S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Rivista di diritto civile*, n. 2, 1999, 466; A. ADDANTE, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *giustizia civile*, n. 4, 2020, 889, spec. 894.

[103] F. BRAVO, *Lo scambio dei dati personali nei contratti di fornitura di servizi digitali,* cit., 42.

È stata poi indicata e criticata un'altra teoria che attribuirebbe all'atto del consenso una funzione costitutiva di un vincolo negoziale. Si è criticato che la natura negoziale del consenso al trattamento ai dati personali è «chiaramente antitetica, sul piano concettuale, al riconoscimento di una revoca dell'atto stesso in quanto il vincolo, una volta contratto, si manifesta irretrattabile agli occhi delle due parti. Tuttavia, nonostante le difficoltà dogmatiche nel prospettare una riposta positiva al quesito se fosse possibile ammettere un potere di revoca del consenso, si fa strada una posizione possibilista che fa leva sull'argomento che non esiste sempre un collegamento tra natura negoziale e non revocabilità, essendo, quest'ultimo», un elemento che viene rintracciato anche in alcuni impegni contrattuali [104].

Come si vedrà qui di seguito, il serrato dibattito sul consenso riguarda anche la sua struttura unitaria o duale.

12. *Il consenso in senso unitario o duale*

In letteratura viene rilevato che per tutte quelle operazioni (*tying*, come si vedrà in seguito) in cui è previsto il rilascio del consenso al trattamento dei dati personali quale *prestazione condizionale* per accedere a un determinato servizio (digitale), sebbene sia incontestabile che il trattamento dei dati divenga di fatto merce di scambio per il servizio, è necessario distinguere la duplicità dei piani disciplinari [105]. Perciò, si deve tener distinto «il *consenso autorizzativo* a carattere unilaterale, che viene "scambiato" al fine di ottenere il prodotto o servizio, e il *consenso negoziale* quale dichiarazione adesiva dell'utente al regolamento che disciplina il rapporto» [106].

Nella "commercializzazione" dei dati personali questi andrebbero inquadrati diversamente sotto il profilo giuridico, individuando un

---

[104] F. Caggia, *Il consenso al trattamento dei dati personali nel diritto europeo,* cit., 428.
[105] C. Irti, *Consenso "negoziato",* cit., 77.
[106] *Ibidem*.

consenso contrattuale ontologicamente distinto rispetto a quello reso in materia di protezione dei dati personali, benché ad esso funzionalmente collegato [107]. Perciò, all'atto autorizzatorio si potrebbe aggiungere un accordo di natura contrattuale, a titolo oneroso o gratuito, avente ad oggetto atti di esercizio dei diritti sui dati personali dell'interessato senza che il secondo si sostituisca al primo. Quindi, «i due consensi resi dall'interessato, di natura diversa, convivono e interagiscono, essendo tra loro funzionalmente collegati» [108].

Si avrebbe così (i) un consenso di natura autorizzatoria, come previsto ai sensi dell'art. 6, par. 1, lett. a), del GDPR «che risponde alle logiche di inquadramento del diritto alla protezione dei dati personali all'interno dei diritti della personalità, indisponibili, intrasmissibili, irrevocabili, e, al contempo, (ii) un ulteriore consenso, 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 sui dati personali dell'interessato medesimo - concorda con il titolare del trattamento le modalità di utilizzo dei dati, anche in una logica di natura patrimoniale, nell'ambito della quale non si spoglia mai del diritto alla protezione dei dati personali» [109]. Infatti, secondo siffatta impostazione, l'interessato conserverebbe il controllo sui dati anche se questi siano stati oggetto di un rapporto contrattuale, poiché potrebbe sempre revocare il consenso autorizzatorio che è stato reso in materia di protezione dei dati personali [110].

D'altro canto, non manca chi predilige una lettura che non considera la manifestazione del consenso in due atti distinti, bensì in senso unitario. I due consensi, nel loro insieme, formano lo scambio servi-

---

[107] F. BRAVO, *Lo scambio dei dati personali nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto,* cit., 44. In questo senso, l'A. critica l'impostazione che ravvisa una natura dispositiva al consenso dell'interessato reso ai sensi della disciplina in materia di protezione dei dati personali, o, traslativa di un diritto su un bene immateriale.

[108] *Ibidem.*

[109] *Ivi*, 45-46.

[110] *Ibidem.*

zio - dati personali, senza che il consenso al trattamento dei dati rappresenti un elemento costitutivo del contratto. Quindi, si fa riferimento a un «consenso autorizzativo a carattere unilaterale, scambiato per ottenere il prodotto-servizio, e di un consenso negoziale quale dichiarazione adesiva dell'utente al regolamento che disciplina il rapporto» [111].

Questa differente teoria sostiene che sia preferibile considerare il GDPR e il contratto fondati su un unico atto la cui disciplina sia ricostruita in base al GDPR, al contratto in generale e alla tutela dei consumatori [112]. Secondo i fautori di questa impostazione interpretativa, «quando il bene personale entra nel contratto, l'atto negoziale che acconsente all'interferenza nella propria sfera personale utilizzando lo specifico "bene" (consenso al trattamento) e l'atto di disposizione patrimoniale del "bene" stesso (consenso contrattuale) partecipano alla medesima fattispecie negoziale stringendosi in un rapporto conformativo, in cui il primo funge da congegno determinativo dell'oggetto del contratto» [113].

Dunque, sulla base giuridica del consenso, le teorie che si sono sviluppate sono diverse e volte a fornire un quadro dogmatico per definire i contorni delle operazioni di *tying* (*infra*, §18) che ormai pervadono il mondo digitale. Tuttavia, prima di descrivere queste operazioni, occorre dedicare la dovuta considerazione anche all'altra base giuridi-

---

[111] V. Ricciuto, *L'equivoco della privacy,* cit., 142.

[112] P. Gallo, *Il consenso al trattamento dei dati personali come prestazione,* cit., 1067.

[113] S. Senigaglia, *La dimensione patrimoniale del diritto alla protezione dei dati personali,* cit., 771. Secondo l'A. sarebbe «meno rappresentativa di questa realtà dello scambio, la ricostruzione che ravvisa nel consenso al trattamento una duplice natura e un ruolo comunque esterno alla fattispecie contrattuale: «da un lato, atto unilaterale di tipo autorizzatorio che esclude l'illegittimità dell'utilizzo di un altrui attributo della personalità da parte di terzi, permettendo la negoziazione di fatto dei dati; dall'altro, espressione della signoria del singolo sulle informazioni che lo riguardano, che non può venir meno a seguito della comunicazione dei dati a terzi, ma trova solo nelle previsioni di legge specifiche limitazioni o deroghe».

ca più volte utilizzata per realizzare operazioni di questo genere: il legittimo interesse del titolare del trattamento.

13. *La base giuridica del legittimo interesse* (*art. 6, par. 1, lett. f, GDPR*)

La base giuridica del legittimo interesse del titolare è anch'essa molto utilizzata nella prassi. Questa, tuttavia, costituisce una base giuridica discussa, stante il costante bilanciamento richiesto con gli interessi, i diritti e le libertà del soggetto interessato. Un bilanciamento che non può essere improntato su fattori di principio, ma è bisognoso di essere adattato alle caratteristiche particolari del singolo caso [114].

Il Garante per la protezione dei dati personali italiano qualche anno or sono ha indicato come buona prassi quella di fornire all'interessato le indicazioni essenziali risultanti dal bilanciamento di cui all'art. 6, par. 1, lett. f), GDPR effettuato nel caso concreto [115]. Tuttavia, con una più recente decisione di altra Autorità di controllo è stata evidenziata la necessità di procedere con tre diversi test, e solo il terzo è composto dal test di bilanciamento [116].

In sostanza, il titolare del trattamento deve dimostrare:

(i) che gli interessi perseguiti con il trattamento sono legittimi (*test della finalità*);

(ii) che il trattamento è necessario al conseguimento di tali interessi (*test sulla necessità*);

---

[114] M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali,* cit., 229

[115] GPDP, *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni di cui al Regolamento UE 2016/679,* 22 febbraio 2018, consultabile al sito www.*garanteprivacy.it*

[116] Il provvedimento è quello della *Autorité de protection des données Gegevenschermingsautoriteit*, *Decision on the merits 21/2022 of 2 February 2022*, DOS-2019-01377, 88-89; nello stesso senso, però, si è poi pronunciato l'EDPB con le linee guida del 8 ottobre 2024, G*uidelines* 1/2024 *on processing of personal data based on Article 6(1)(f) GDPR*, consultabili al sito www.edpb.europa.eu, 7-12.

(iii) il bilanciamento degli interessi perseguiti con gli interessi, le libertà e i diritti degli interessati (*test di bilanciamento*).

Con il test di bilanciamento, nel suo complesso, dovranno essere considerati alcuni elementi tra cui la natura dell'interesse legittimo del titolare e l'eventualità che il trattamento dei dati sia necessario per l'esercizio di un diritto fondamentale dello stesso titolare. Inoltre, non possono essere trascurate le ragionevoli aspettative degli interessati su ciò che accadrà ai loro dati, nonché la natura dei dati e le modalità di trattamento [117]. Le garanzie supplementari che potrebbero limitare l'incidenza del trattamento sull'interessato sono la minimizzazione dei dati, le tecnologie di rafforzamento della tutela della vita privata, una maggiore trasparenza e la portabilità dei dati [118].

Da un punto di vista metodologico, il test comparatistico e di bilanciamento deve fondarsi su due livelli:

da un lato, l'analisi del legittimo interesse espresso dal titolare e l'impatto sugli interessati. All'interno di tale valutazione devono essere già considerate le misure di salvaguardia messe a punto dal titolare a beneficio dell'interessato. Solo nel caso di esito negativo rispetto ad un provvisorio bilanciamento sarebbe necessario vagliare la possibilità di correttivi mediante la previsione di ulteriori misure [119].

L'interesse del titolare individuato dev'essere concreto ed effettivo. A fronte di interessi di per se preminenti per la società, altri possono caratterizzarsi per la loro natura controversa come, ad esempio, l'ipotesi di un'impresa «il cui interesse economico è venire a conoscenza del maggior numero possibile di informazioni sui suoi potenziali clienti al fine di pubblicizzare in maniera più mirata i suoi prodotti

---

[117] Le aspettative dell'interessato sono state messe in risalto anche dalla pronuncia della Corte di giustizia, CGUE, C-708/18, 11 dicembre 2019, *TK v. Asociatia de Proprietari bloc M5A-ScaraA*, § 58.

[118] D. Poletti, *Le condizioni di liceità del trattamento dei dati personali,* cit., 2788.

[119] Gruppo di Lavoro Art. 29 per la protezione dei dati, Parere n. 6/2014, *sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 09 aprile 2014, 40, consultabile al sito www.*ec.europa.eu*

o servizi»[120] benché venga ammesso che il titolare del trattamento, possa avere un interesse legittimo «a conoscere le preferenze dei loro clienti per poter personalizzare meglio le loro offerte e, in definitiva, offrire prodotti e servizi in grado di soddisfare meglio le esigenze e i desideri dei clienti»[121].

Va da sé che lo scopo dell'intera valutazione consiste nell'evitare la creazione di un impatto sproporzionato a carico dell'interessato[122]; quindi, in primo luogo, esaminando quella che è la natura dei dati acquisiti e trattati, tenendo in debita considerazione che alcuni di essi, apparentemente innocui, se trattati su vasta scala e combinati con altri dati, potrebbero dare luogo a deduzioni su dati più sensibili, o "particolari"[123].

Un altro elemento che deve essere tenuto in debita considerazione

---

[120] Gruppo di Lavoro Art. 29 per la protezione dei dati, Parere n. 6/2014, cit, 29, in cui vengono elencati, a titolo esemplificativo, alcuni degli ambiti più comuni in cui è possibile individuare un legittimo interesse. Tra questi vengono riportati 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.

[121] Nel documento, a pag. 30, si aggiunge che tale interesse potrebbe costituire una base giuridica adeguata ad alcune attività di commercializzazione, sia online che offline, «purché sussistano adeguate garanzie» incluso il meccanismo consistente nel diritto di opposizione. Ciò «non significa che i responsabili del trattamento potranno avvalersi dell'articolo 7, lettera f), per controllare indebitamente le attività online o offline dei loro clienti, combinare grandi quantitativi di dati che li riguardano, dopo averli ricavati da varie fonti e averli inizialmente raccolti in altri contesti e per finalità differenti, e creare (e, ad esempio, grazie agli intermediari che forniscono dati, anche effettuare la compravendita di) profili complessi delle personalità e delle preferenze dei clienti a loro insaputa, senza un meccanismo efficace che permetta di opporsi al trattamento dei dati e tantomeno senza il loro consenso informato. È probabile che tale attività di profilazione costituisca una considerevole ingerenza nella vita privata del cliente e, in tal caso, sull'interesse del responsabile del trattamento prevarrebbero gli interessi e i diritti dell'interessato».

[122] Gruppo di Lavoro Art. 29 per la protezione dei dati, Parere n. 6/2020, cit., 48.

[123] *Ivi*, 45-46.

è lo *status* dell'interessato e del responsabile (o titolare) del trattamento. In altri termini, a seconda che il titolare sia una persona o un'organizzazione di piccole dimensioni, una grande impresa multinazionale o un ente pubblico, e in base alle circostanze specifiche, la sua posizione potrebbe essere più o meno dominante rispetto all'interessato [124].

In ogni caso, le motivazioni per cui il titolare ritiene che i diritti dell'interessato non prevalgono sul suo legittimo interesse devono essere enunciate in modo chiaro [125]. Molti attori digitali fanno spesso ricorso alla base giuridica del legittimo interesse per il trattamento dei dati personali; l'utilizzo di questa base legale fa leva sul considerando n. 47 GDPR il quale prevede la possibilità di configurare un legittimo interesse nel trattamento di dati personali per finalità di *marketing* diretto.

Tuttavia, avvalersi dell'indicazione - non vincolante - del legislatore senza una corretta, lecita e trasparente condotta nel trattamento dei dati potrebbe sfociare in un abuso.

Ciò che viene indicato dal GDPR è una possibilità, non un auto-

---

[124] *Ivi*, 48.

[125] In particolare, a pagina 52 del parere n. 6/2020 viene specificato che se vengono occultate «informazioni importanti in merito a un non previsto ulteriore utilizzo dei dati in termini legalistici nascosto nei caratteri minuscoli di un contratto, questo comportamento potrebbe costituire una violazione delle norme in materia di tutela dei consumatori. (...) In alcuni casi, per esempio, gli utenti di servizi "gratuiti" online, quali motori di ricerca, posta elettronica, mezzi di comunicazione sociale, archiviazione di documenti o altre applicazioni online o mobili, non sono pienamente consapevoli della misura in cui le loro attività sono registrate e analizzate al fine di generare valore per il fornitore di servizi e pertanto non si preoccupano dei rischi connessi. Al fine di responsabilizzare gli interessati in queste situazioni, una prima condizione preliminare, necessaria ma tutt'altro che sufficiente di per sé, è chiarire che i servizi non sono gratuiti e che, invece, i consumatori pagano utilizzando i loro dati personali. Le condizioni e le garanzie subordinatamente alle quali potrebbero essere utilizzati i dati devono a loro volta essere indicate chiaramente in ogni caso al fine di garantire la validità del consenso di cui all'articolo 7, lettera a), oppure un bilanciamento favorevole ai sensi dell'articolo 7, lettera f)».

matismo. Il legittimo interesse abbisogna in ogni caso di un test comparatistico tra le posizioni giuridiche in gioco che è rimesso - per il principio di *accountability* - in capo al titolare del trattamento.

La valutazione in questione è strettamente legata al principio di proporzionalità e trasparenza. Essa, oltre a identificare qual è il concreto ed effettivo legittimo interesse, considerando la natura dei dati trattati, le ragionevoli aspettative e lo *status* dell'interessato, esige, nel caso di esito favorevole al legittimo interesse del titolare del trattamento, la formulazione di una motivazione chiara ed esauriente. Suscita pertanto perplessità, ad esempio, quella prassi degli operatori digitali che si limita alla semplice indicazione del legittimo interesse del titolare e all'individuazione della finalità di trattamento.

Va da sé che il principio di trasparenza si estrinseca differentemente a seconda delle circostanze e delle caratteristiche del caso concreto. Gli elementi che si devono considerare, peraltro, differiscono a seconda che siano previste o meno decisioni automatizzate, ovvero, a seconda che sia prevista o meno una profilazione.

Tra i vari elementi, le legittime aspettative dell'utente/interessato hanno rivestito un ruolo centrale in una fondamentale e recente pronuncia della Corte di Giustizia europea (CGUE C-252/21, 4 luglio 2023) che ha interessato la base giuridica del legittimo interesse. La CGUE, pronunciandosi in riferimento a vicende legate al trattamento dei dati personali da parte di Meta per finalità di *marketing*, ha sottolineato come nella ponderazione dell'interesse del titolare e dei diritti dell'interessato occorre tener conto delle ragionevoli aspettative dell'interessato e della portata del trattamento, oltre al suo impatto sulla persona [126].

Ebbene, nella sentenza si legge che «(...) malgrado la gratuità dei servizi di un social network online quale Facebook, l'utente di quest'ultimo non può ragionevolmente attendersi che, senza il suo consenso, l'operatore di tale social network tratti i suoi dati personali a fini di personalizzazione della pubblicità. In tali circostanze, si deve

[126] Sentenza CGUE, C-252/21, § 116.

ritenere che i diritti fondamentali e gli interessi di tale utente prevalgano sull'interesse dell'operatore a tale personalizzazione della pubblicità mediante la quale egli finanzia la sua attività, cosicché il trattamento da quest'ultimo effettuato a tali fini non può rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD»[127]. Pertanto, la pronuncia, sul tema del legittimo interesse conclude che tale norma deve essere interpretata nel senso della legittimità di un trattamento in virtù di tale base giuridica solo se l'operatore digitale indichi agli utenti, presso cui i dati vengono raccolti, un legittimo interesse perseguito e che il trattamento venga effettuato entro i limiti di quanto necessario alla realizzazione dell'interesse stesso; che dal contemperamento degli interessi contrapposti risulti che i diritti e le libertà degli utenti non prevalgano sull'interesse del titolare del trattamento o di terzi[128].

Su questo stesso tema è doveroso accennare alla recente adozione di una decisione urgente e vincolante da parte dell'EDPB del 27 ottobre 2023 sul trattamento dei dati personali per la pubblicità comportamentale di Meta[129].

Con questa decisione l'Organismo ha incaricato il DPA irlandese di adottare misure nei confronti di Meta e di imporre un divieto di trattamento dei dati personali per la pubblicità comportamentale sulle basi giuridiche del contratto e dell'interesse legittimo in tutto lo Spazio economico europeo (SEE)[130].

La più recente linea politica che alcuni operatori come Meta stanno adottando riguarda una doppia opzione lasciata all'utente e rappresentata dal consenso al trattamento dei dati personali per finalità di *marketing* in cambio del servizio, oppure, l'accesso al servizio dietro paga-

---

[127] *Ivi*, § 117.

[128] *Ivi*, § 126.

[129] EDPB, *Urgent Binding Decision on processing of personal data for behavioural advertising by Meta*, consultabile al sito www.edpb.europa.eu

[130] Tale decisione ha fatto seguito a una richiesta dell'Autorità norvegese per la protezione dei dati affinché fossero adottare misure definitive in materia che avrebbero avuto effetto nell'intero Spazio economico europeo (SEE).

mento (pecuniario) di un abbonamento. Quest'ultima opzione del pagamento di un corrispettivo non comporta alcun trattamento dei dati personali per finalità commerciali [131]; si tratta della stessa scelta operata da molti editori online nell'ultimo anno che d'ora in poi verrà identificata come opzione del «doppio binario» oppure *pay or consent*.

14. *Ancora sulla base giuridica del legittimo interesse del titolare del trattamento (o di un terzo). Le recenti linee guida dell'EDPB*

L'*European Data Protection Board*, a ottobre 2024, si è espressa adottando le linee guida sul trattamento dei dati personali in virtù del legittimo interesse del titolare del trattamento o di un terzo [132]. Lo schema logico seguito dal Comitato ricalca quello dell'autorità di controllo austriaca del febbraio 2022.

Anche questo documento mette in risalto che il trattamento in virtù di tale base giuridica è legittimo allorché vengano soddisfatte le tre condizioni ormai già note: (i) il perseguimento di un legittimo interesse da parte del responsabile del trattamento o di un terzo; (ii) la necessità di questa base giuridica; (iii) il test di bilanciamento.

In relazione al primo punto, vengono identificati quei casi in cui la giurisprudenza della CGUE ha ritenuto legittimi gli interessi perseguiti [133] e opera una distinzione concettuale tra "finalità" del trattamento

---

[131] Una opzione che avevo già prospettato in G. PROIETTI, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in *Contratto e impresa*, vol. 32, n. 3, 2022, 880, spec. 918.

[132] EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, 8 ottobre 2024, consultabile al sito www.edpb.europa.eu.

[133] *Ivi*, 7-8, tra questi: la nota pronuncia sul caso, CGUE, C-131/12, 13 maggio 2014, *Google Spain*, eur-lex.europa.eu; in tema di garanzia del funzionamento continuo di accesso pubblico ai siti web CGUE, C-582/14, 19 ottobre 2016, *Breyer*, § 60, eur-lex.europa.eu; in tema di ottenimento dei dati personali di una persona che ha danneggiato la proprietà di qualcuno per poterla citare in giudizio per danni, CGUE, C-13/16, 4 maggio 2017, *Rīgas satiksme*, § 29, eur-lex.europa.eu; cosi come

di cui all'art. 5, lett. b), GDPR e il concetto di "interesse" di cui si discute.

La prima, rappresenta il motivo per il quale i dati vengono trattati, l'interesse, invece, costituisce il vantaggio più ampio che il responsabile del trattamento o un terzo può avere nell'intraprendere un determinato trattamento [134].

L'interesse perseguito deve soddisfare a sua volta tre condizioni perché sia considerato legittimo e possa costituire una valida base giuridica:

a) non deve essere contrario alla normativa europea o di uno Stato membro [135].

b) dev'essere espresso in modo chiaro e preciso. Il perimetro dell'interesse perseguito deve essere chiaramente identificato per permettere di essere adeguatamente bilanciato con gli interessi o i diritti e le libertà fondamentali dell'interessato [136].

CGUE, C-597/19, 17 giugno 2021, *M.I.C.M.*, § 108, eur-lex.europa.eu; sulla protezione della proprietà, della salute e della vita dei comproprietari di un edificio, CGUE, C-708/18, 11 dicembre 2019, *Asociația de Proprietari bloc M5A-ScaraA*, § 42, eur-lex.europa.eu; per il miglioramento dei prodotti, CGUE, C-252/21, cit., § 122, eur-lex.europa.eu.

[134] *Ivi*, 7, il Comitato riporta il caso di un responsabile del trattamento che ha *interesse* a promuovere i propri prodotti, e questo interesse può essere portato avanti trattando i dati personali per finalità di *marketing* diretto.

[135] *Ivi*, 8, l'EDPB riporta la pronuncia CGUE, C-621/22, 4 ottobre 2024, *Koninklijke Nederlandse Lawn Tennisbond*, § 49, eur-lex.europa.eu. Il Comitato riporta poi, a mero titolo esemplificativo, il caso di una impresa venditrice di sigarette elettroniche che intende promuovere i suoi prodotti mediante l'invio di e-mail promozionali ai propri clienti residenti in una determinata area europea. Per raggiungere tale finalità, raccoglie - e quindi tratta - i dati personali (come l'indirizzo e-mail e il nome) delle persone interessate. Benché il trattamento dei dati personali per finalità di marketing diretto possa talvolta considerarsi effettuato per un interesse legittimo, in circostanze di questo genere l'interesse non sarebbe "legittimo" perché contrastante con la normativa europea. Vale a dire, le comunicazioni commerciali con lo scopo o l'effetto diretto o indiretto di promuovere le sigarette elettroniche e i contenitori di liquido di ricarica sono vietate dalla direttiva UE sui prodotti del tabacco e dalle norme nazionali che la recepiscono.

[136] *Ibidem*. Il Comitato riporta l'esempio della istituzione di una organizzazione di "controllo del vicinato" la quale, "per il bene della società", ha intenzione di in-

c) dev'essere reale e attuale, non speculativo [137].

In questa fase di valutazione della legittimità dell'interesse, il Comitato fa poi riferimento al considerando n. 47 GDPR, il quale rileva un esempio di possibile indicatore senza che però possa costituire un automatismo [138]. Il considerando chiarisce che un «interesse legittimo potrebbe sussistere, ad esempio, quando esiste una relazione pertinente e appropriata tra l'interessato e il responsabile del trattamento, ad esempio quando l'interessato è un cliente o al servizio del responsabile del trattamento». Questo indicatore non pregiudica l'obbligo del responsabile di valutare e garantire tutte le tre condizioni richieste per avvalersi della base giuridica di cui all'art. 6, par. 1, lett. f, GDPR [139].

---

stallare un sistema di videosorveglianza in un determinato quartiere per monitorare eventuali attività criminali nella zona. Sebbene la protezione della proprietà, della salute e della vita possa in alcune circostanze essere considerata un interesse legittimo, l'interesse espresso dal responsabile del trattamento in riferimento al trattamento si presenta molto vago, poiché formulato in termini generali e senza far riferimento a questioni specifiche di sicurezza. Ciò impedisce di valutare la legittimità ed eventualmente proseguire il restante processo di valutazione in tre fasi previsto per l'art. 6, par. 1, lett. f, GDPR.

[137] *Ibidem*. Il Comitato riporta la pronuncia CGUE, C-708/18, 11 dicembre 2019, *Asociația de Proprietari*, cit, § 44. L'esempio che viene riportato riguarda una testata giornalistica che intende creare un database costituito dai vecchi iscritti che non hanno rinnovato l'abbonamento con la finalità di recuperare tali contatti in caso di lancio di una nuova rivista, nell'ambito del rapporto con i clienti. Al momento della creazione del database, però, il giornale non ha un concreto piano per sviluppare e lanciare una nuova rivista. In casi come questo l'interesse perseguito dal titolare del trattamento non può essere considerato reale e attuale, poiché il lancio di una nuova rivista è solo ipotetico. L'interesse non può essere considerato "legittimo".

[138] Sul considerando n. 47, in particolare nella parte in cui si fa riferimento al marketing diretto, sia consentito un rinvio a G. PROIETTI, *Algoritmi e interesse del titolare nel trattamento dei dati, cit.*, 909, laddove evidenziavo l'assenza di un simile automatismo, ossia che «avvalersi dell'indicazione (...) del legislatore senza una corretta, lecita e trasparente condotta nel trattamento dei dati potrebbe sfociare in un abuso. Ciò che viene indicato nel Regolamento europeo è una eventualità, non un automatismo».

[139] EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, cit., 8.

Sempre in riferimento alla prima condizione richiesta, il Comitato rileva che l'interesse perseguito dal responsabile del trattamento deve essere correlato alle attività effettive del responsabile stesso [140].

Però l'art. 6, lett. f), GDPR fa riferimento anche al perseguimento di interessi di terzi soggetti. Quindi, in alcuni casi, il trattamento dei dati personali può servire a perseguire contemporaneamente i legittimi interessi del responsabile del trattamento e quelli di un terzo. La legittimità dell'interesse di un terzo deve essere valutata secondo gli stessi criteri che si applicano agli interessi del responsabile del trattamento [141].

I contesti entro i quali gli interessi di un terzo possono essere legittimamente perseguiti per finalità di trattamento vengono, a titolo esemplificativo, così compendiati:

1) esercizio del diritto di difesa o pretese legali; 2) divulgazione di

---

[140] *Ivi*, 9-11. Viene riportata la giurisprudenza della Corte di Giustizia in virtù della quale è stato ritenuto che, sebbene la condivisione di informazioni con le forze dell'ordine per la prevenzione, individuazione e il perseguimento dei reati costituisca un interesse legittimo in quanto tale, non è di per sé in grado, in linea di principio, di costituire un interesse legittimo perseguito da un responsabile del trattamento la cui attività è essenzialmente di natura economica e commerciale, in quanto non sarebbe correlato alla sua attività (CGUE, C-252/21, cit., § 124).

[141] Il Comitato riporta il caso del tassista che aveva parcheggiato il suo veicolo sul ciglio della strada. La narrativa del caso prevede che mentre uno scooter passava accanto al taxi, il passeggero sul sedile posteriore del taxi apre la portiera urtando e danneggiando lo scooter. Il tassista viene identificato come responsabile dell'incidente e il proprietario dello scooter chiede la liquidazione del danno alla compagnia assicurativa del tassista che però imputa la responsabilità sul passeggero e quindi fornisce risposta negativa. A questo punto, il proprietario dello scooter si rivolge alla compagnia di taxi chiedendole informazioni sull'identità del passeggero per avviare il relativo procedimento civile e ottenere così il risarcimento dei danni. Il proprietario dello scooter, in questo caso, è un terzo che ha un interesse legittimo all'ottenimento dei dati riguardanti la persona che ha causato il danno. La comunicazione dei dati può, quindi, essere considerata effettuata al fine di perseguire gli interessi legittimi di un terzo.

dati per finalità di trasparenza; 3) ricerca scientifica, storica o di altro genere; 4) interesse pubblico generale o interesse di terzi [142].

La seconda condizione da soddisfare per ritenere lecito il trattamento in virtù di questa base giuridica si può sintetizzare nella "necessità" di ricorrere a tale base. In altri termini, occorre valutare se gli interessi non possano essere ragionevolmente perseguiti in modo parimenti efficace ricorrendo a un'altra base giuridica, meno restrittiva dei diritti e delle libertà degli interessati coinvolti [143]. Tale valutazione dev'essere posta in sinergia con il principio di minimizzazione dei dati previsto all'art. 5, lett. c), GDPR.

La terza condizione riguarda, come anticipato, il test di bilanciamento tra gli interessi in gioco [144]. In questa fase il responsabile deve identificare e descrivere i) gli interessi, i diritti e le libertà fondamentali degli interessati; ii) l'impatto del trattamento sugli interessati, tra cui la natura dei dati da trattare (particolare rilievo è chiaramente attribuito ai dati particolari, ossia sensibili), il contesto del trattamento [145] ed

---

[142] Il Comitato specifica che gli interessi di terzi, di cui all'art. 6, § 1, lett. f, GDPR non vanno confusi con gli interessi della comunità in generale (interessi pubblici generali), sebbene in alcuni casi gli interessi perseguiti da uno specifico responsabile del trattamento o da una specifica terza parte possano servire anche interessi più ampi; a tal proposito riporta un passaggio della sentenza Schufa della Corte di Giustizia europea, § 83.

[143] EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, cit., 12.

[144] Questa fase viene trattata in EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, cit., 13-15.

[145] L'EDPB nelle linee guida, 14, sottolinea che in riferimento al contesto il responsabile del trattamento deve tenere in considerazione vari aspetti, tra i quali: (i) la portata del trattamento e la quantità di dati personali da trattare (in termini di volume complessivo di dati, volume di dati per interessato e numero di interessati); (ii) lo status del responsabile del trattamento, anche nei confronti dell'interessato (ad esempio, un rapporto di lavoro dipendente richiederà probabilmente una valutazione diversa da quella relativa a un rapporto fornitore di servizi-cliente); (iii) se i dati personali da trattare sono combinati o meno con altra serie di dati; (iv) il grado di

eventuali ulteriori conseguenze del trattamento [146]; iii) le ragionevoli aspettative dell'interessato; iv) il bilanciamento finale dei diritti e degli interessi contrapposti, compresa la possibilità di ulteriori misure di attenuazione.

Questo test deve essere svolto sul presupposto che il responsabile del trattamento si sia già conformato ai principi e agli obblighi stabiliti nel GDPR. I diritti e le libertà fondamentali degli interessati che devono essere presi in considerazione comprendono il diritto alla protezione dei dati e alla *privacy*, così come altri diritti e libertà fondamentali, quali il diritto alla libertà e alla sicurezza, la libertà di espressione e di informazione, la libertà di pensiero, di coscienza e di religione, la libertà di riunione e di associazione, il divieto di discriminazione, il diritto di proprietà o il diritto all'integrità fisica e mentale che possono essere pregiudicati dal trattamento, direttamente o indirettamente.

L'impatto che il trattamento può avere sui diritti dell'interessato deve essere valutato obiettivamente. Può accadere che emerga in modo chiaro che un gran numero di interessati condivide gli stessi interessi e, perciò, una valutazione combinata di tali interessi può essere

---

accessibilità e/o pubblicità dei dati da trattare, e (v) lo status dell'interessato (ad esempio, soggetti vulnerabili o minori).

[146] *Ibidem*. I fattori che il responsabile del trattamento dovrebbe considerare includono: (i) potenziali decisioni o azioni future da parte di terzi che potrebbero basarsi sui dati personali da trattare da parte del responsabile del trattamento; (ii) la possibile produzione di effetti giuridici riguardanti l'interessato; (iii) l'esclusione o la discriminazione di persone; (iv) diffamazione o, più in generale, situazioni in cui vi è il rischio di danneggiare la reputazione, il potere negoziale o l'autonomia dell'interessato; (v) perdite economiche che potrebbero essere subite dall'interessato; (vi) esclusione da un servizio per il quale non esiste una reale alternativa, e (vii) i rischi per la libertà, la sicurezza, l'integrità fisica e mentale o la vita delle persone fisiche. Inoltre, il responsabile dovrebbe considerare i possibili impatti emotivi derivanti dal fatto che l'interessato perda il controllo sulle informazioni personali o si renda conto che queste sono state utilizzate in modo improprio o compromesse. Si deve poi considerare il c.d. *chilling effect* che può derivare dal monitoraggio/tracciamento continuo o dal rischio di essere identificati. Ad esempio, il monitoraggio continuo dell'attività online da parte di una piattaforma può dare la sensazione che la vita privata dell'interessato sia continuamente sorvegliata.

sufficiente (ad esempio, nel settore della videosorveglianza). Però, quanto più un trattamento è invasivo, tanto più devono essere considerate le circostanze specifiche.

Inoltre, il responsabile del trattamento non deve basare la propria valutazione degli interessi sulla presunzione che tutti gli interessati condividano gli stessi interessi quando ha - o dovrebbe avere - indicazioni concrete dell'esistenza di particolari interessi individuali o quando, da una prospettiva oggettiva, è semplicemente improbabile che tutti gli interessati abbiano gli stessi interessi ipotizzati dal responsabile. Ciò si riscontra in modo particolare nei rapporti tra datore di lavoro e dipendente.

Infine, il Comitato rammenta che, per le ipotesi in cui vengono identificati rischi elevati, il responsabile del trattamento è tenuto a considerare la necessità di procedere con una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 GDPR [147].

Nel test di bilanciamento viene attribuito un ruolo importante, come già visto in precedenza, alle ragionevoli aspettative dell'interessato [148]. Viene operata una distinzione tra la nozione di "ragionevole aspettativa" e ciò che si considera "prassi comune" in alcuni settori. Il fatto che alcuni tipi di dati personali siano comunemente trattati in un determinato settore non significa che l'interessato possa ragionevolmente aspettarsi tale trattamento. Le ragionevoli aspettative non dipendono esclusivamente dalle informazioni fornite agli interessati, sebbene l'omissione di informazioni contribuisca a sorprendere l'interessato di un determinato trattamento.

Quindi, vengono elencati alcuni elementi che possono fungere da parametro nella valutazione di tali ragionevoli aspettative:

(i) caratteristiche del rapporto con l'interessato o del servizio reso [149]; (ii) caratteristiche riguardanti l'interessato "medio". Il bilancia-

---

[147] *Ivi*, 16.

[148] *Ibidem*.

[149] Nell'ambito di tale elemento occorre analizzare: (a) l'esistenza stessa di un rapporto con l'interessato (ad esempio, si dovrebbe distinguere tra clienti e non

mento, infatti, deve prendere in considerazione l'interessato "medio", salvo che il trattamento non sia suscettibile di interessare gruppi diversi di interessati con caratteristiche diverse e tenere conto di:

(a) età dell'interessato (le aspettative ragionevoli dei minori possono essere diverse da quelle degli adulti), (b) la misura in cui l'interessato è un personaggio pubblico, e (c) la posizione (professionale) che l'interessato ricopre e il livello di comprensione e conoscenza del trattamento previsto che è probabile che abbia in un determinato contesto (ad esempio, il personale da coinvolgere in un processo di colloquio di lavoro spesso si aspetta che alcuni dei suoi dati personali vengano condivisi con i candidati).

Ad esito di questa terza fase riguardante il test di bilanciamento, nel caso in cui emerga che i diritti e le libertà dell'interessato prevalgono sui legittimi interessi perseguiti, il responsabile del trattamento può valutare l'introduzione di misure di attenuazione volte a limitare l'impatto del trattamento e raggiungere un equilibrio tra gli interessi e diritti in gioco. Tali misure non devono essere confuse con quelle che il responsabile è tenuto comunque ad adottare ai sensi del GDPR [150].

---

clienti), compresa la data di cessazione del rapporto, se esistente; (b) la prossimità del rapporto. Ad esempio, i casi in cui un responsabile del trattamento fa parte di un gruppo di aziende con un unico marchio rispetto a un gruppo di aziende che hanno solo legami economici sconosciuti al cliente medio. In quest'ultimo caso è meno probabile che l'interessato si aspetti ragionevolmente la condivisione dei dati tra le entità del gruppo; (c) il luogo e il contesto della raccolta dei dati (ad esempio, gli interessati potrebbero aspettarsi la presenza di telecamere a circuito chiuso in una banca, ma non nelle strutture sanitarie o nelle saune); (d) la natura e le caratteristiche del servizio (ad esempio, un cliente abituale e un semplice cliente potenziale che si è iscritto solo a una newsletter avranno aspettative ragionevoli diverse); (e) i requisiti legali applicabili al contesto in questione (ad esempio, i requisiti di riservatezza applicabili al rapporto in questione).

[150] Tra gli esempi di misure aggiuntive vengono menzionate, a titolo esemplificativo, la possibilità per l'interessato di esercitare il diritto di cancellazione anche quando non si applicano i motivi specifici elencati nell'art. 17, § 1, GDPR; la possibilità di esercitare il diritto di opposizione senza alcuna delle limitazioni di cui all'art. 21 GDPR; la possibilità di esercitare il diritto alla portabilità dei dati anche quando il trattamento si basa sull'art. 6, § 1, lett. f, GDPR.

Nella terza sezione delle linee guida viene poi illustrata la relazione tra il legittimo interesse e i diritti degli interessati. Viene menzionata la trasparenza e le informazioni che devono essere rese all'interessato, il diritto di accesso ai dati, il diritto di opposizione, di cancellazione, rettifica, il diritto di limitazione e l'aspetto delle decisioni automatizzate, inclusa la profilazione [151]. Per questi ultimi aspetti, indipendentemente dal fatto che il responsabile del trattamento intenda intraprendere una profilazione che porti a un processo decisionale automatizzato rientrante nell'art. 22 GDPR, vengono individuati alcuni elementi particolarmente rilevanti nei casi in cui si effettui l'esercizio del test di bilanciamento prima di invocare l'art. 6, par. 1, lett. f), GDPR come base giuridica:

(i) il livello di dettaglio del profilo; (ii) l'esaustività del profilo (se il profilo descrive solo un piccolo aspetto dell'interessato o se traccia un quadro più completo); (iii) l'impatto della profilazione (gli effetti sull'interessato); (iv) la possibile combinazione futura dei profili; e (v) le garanzie che assicurano l'equità, la non discriminazione e l'accuratezza del processo di profilazione.

15. *L'applicazione del legittimo interesse nel contesto del marketing diretto (secondo le linee guida EDPB)*

La sezione IV delle linee guida predisposte dall'EDPB è dedicata ai diversi contesti in cui può trovare applicazione la base giuridica di cui all'art. 6, lett. f), GDPR. Tra questi, un paragrafo è dedicato al *marketing* diretto, richiamato direttamente dal considerando n. 47 [152].

Il *marketing* diretto non è definito nel GDPR, ma la giurisprudenza della Corte di giustizia europea suggerisce che la pubblicità personalizzata potrebbe essere considerata una forma di *marketing* diretto [153].

---

[151] EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, cit., 19-25.

[152] *Ivi,* 30 ss.

[153] CGUE, 4 luglio 2023, C-252/21, cit., § 115.

Inoltre, la stessa Corte ha interpretato la nozione di comunicazione a fini di marketing diretto ai sensi della direttiva ePrivacy [154], strettamente legata al GDPR, e regola l'invio di comunicazioni di *marketing* diretto.

In particolare, la CGUE ha stabilito che, per valutare se una comunicazione è effettuata a fini di *marketing* diretto, occorre verificare se essa persegua uno scopo commerciale e sia rivolta direttamente e individualmente a un consumatore. La CGUE ha ritenuto irrilevante il fatto che la pubblicità sia indirizzata a un destinatario predeterminato e individualmente identificato o sia inviata in massa e in modo casuale a più destinatari. Ciò che conta è che vi sia una comunicazione a scopo commerciale che raggiunge direttamente e individualmente un consumatore. Si è ritenuto che la pubblicità consistente nella visualizzazione di *banner* pubblicitari, mascherati da e-mail, nelle caselle di posta elettronica private degli utenti di un servizio di posta elettronica è una forma di *marketing* diretto (anche se tale pubblicità non comporta l'invio di un'e-mail a un consumatore specifico).

Questa interpretazione può, in linea di principio, essere utilizzata analogamente per comprendere il significato di *marketing* anche nell'ambito del GDPR.

Viene sottolineato che il riferimento presente nel considerando n. 47 del GDPR non può costituire un automatismo e, per alcuni casi, può essere richiesta una base giuridica diversa, come il consenso, precludendo quindi l'uso del legittimo interesse.

In particolare, ai sensi della direttiva ePrivacy, l'invio di comunicazioni non richieste a fini di *marketing* diretto tramite e-mail, SMS, MMS e altri tipi di applicazioni simili può avvenire solo previo consenso da parte del singolo destinatario.

L'art. 5, par. 3, direttiva ePrivacy richiede anche il consenso per l'uso di tecniche di tracciamento, come la memorizzazione di cookie o l'accesso alle informazioni nell'apparecchiatura terminale dell'utente.

---

[154] CGUE, C-102/20, 25 novembre 2021, *StWL Städtische Werke Lauf a.d. Pegnitz*, § 47-50, eur-lex.europa.eu.

Pertanto, quando queste tecniche sono utilizzate nel contesto di attività di *marketing* diretto, questi requisiti di consenso devono essere rispettati. Perciò, il consenso costituisce la base giuridica appropriata sia per la memorizzazione e l'accesso alle informazioni già acquisite sul dispositivo dell'utente, sia per il successivo trattamento dei dati personali, precludendo di norma il ricorso all'art. 6, lett. f), GDPR.

L'EDPB dà poi atto del fatto che la direttiva e-privacy prevede anche alcune eccezioni al consenso imposto. Ad esempio, un'eccezione al requisito del consenso è consentita dall'art. 13, par. 2, della direttiva ePrivacy quando i dati elettronici di contatto sono stati ottenuti legittimamente - ossia, quando sono stati ottenuti in conformità al GDPR - dai propri clienti nel contesto della vendita di un prodotto o di un servizio.

In questo ultimo caso, il soggetto che ha ottenuto questi dati elettronici di contatto dai propri clienti può utilizzarli per il *marketing* diretto di propri prodotti o servizi simili a condizione che i clienti possano opporsi in modo chiaro e distinto a tale uso, in modo semplice e gratuito, e che siano stati informati di conseguenza al momento della raccolta iniziale dei dati di contatto e in occasione di ogni messaggio, nel caso in cui il cliente non abbia rifiutato tale uso.

Viene ancora sottolineata l'intersezione tra la disciplina del GDPR e la direttiva ePrivacy. Viene specificato che nei casi in cui il trattamento dei dati personali rientra nell'ambito di applicazione materiale di entrambi gli atti legislativi, come il caso del *marketing* diretto tramite mezzi di comunicazione elettronici che non comporta il trattamento di dati personali (si pensi al *marketing* diretto rivolto a persone giuridiche) l'unica disciplina è quella della direttiva ePrivacy. Però, quando è in gioco il trattamento dei dati personali, la direttiva ePrivacy dev'essere considerata come *lex specialis* nella misura in cui disciplina tale trattamento.

Per contro, le comunicazioni a scopo di *marketing* diretto che non sono fornite con mezzi di comunicazione elettronici (ad esempio, una lettera) non rientrano nell'ambito di applicazione materiale della direttiva ePrivacy e non richiedono il consenso ai sensi di tale direttiva. Infine, i responsabili del trattamento dovrebbero valutare anche l'ambito

di applicazione delle norme nazionali di attuazione della direttiva ePrivacy, le quali possono occasionalmente imporre requisiti di consenso che vanno al di là di quelli stabiliti dalla direttiva (ad esempio, per quanto riguarda il *marketing* diretto verso i professionisti).

Ogni valutazione deve essere comunque rimessa alle circostanze del caso concreto. È essenziale che i responsabili del trattamento verifichino se l'interesse di *marketing* perseguito non possa essere ragionevolmente conseguito in modo altrettanto efficace con altri mezzi meno restrittivi delle libertà e dei diritti fondamentali degli interessati, in particolare i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti dagli artt. 7 e 8 della Carta, e sia garantito e rispettato il principio di "minimizzazione dei dati" sancito dall'art. 5, par. 1, lett. c), GDPR. I responsabili del trattamento sono chiamati alla implementazione di garanzie e misure di attenuazione appropriate, come l'utilizzo di tecnologie per il miglioramento della privacy.

Il Comitato rileva come sia improbabile che il test di bilanciamento produca un esito positivo nei casi di pratiche intrusive di profilazione e di tracciamento per finalità di *marketing*, come quelle che prevedono il tracciamento delle persone su più siti web, luoghi, dispositivi o servizi. Per contro, è più agevole giustificare un esito positivo per quelle attività di *marketing* meno invasive, come la campagna pubblicitaria consistente nell'invio della stessa comunicazione commerciale (ad esempio, un catalogo di prodotti) a tutti i clienti esistenti che hanno già acquistato prodotti simili a quelli pubblicizzati.

Qualora i dati personali siano trattati per finalità di *marketing* diretto, l'interessato ha uno specifico diritto di opporsi a tale trattamento ai sensi dell'art. 21, par. 2, GDPR. A differenza della regola generale sancita nel primo paragrafo dell'art. 21 GDPR, nel caso del *marketing* diretto il diritto è incondizionato e prescinde dalla base giuridica invocata dal responsabile del trattamento. Non è richiesto che l'interessato fornisca una motivazione quando si oppone poiché lo scopo dell'obiezione è irrilevante, e non è necessario alcun "bilanciamento di interessi" per valutare il merito di un suo accoglimento.

Per completare l'analisi della base del legittimo interesse, merita di

essere esaminata la già cennata decisione della CGUE sul caso IAB Europe.

16. *Il legittimo interesse nella recente decisione IAB Europe (CGUE - C-604/2022)*

Nel precedente § 4 si è vista la recente decisione della Corte di Giustizia europea nel caso IAB Europe per quanto riguarda il profilo della definizione di dato personale. Però, con questa decisione la Corte ha affrontato anche il tema della base giuridica del legittimo interesse riprendendo l'analisi che ha effettuato l'Autorità di controllo il cui provvedimento era stato impugnato [155].

Nel caso IAB Europe, l'Autorità di controllo ha rilevato la sussistenza della prima condizione richiesta per la base giuridica in esame poiché lo scopo di acquisire l'approvazione e le preferenze degli utenti per garantire e poter dimostrare che questi hanno validamente acconsentito o che non si siano opposti al trattamento dei loro dati personali a fini pubblicitari può considerarsi effettuato per un interesse legittimo. La possibilità di memorizzare le preferenze degli utenti è una parte essenziale del TCF e l'Autorità ha rilevato che ciò avviene conformemente all'interesse (legittimo) della società e dei terzi coinvolti, come i fornitori di tecnologia pubblicitaria che partecipano alle operazioni [156].

Per la seconda condizione, occorre domandarsi se quel risultato possa essere raggiunto con altri mezzi senza trattare i dati personali o senza un trattamento inutilmente oneroso per gli interessati. Occorre, nel caso concreto, verificare se i dati personali inclusi nella Stringa TC siano circoscritti a quanto strettamente necessario per acquisire il consenso, le opposizioni e le preferenze di un utente specifico (principio di minimizzazione). L'Autorità rileva, nella decisione in esame,

---

[155] Il citato provvedimento dell'Autorità belga lo affronta a partire dal § 409, 88.
[156] *Ivi*, § 413-415.

che le informazioni trattate in una "TC String" sono limitate ai dati strettamente necessari per raggiungere lo scopo prefissato e, pertanto, la condizione è soddisfatta [157].

Nella valutazione dell'esistenza della terza condizione, viene posto in risalto l'elemento delle ragionevoli aspettative dell'interessato (considerando n. 47 GDPR). Secondo l'Autorità, è necessario stabilire se l'interessato possa ragionevolmente aspettarsi, al momento e nel contesto della raccolta dei dati personali, che il trattamento possa avvenire per una specifica finalità. L'Autorità ritiene non sussistente questa condizione poiché agli utenti non viene offerta alcuna opzione per opporsi completamente al trattamento delle loro preferenze nel contesto del TCF. Infatti, a prescindere dalla scelta effettuata, il CMP genera la stringa TC prima di collegarla all'ID utente unico dell'utente attraverso un *cookie euconsent-v2* collocato sul dispositivo finale dell'interessato di cui quest'ultimo non viene informato [158].

Nel provvedimento, inoltre, si legge che viene valutata anche la gravità della violazione dei diritti e delle libertà dell'interessato come primario elemento della valutazione di un legittimo interesse conforme al GDPR. È perciò necessario considerare la natura dei dati personali, in particolare la loro natura potenzialmente sensibile, nonché la natura e le modalità specifiche del loro trattamento, in particolare il numero di persone che accedono e le modalità di acquisizione di tale accesso. Nel caso concreto, viene evidenziato, in termini negativi, l'elevato numero di organizzazioni partecipanti che possono accedere alla stringa, oltre al ridotto controllo da parte degli interessati sulla natura e sulla portata del trattamento dei loro dati personali da parte di tali organizzazioni [159].

Dunque, esaurita anche l'analisi del legittimo interesse, può essere ripresa quella distinzione teorica finora lasciata in sospeso, ossia la tesi

---

[157] *Ivi*, § 416-418.
[158] *Ivi*, § 419-422.
[159] *Ivi*, § 423.

patrimonialistica che si contrappone a quella personalistica nelnl'ambito del trattamento dei dati.

17. *La teoria patrimonialistica e personalistica sul trattamento dei dati personali*

Il GDPR, all'art. 1, dopo aver precisato l'obiettivo di stabilire norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e norme relative alla circolazione di tali dati, sancisce che il diritto alla protezione dei dati personali è un diritto fondamentale. Con il paragrafo 3, invece, viene stabilito 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 [160]. La tutela della *privacy* pur dovendo essere compresa nell'ambito dei diritti della personalità, deve coniugarsi con l'esigenza della libera circolazione; le due logiche sarebbero di per sé in una posizione antitetica perché l'esclusività dei diritti assoluti mal si concilia con la funzione circolatoria [161].

---

[160] Per completezza è necessario precisare la premura del legislatore europeo, il quale intende garantire una libera circolazione anche dei dati non personali all'interno del mercato unico europeo prevedendo un espresso divieto di localizzazione nel Regolamento (UE) 2018/1807. L'art. 4, dedicato alla libera circolazione dei dati all'interno dell'Unione, al § 1, co. 1, prevede che «gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità».

[161] M. FRANZONI, *Lesione dei diritti della persona,* cit. 7-12. L'A. sottolinea che l'utilizzo dei *big data* hanno cambiato il modo di considerare il bilanciamento che tradizionalmente viene effettuato per risolvere un conflitto tra più diritti della personalità. Aggiunge poi che «sta mutando un certo modo di apprezzare i diritti della personalità in conseguenza dell'impiego dell'intelligenza artificiale nella rete. Non sta cambiando il sistema di valori sui quali poggiano i diritti della personalità: più verosimilmente, sta cambiando la sostanza di questi diritti. (...) Il punto è che l'utilità sociale prodotta dal corretto funzionamento di un algoritmo di machine learning supera di gran lunga l'interesse di colui i cui "frammenti di vita privata" vengono processati, sicché anche lui può trarre un vantaggio, spesso inconsapevole (...)».

Dunque, si può dire che è lo stesso tenore dell'art. 1 GDPR a dar vita a quel dibattito sulla natura del dato personale, provocando così quella scissione teorica tra modello patrimonialistico [162] e modello personalistico [163].

Quindi, il GDPR ha apportato una importante novità in tema di bilanciamento tra diritti e libertà. Il par. 3 dell'art. 1 GDPR «fornisce un'indicazione di principio volta a cristallizzare una relazione perpetua tra una libertà "fondamentale" (quella di circolazione dei dati) ed un diritto fondamentale (quello alla protezione dei dati), affermando implicitamente che la prima, rispetto alla seconda, costituirebbe una "prerogativa assoluta"» poiché non soggetta a limitazione [164].

Ciò è dovuto al fatto che «l'economia dei beni immateriali o dematerializzati, al cui interno ci si muove quando si riflette sui *big data*, segue logiche molto diverse da quelle dell'economia reale». Il mondo digitale costituirebbe un universo parallelo, che funziona con regole necessariamente proprie e non riflesse da quelle del mondo reale.

[162] J. Litman, *Information Privacy/Information Property*, in *SSRN Scholarly Paper* n. ID 218274, Rochester, NY, 2000.

[163] G. Mirabelli, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali,* cit., 323; incentrato sull'aspetto personalistico, senza negare il fenomeno circolatorio del dato e un consenso di tipo negoziale, S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 82. Oltre ad un valore puramente commerciale, merita menzione un ulteriore aspetto del dato personale, ovvero il collegamento ad un suo valore amministrativo, definito «come misura della capacità per l'amministrazione di estrarre informazioni utili al perseguimento di una certa finalità pubblicistica e univocamente riferibili al soggetto che abbia "prodotto" il dato» in questione; in questo senso, legato agli scopi dei sistemi di social scoring, si veda G. Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale di diritto amministrativo*, n. 3, 2021, 325.

[164] F. Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?,* in *Contratto e Impresa,* vol. 34, n. 1, 2018, 190. L'A., tuttavia, rileva che l'applicazione della clausola di limitazione generale prevista dall'art. 52, par. 1, della Carta UE non può essere applicata nel modo in cui ha operato il legislatore europeo mediante l'art. 1, par. 3, del GDPR, ovvero demandando al legislatore "ordinario", in via generale ed astratta, la scelta in ordine al posizionamento gerarchico dei diritti e delle libertà fondamentali reciprocamente confliggenti. Dunque, la disposizione in questione si presterebbe ad una censura con una pregiudiziale di validità ai sensi dell'art. 267, par. 1 lett. b, TFUE.

L'originaria concezione di *privacy* si improntava su un modello dominicale in cui tutti i beni del soggetto proprietario erano esclusivi e sotto il suo pieno controllo (*property privacy*), mentre il modello attuale si fonda su una prospettiva dinamica (*personality privacy*), volta a realizzare l'identità digitale dell'individuo interessato [165].

In linea generale, i dati personali sono concepiti come un *asset* strategico con peculiari caratteristiche tali da attribuire un vantaggio concorrenziale a chi ne ha la disponibilità esclusiva. Rimarrebbe tuttavia da definire in modo più specifico la loro natura, così come la tipologia e la genesi dei diritti vantati su di essi [166] in una realtà socioeconomica in cui il loro destino risulta sempre più incentrato sulla circolazione [167].

---

[165] V. RICCIUTO, *L'equivoco della privacy,* cit., 60.

[166] A. VACCHI, *Intelligenza artificiale, impresa e nuovi modelli di business*, in *XXVI lezioni di diritto dell'intelligenza artificiale,* cit.*,* 366. L'A. in particolare, si focalizza sull'ipotesi in cui una impresa fornitrice si 'arricchisca' mediante l'acquisizione di dati provenienti dall'impresa committente consentendo così un miglioramento della propria IA e un maggior *know-how.* Tale scenario, come sottolineato, produce ripercussioni sia in materia contrattuale, sia in ambito concorrenziale.

[167] Per una ricostruzione del dibattito sulla concezione meramente personalistica del dato personale, contrapposta ad una logica patrimonialistica, si veda B. PARENZO, *Sull'importanza dl dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali "gratuiti"*, in *Diritto di famiglia e delle persone*, vol. 38, n. 2, 2021, 1462-1470. L'A. sostiene che sebbene non possa essere concepita una cessione definitiva della titolarità del *bene* dato personale «ne è invece pensabile una "cessione in godimento", la quale pure, però, in considerazione della peculiare natura identitaria del dato medesimo, non può essere dotata del crisma della definitività: l'interessato che deduce in contratto, in funzione di scambio, la (sola) "utilizzabilità" del dato deve sempre poterne tornare nell'esclusivo godimento; di qui, infatti, la previsione di un diritto di revocare "in qualsiasi momento" il consenso al trattamento dei dati personali di cui all'art. 7, par. 3, GDPR (...)». Autorevole dottrina conferisce valore commerciale ai dati personali, assimilandoli ai beni in senso giuridico e in quanto tali suscettibili di essere oggetto di disposizione mediante contratto, G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, Torino, Utet, 2011, 38; V. ZENO-ZENCOVICH, *Una lettura comparatistica della L. 675/96 sul trattamento dei dati personali*, in *Trattamento dei dati e tutela della persona*, cit., 169; si veda altresì G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione*

Perciò, da un lato, secondo una tesi *patrimonialistica*, in una società sempre più *data driven,* i dati acquisiscono un valore di natura patrimoniale, tanto da segnare il passaggio da una dimensione *morale* ad una *negoziale*[168], dall'altro lato, invece, secondo una logica personalistica, si esclude la possibilità di uno scambio tra dati personali e un determinato servizio[169]. I fautori di quest'ultima teoria sostengono che il dato personale costituisce l'estrinsecazione dell'identità e della personalità dei soggetti; esso rientrerebbe nell'alveo dei diritti fondamentali, intrasmissibili e quindi indisponibili, impendendone la commercializzazione[170].

---

dei servizi in rete, in *Rivista trimestrale diritto e procedura civile*, 2018, 411-440. Colui il quale acquisisce il consenso altrui al trattamento dei dati personali, non acquista il consenso dell'avente diritto, bensì le specifiche informazioni, A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, Giuffrè, 2007, 71.

[168] G. D'Ippolito, *Commercializzazione dei dati personali: dato personale tra approccio morale e negoziale*, in *Diritto dell'informazione e dell'informatica*, vol. 41, n. 3, 2020, 634; si veda poi G. Pitruzzella, *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, n. 1, 2016, 16, secondo cui non v'è una contrapposizione intrinseca tra il mercato e i diritti fondamentali; l'obiettivo deve essere volto a definire le regole che consentono al mercato un funzionamento efficiente ed equo, soddisfacendo gli interessi degli individui, dell'economia e della società mediante l'innovazione, la fiducia e l'empowerment degli utenti.

[169] G. Alpa, *L'intelligenza artificiale. Il contesto giuridico*, Modena, Mucchi editore, 2021, 73, rileva come si stiano consolidando due differenti letture del testo del GDPR: un indirizzo garantista e un indirizzo liberista. L'A. ritiene che «il diritto alla privacy digitale non sia negoziabile, che i dati personali non siano un bene che si immette sul mercato per una circolazione appropriativa, che non vi sia "scambio" tra dati e servizi, ma piuttosto consenso al trattamento (cioè autodeterminazione dell'avente diritto e non un consenso avente natura negoziale) con acquisizione gratuita di servizi. In altri termini, che non si debba o possa fare un contratto di scambio tra dati personali e servizi, in quanto certi dati personali non si possono negoziare perché così facendo si lederebbe la dignità della persona e altri dovrebbero comunque implicare la salvaguardia di un diritto morale; in più, non si potrebbe garantire l'esclusività della cessione dei dati, perché i destinatari dei dati sono molteplici ed essi non si possono cambiare in quanto identificativi sempre della medesima persona che li trasferisce».

[170] S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei*

L'approccio europeo originariamente adottato era quello di inquadrare i dati personali nell'ambito dei diritti della personalità [171]. Il dirit-

dati personali, in *Rivista critica di diritto privato*, 1997, 583; si veda la ricostruzione del tema operata da V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Diritto dell'informazione e dell'informatica*, vol. 34, n. 4-5, 2018, 698, il quale rileva come sia necessario «prendere atto che l'idea di privacy che discende dal modello comunitario è un quid novi, che il dibattito relativo all'indisponibilità dei diritti della personalità appare superato ed obsoleto innanzi ad un nuovo diritto le cui sfaccettature non possono cogliersi solamente con le lenti della dottrina italiana ma facendo necessariamente i conti con il processo di integrazione europea che, non certo insensibile alle istanze personaliste, si sviluppa e nasce attorno al fenomeno economico». L'A. successivamente, a pagina 713, riporta l'esempio normativo della direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale la quale al par. 1 dell'art. 3, prevede la sua applicazione «ai contratti in cui il fornitore fornisce contenuto digitale al consumatore, o si impegna a farlo, e in cambio del quale il consumatore corrisponde un prezzo oppure fornisce attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato». Tuttavia, il testo definitivo della disposizione, confluito nella direttiva UE 2019/770, risulta differente, stabilendo che «la presente direttiva si applica a qualsiasi contratto in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si impegna a corrispondere un prezzo. La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti». Sulle differenti tendenze che si presentano invece nell'esperienza nordamericana, suddivise in liberista, quella che trasforma i dati in diritti assimilabili al *copyright* e quella garantista, si veda G. ALPA, *Il diritto di essere se stessi*, Milano, La nave di Teseo, 2021, 264.

[171] In letteratura v'è chi addirittura ritiene che molte tesi di giuristi che si focalizzano sulla persona costituiscano astratte e inutili proclamazioni che si traducono in ipocrisie. In tal senso F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giurisprudenza italiana*, n. 12, 2019, 2799, secondo il quale su questo tema «si gioca una battaglia culturale di carattere epocale: quella dell'attribuzione sociale di valore a entità prive di un preciso valore economico, per lo meno

to alla tutela dei dati personali tra i diritti fondamentali fa sì che venga attribuito valore al carattere non patrimoniale e indisponibile dei diritti della personalità. Un orientamento di questo genere non concepisce la possibilità di cedere i diritti di cui si discute, i quali rimangono indissolubilmente legati al soggetto titolare [172]. La questione sulla patrimonializzazione dei dati personali, come si è visto, quindi, è già da tempo oggetto di un acceso dibattito dottrinale [173].

In questo dibattito è stato rilevato che una tutela di tipo proprietario sarebbe antitetica rispetto al fenomeno della circolazione. Invero, in una concezione dominicale, dal momento della sua circolazione, l'interessato perderebbe ogni signoria sul bene (dato) ceduto, ossia, «ogni possibilità di controllarne il trattamento, ogni opportunità di far prevalere la propria volontà su quella del nuovo proprietario» [174]. Una simile concezione, perciò, finirebbe per negare il fenomeno circolatorio e ne impedirebbe la disponibilità [175].

Invece, secondo una contrapposta impostazione, favorevole alla circolazione del dato personale, essa avviene per mezzo di negozi dispositivi, costitutivi di un diritto a trattare i dati personali. Con l'operazione in questione l'interessato non aliena i propri dati, ma conserva

---

per chi le produce; quella della creazione di un'alternativa al mercato, dimostrando che quest'ultimo non è l'unico dispositivo sociale di conferimento di un valore misurabile». Secondo l'A., il GDPR non sembra far parte della battaglia in questione.

[172] A. Stazi, F. Corrado, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica,* cit., 450-455.

[173] Sul punto, ancora, si veda M. Cocuccio, *Dimensione "patrimoniale" del dato personale e tutele risarcitorie*, in *diritto di famiglia e delle persone*, vol. 41, n. 1, 2022, 230; S. Senigaglia, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit., 760; A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto,* Napoli, Edizioni scientifiche italiane, 2017; C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, cit., 37 ss.; E. Tosi, *Diritto privato delle nuove tecnologie digitali*, Milano, Giuffré, 2021, 169-177.

[174] V. Ricciuto, *L'equivoco della privacy,* cit. 62.

[175] *Ibidem*. Dunque, si negherebbe la qualificazione del dato come bene giuridico e si escluderebbe lo stesso valore economico e il fondamento stesso dell'intero fenomeno della società dell'informazione e dell'economia digitale.

su di loro ogni forma di controllo e prerogativa pur dinanzi al trattamento che altri soggetti esercitano [176].

Secondo una concezione di questo genere, pertanto, non si discute di proprietà del dato verso chi lo genera, bensì di permettere il suo sfruttamento economico riconoscendo al loro titolare la possibilità di assoggettarli al trattamento per finalità commerciali, rilasciando il consenso anche dietro compenso, sotto forma di utilità come il servizio digitale [177]. Ciò senza che venga negata la natura propria dei più tradizionali diritti della personalità [178]. Perciò, secondo questa interpretazione, i dati personali non costituiscono l'oggetto di uno scambio in senso giuridico e occorrerebbe abbandonare l'espressione «scambio servizi/dati» [179]. Invero, ciò che viene "acquistato" dal professionista sarebbe il diritto a trattare i dati personali dell'interessato per finalità estranee all'esecuzione della fornitura [180].

La tesi che abbraccia e riconosce il valore (di fatto) economico ai dati personali, alle preferenze dei consumatori e ad altri contenuti, sembrerebbe preponderante in seno ad alcune istituzioni come l'AGCM [181]. In particolare, con il provvedimento del 7 dicembre 2018, quest'ultima ha riconosciuto il valore economico e commerciale

---

[176] *Ibidem*. Si veda anche F. BRAVO, *il diritto a trattare dati personali nello svolgimento dell'attività economica*, Milano, Cedam, n. 3, 2018, 22.

[177] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali,* cit., 57.

[178] *Ibidem*. Secondo l'A., per valutare le penetranti disuguaglianze di fatto tra i soggetti del rapporto non si dovrebbe tanto guardare al carattere formale del soggetto agente, ma al tipo di attività svolta, conferendo rilievo alle modalità di esercizio del potere e controllo. Perciò questi scambi vanno sussunti nella disciplina del contratto.

[179] C. SOLINAS, *La circolazione dei dati personali nell'ottica dello scambio tra diritti*, in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali,* in V. RICCIUTO, C. SOLINAS (a cura di), III., Milano, n. 13, 2022, 109, spec. 130.

[180] *Ivi*., 131. Secondo l'A., «l'interessato non trasferisce la titolarità dei dati personali, non si spoglia del diritto fondamentale alla protezione dei dati personali, bensì costituisce in capo al titolare un ben preciso diritto al trattamento dei dati personali».

[181] G. D'IPPOLITO, *Commercializzazione dei dati personali,* cit*.,* 640. Secondo l'A. tale

dei dati, rilevando nel caso di specie una forviante enfatizzazione da parte del titolare del trattamento (Facebook) sulla gratuità dell'utilizzo della piattaforma. La vicenda, definita in sede giurisdizionale, è culminata in due importanti pronunce che oggi ne costituiscono il riferimento principale [182].

Entrambe le sentenze riconoscono lo sfruttamento per fini commerciali dei dati personali da parte dei *social network*, costituendo la materia prima di un processo produttivo che confluisce nella profilazione degli utenti [183]. Tuttavia, mentre i giudici del TAR si sono spinti sino a ritenere il dato personale come oggetto di compravendita, dal canto suo il Consiglio di Stato ha delineato il carattere della patrimonializzazione nell'ambito dello sfruttamento del dato personale messo a disposizione dall'interessato in favore di un soggetto che lo utilizzerà anche per fini commerciali [184]. La pronuncia di primo grado è stata anche una occasione per la dottrina più favorevole alla patrimonializzazione del dato personale per ribadire la propria tesi [185].

Su questa stessa linea è sostanzialmente intervenuta anche la più recente, e già citata, sentenza della Corte di Giustizia europea del 4 luglio 2023.

La Corte ha definito il quadro di raccolta e di trattamento dei dati da parte di Meta, ossia, un sistema basato sul contratto d'uso a cui gli

---

fenomeno della commercializzazione dei dati personali sarebbe accolto anche dalla giurisprudenza del Tar Lazio (TAR Lazio, Sez. I, 10 gennaio 2020, n. 261).

[182] Il riferimento è alla sentenza del Tar Lazio, Sez. I, 10 gennaio 2020, n. 261, in *Foro amm.*, 2020, 99 e alla successiva sentenza del Consiglio di Stato, 29 marzo 2021, n. 2631, in *Foro it.*, n. 3, 2021, 325. Il Consiglio di Stato ha rilevato come i dati personali costituiscono «patrimonio di rilevante valore economico».

[183] In questo senso, B. Parenzo, *Sull'importanza dl dire le cose come stanno,* cit., 1457 ss.

[184] *Ibidem*.

[185] Si veda in tal senso C. Solinas, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in *Giurisprudenza italiana*, n. 2, 2021, 321 e ss. secondo cui la pronuncia del TAR suggella la possibilità di coniugare le esigenze di tutela della persona con gli strumenti del diritto patrimoniale. Il fenomeno (della patrimonializzazione dei dati personali, n.d.r.) viene ritenuto inevitabile e in crescita esponenziale.

utenti aderiscono tramite l'attivazione del pulsante «Iscriviti» e con il quale accettano le condizioni generali stabilite dalla piattaforma. Per il trattamento dei dati personali, specifica la sentenza, le condizioni generali rinviano alle regole sull'uso dei dati e dei marcatori (*cookies*) in virtù delle quali vengono raccolti dati riferiti agli utenti e ai loro dispositivi, relativi alle loro attività all'interno e all'esterno del *social network*, mettendoli in relazione con gli *account* Facebook degli utenti interessati.

Tali ultimi dati, relativi alle attività al di fuori del *social network* (dati off Facebook), riguardano le informazioni sulla consultazione di pagine Internet e di applicazioni di terzi che sono collegate a Facebook attraverso interfacce di programmazione, oltre ai dati riguardanti l'utilizzo degli altri servizi online appartenenti al gruppo Meta [186]. Viene, quindi, dettagliato un modello di profilazione degli utenti con dati che vengono raccolti all'interno e all'esterno della piattaforma per essere combinati tra loro anche con diversi altri *account*. La Corte rileva, perciò, come l'accesso ai dati personali e il loro sfruttamento rivesta una fondamentale importanza nell'economia digitale. La sua pregnanza è illustrata dal modello economico ricordato, ossia strutturato attraverso il finanziamento che avviene con la commercializzazione di messaggi pubblicitari personalizzati in base alle profilazioni degli utenti [187].

18. *Il trattamento dei dati come condizione necessaria per accedere al servizio digitale: le operazioni di tying*

Si è visto come si possono verificare situazioni in cui un'impresa offra un determinato servizio richiedendo all'utente la prestazione del consenso al trattamento dei dati personali come condizione per

[186] Sentenza CGUE, C-252/21, cit., § 28.
[187] *Ivi*, § 50.

l'accesso [188]. Queste sono le cc.dd. operazioni di *tying* [189]. In questi casi si genera uno scambio tale da rendere la trasmissione dei dati personali il corrispettivo della prestazione offerta, costituito da quei dati personali non necessari per l'erogazione del servizio richiesto, ma indispensabili per diversi fini come il *marketing* o la profilazione dell'utente [190]. È una operazione che si differenzia dal *pay or consent*.

---

[188] L'offerta di servizi *online* apparentemente gratuita che in realtà prevede come corrispettivo lo sfruttamento dei dati personali è anche denominata "trappola del dono". In questo senso si veda A. De Franceschi, *Il pagamento mediante dati personali*, in *I dati personali nel diritto europeo*, cit., 1387 ss. Sul tema del servizio come gratuito inteso come "slogan per gli allocchi" si veda G. Resta, V. Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi di rete*, in *Rivista Trimestrale di diritto e procedura civile*, n. 2, 2018, 414.

[189] Alcuni hanno rilevato che astrattamente queste operazioni in cui l'accesso ad un bene o servizio viene subordinato alla prestazione di un consenso finalizzato ad un trattamento non necessario sarebbero vietate dall'art. 101 par. 1 lett. e) TFUE perché potrebbero impedire, restringere o falsare il gioco della concorrenza. C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in C*ontratto e impresa*, vol. 35, n. 2, 2020, 882.

[190] S. Thobani, *Il mercato dei dati personali,* cit., 132. L'A. nel suo contributo a pag. 133 cita casi in cui l'AGCM (provvedimenti nn. 10276, 10277, 10278 e 10279 del 20 dicembre 2001) ha sanzionato la pratica di pubblicizzazione di un servizio come gratuito a fronte di un consenso dell'utente al trattamento dei propri dati per la ricezione di e-mail pubblicitarie. L'autorità ha quindi configurato l'obbligo facente capo al destinatario di tollerare l'invio di posta elettronica di pubblicità basate sul proprio utilizzo del web come una vera e propria prestazione passiva, non indifferente ai fini della valutazione della convenienza dell'offerta. Inoltre, l'A., successivamente, opera un collegamento con la direttiva n. 770 del 2019 la quale all'art. 3, par.1, prevede la sua applicazione non solo quando viene offerto al consumatore un servizio o contenuto digitale in cambio di un prezzo, ma anche quando l'operatore fornisce o si impegna a fornire contenuto digitale o servizio digitale e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico. L'intenzione è quella di equiparare le tutele a favore del consumatore a prescindere dalla modalità di pagamento del servizio, ossia se mediante denaro o dati personali. Sul tema si veda altresì M. Franzoni, *Lesione dei diritti della persona e tutela della privacy*, in *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., 344, il quale discutendo della funzionalità del consenso nell'epoca delle nuove tecnologie rileva come il consenso «al tratta-

Secondo parte della dottrina, dalla lettura dell'art. 7, par. 4, GDPR non potrebbe essere ricavato alcun divieto generalizzato alle operazioni di *tying*, non essendo vietato subordinare l'esecuzione di un contratto alla prestazione del consenso al trattamento dei dati [191]. Su questo tema è intervenuta anche la giurisprudenza di legittimità con una pronuncia del 2018 [192]. Questa decisione è originata da una vicenda in cui un soggetto che offriva il servizio di *newsletter* senza alcun corrispettivo monetario e subordinava l'accesso alla prestazione del consenso al trattamento dei dati personali. Nell'ambito di tale *policy privacy* era previsto che l'utente avrebbe ricevuto comunicazioni promozionali e informazioni commerciali da parte di terzi. La Cassazione, benché abbia accolto il ricorso del Garante per la Protezione dei Dati Personali per motivazioni legate a un consenso che nel caso di specie non è stato ritenuto "specifico", ha d'altra parte enunciato un principio fondamentale, legato proprio alle operazioni di *tying*. I giudici hanno sostanzialmente ammesso la possibilità di subordinare l'erogazione di un servizio alla prestazione del consenso al trattamento dei dati personali non necessario a seconda della natura *infungibile* e *irrinunciabile* del servizio stesso.

In altri termini, sarebbe possibile per il gestore di un portale riguardante 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».

La Suprema Corte aggiunge, quindi, che l'ordinamento non vieta lo scambio di dati personali, ma esige che lo scambio sia frutto di un

---

mento dei propri dati, "necessario" per accedere a beni o servizi, se è finalizzato ad un trattamento non necessario e scollegato dalla prestazione primaria e principale, diventa strumento di scambio di utilità, per ottenere le quali l'interessato può essere disposto a perdere persino la propria dignità».

[191] S. THOBANI, *Il mercato dei dati personali,* cit., 140.

[192] Cass. civ., 02 luglio 2018, n. 17278, *Giur. It.*, n. 3, 2019, 530, con nota di S. THOBANI.

consenso pieno e non coartato. Va da sé che la decisione assunta dalla Corte deve essere modellata a seconda del significato che viene attribuito alla natura infungibile o irrinunciabile del servizio offerto che non viene definito in modo univoco [193].

In letteratura, sebbene sia sempre più prevalente una tesi a favore della patrimonializzazione dei dati personali [194], come si è visto, i percorsi seguiti sono differenti e strutturati su varie impostazioni. Si può individuare una prima divisione tra modelli ipotetici in cui la *cessione* del dato personale costituisce la prestazione principale, anche a fronte di un corrispettivo monetario e quella in cui, invece, la *cessione* del dato personale costituisce una prestazione che l'interessato esegue al fine di poter accedere a diversi beni o servizi [195]. Perciò, una volta superati gli ostacoli verso una trattazione del tema in ottica patrimoniale e con la

---

[193] C. Basunti, *La (perduta) centralità del consenso,* cit., 887–888. L'A. sottolinea in merito alla natura irrinunciabile di un servizio come non sia facile stabilire il grado di importanza che può avere per un determinato individuo, il quale costituisce un fattore mutevole anche a seconda del momento e del luogo. Per l'infungibilità, invece, si chiede se il servizio che richiede per l'accesso il consenso dei dati personali per finalità commerciali possa essere considerato fungibile con un servizio analogo che per l'accesso richiede il pagamento di una somma di denaro. Su quest'ultimo aspetto, secondo l'A., la Cassazione fornirebbe risposta affermativa là dove riferisce che l'interessato sarebbe in grado di reperire le stesse informazioni «per altra via, eventualmente attraverso siti a pagamento».

[194] E. Tosi, *Diritto privato delle nuove tecnologie digitali,* cit., 148, sottolinea la progressiva patrimonializzazione dei dati personali ponendo l'accento sul fatto che questi ultimi possiedono un significativo valore economico e spesso vengono utilizzati quale corrispettivo «per prestazioni di servizi digitali, e "cessione" del diritto di sfruttamento economico, temporaneo e non esclusivo, dei propri dati personali condizionata all'osservanza del GDPR». Ciò che rileva, aggiunge l'A., non è rappresentato dal dato personale in sé, ma dal suo valore commerciale derivante dall'analisi massiva di quei metadati che vengono generati dai motori di ricerca così come dagli *smartphone*, *digital assistant* e *wearbles*.

[195] V. Ricciuto, *La patrimonializzazione dei dati personali,* cit., 716. Secondo l'A. la prima ipotesi è quella delle banche dati che acquistano dati dagli interessati o da terzi mentre la seconda ipotesi è quella dei contratti per l'accesso ai *social networks* o ad applicazioni e servizi telematici.

consapevolezza di una circolazione dei dati personali fondata sul contratto, si sottolinea la necessità di individuare i modelli e le discipline applicabili [196].

Il dibattito sulla natura e sul valore da attribuire ai dati personali è ancora aperto, benché la scienza giuridica sembri sempre più orientata ad ammettere un approccio di natura patrimoniale ed economica senza elidere i connotati tipici dei diritti della personalità. Verso quest'ultima direzione sembra andare lo stesso legislatore europeo con l'introduzione delle recenti novità normative.

---

[196] *Ivi*, 718. L'A. si chiede se il contratto avente ad oggetto i dati personali sia da inquadrare tra quelli traslativi che configurano una cessione di un diritto di stampo proprietario sul bene; ovvero se fosse possibile o meno ragionare di un trasferimento di diritti sul bene "dato personale" in capo al titolare del trattamento. In alternativa, se il diritto del titolare sul dato personale deve essere ricostruito in base ad una diversa situazione giuridica soggettiva, di stampo non proprietario. Se si concepisce il diritto del titolare al di fuori di una ipotesi di natura proprietaria, e quindi che esula dal trasferimento vero e proprio, ci si chiede se la circolazione del dato personale possa avvenire mediante quei contratti ascrivibili a quelli di godimento. Tuttavia, l'a. rileva come anche i principali modelli di contratti di godimento non sembrano offrire una soluzione soddisfacente. Viceversa, non manca in letteratura chi sostiene che «la scelta di non circoscrivere l'operazione economica all'interno di uno schema negoziale definito risulta condivisibile alla luce della camaleontica realtà digitale e delle poliedriche strutture economiche (...), oltre che del giudizio di cui all'art. 1322 c.c. che impone di valutare, in una dimensione concreta e non astratta, la meritevolezza degli interessi sottesi ad una certa operazione negoziale». In questo senso, P. CARNOVALE, *La funzione sinallagmatica del trattamento dei dati personali nella fornitura di servizi digitali,* in *giustiziacivile.com*, n. 10, 2021, nota a sentenza del 20 ottobre 2021, 8. Sulla qualificazione e struttura dello schema contrattuale si registra chi sostiene che il contratto, sicuramente atipico, abbia una causa mista perché da un lato viene prestato il consenso al trattamento dei dati personali e dall'altro si consegue un bene o servizio. Non si tratta di un contratto di vendita di beni digitali né di una permuta tra dati e beni digitali visto che il contratto non ha ad oggetto la titolarità dei dati, la quale resta in capo al titolare, bensì solo il diritto allo sfruttamento economico nei limiti e finalità contrattuali. Trattandosi spesso di una raccolta dei dati personali per finalità di *marketing* la causa è mista, e le prestazioni principali devono rintracciarsi nel consenso al trattamento e nella fornitura dei beni. In questo senso P. GALLO, *Il consenso al trattamento dei dati personali come prestazione, cit.,* 1065.

19. *Le prescrizioni concernenti i contratti di fornitura di contenuto digitale o dei servizi digitali tra operatori economici e consumatori (la direttiva UE 2019/770)*

Le direttive (UE) 2019/770, 2019/771 e la 2019/2161/UE hanno apportato modifiche di un certo rilievo in materia di dati personali nell'ambito dei contenuti e servizi digitali [197] rafforzando la diretta connessione esistente tra le esigenze consumeristiche e quelle di *data protection* [198]. Le direttive (UE) 2019/770 e 771 avrebbero dovuto essere oggetto di un intervento organico, poi fallito, che avrebbe condotto all'adozione di un regolamento europeo riguardante la vendita [199].

In particolare, con la direttiva n. 770 del 2019 (complementare alla direttiva UE 2019/771) [200] vengono stabilite alcune regole a tutela degli interessi dei consumatori prevedendo, quindi, diritti che possano

---

[197] A. Morace Pinelli, *La circolazione dei dati personali tra tutela della persona, contratto e mercato,* cit., 1331-1333.

[198] Per una delle prime analisi della normativa, si veda C. Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giustizia civile*, n. 3, 2019, 508; In senso critico si veda altresì A. Barenghi, *Osservazioni sulla nuova disciplina delle garanzie nella vendita di beni di consumo*, in *Contratto e impresa*, vol. 35, n. 2, 2020, 806, il quale ritiene che la direttiva 770 «già ad uno sguardo d'insieme appare insoddisfacente, come insoddisfacente appare la sua tecnica legislativa, notevolmente deteriorata anche al livello del *drafting* (nel testo e negli stessi *considerando*) rispetto alla direttiva precedente. Del pari deludente appare per l'eccesso di profili compromissori (che coinvolgono anche aspetti qualificanti della disciplina) e, ancora, la rinuncia a disciplinare questioni di particolare rilievo, in qualche modo preannunciate nella precedente direttiva».

[199] G. Alpa, *Aspetti della nuova disciplina delle vendite nell'Unione europea*, in *Contratto e impresa*, vol. 32, n. 3, 2019, 825.

[200] La direttiva n. 771 è applicabile ai contratti di vendita di beni, compresi i beni con elementi digitali. Per «beni con elementi digitali» dovrebbero intendersi i beni che incorporano o che sono interconnessi con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni dei beni. Per una maggiore illustrazione del tema cfr. considerando 22 e 23 direttiva UE 2019/770.

favorire la fiducia nell'acquisto di contenuti digitali o di servizi digitali [201].

L'ambito di applicazione della direttiva riguarda i contratti tra operatori economici e i consumatori per la fornitura di contenuto digitale o di servizi digitali. Perciò, l'intento è quello di armonizzare le norme sulla conformità del contenuto digitale o del servizio digitale al contratto, i rimedi in caso di difetto di conformità o di mancata fornitura e le modalità di esercizio di tali rimedi, oltre alla modifica del contenuto digitale o del servizio digitale [202].

Ma, ai fini di quanto si discute, l'ambito disciplinare della direttiva che più interessa riguarda le operazioni di *tying*.

A tal proposito, merita di essere citata testualmente la prima parte del considerando n. 24 della direttiva n. 770, là dove si legge che la «fornitura di contenuti digitali o di servizi digitali spesso prevede

---

[201] Secondo alcuni, la direttiva si pone in continuità con il reg. UE 2016/679. S. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali,* cit., 768, infatti, sostiene che il GDPR è improntato all'esigenza della circolazione dei dati, nella consapevolezza che le informazioni personali dei consumatori «costituiscono il fulcro economico della maggior parte delle imprese che forniscono servizi della società dell'informazione e svolgono attività di commercio elettronico»; con la dir. 2019/770/UE il legislatore europeo «ha inteso regolare una fattispecie di quel fenomeno, vale a dire la fornitura onerosa di contenuti o servizi digitali, attuata o verso il pagamento di un prezzo o verso la fornitura di dati personali. I quali, al pari del prezzo, integrano pur sempre una (contro)prestazione, che si pone in rapporto di corrispettività con quella ricevuta, come ulteriormente suffragato (...) anche dalla dir. 2019/2161/UE del 27 novembre 2019 per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori».

[202] Per quanto suggestiva, non sembra condivisibile la tesi riconducibile a G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie*, in *Jus civile,* n. 2, 2020, 402-404 secondo cui non andrebbe confuso l'ambito di applicazione della direttiva (UE) 2019/770 con il consenso ai *cookie* visto che il considerando 19 della normativa europea esclude l'ambito dei servizi di accesso a internet dalla sua applicazione. Infatti, i *cookie* (particolarmente quelli di profilazione) costituiscono solo una tecnica di acquisizione dei dati personali dell'utente che viene poi tracciato e spesso il consenso è previsto come condizione per l'accesso ad un servizio digitale (si pensi a molti quotidiani *online*), diverso, quindi, dal servizio di accesso a internet che attiene all'IP.

che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato. Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali. La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali. I dati personali potrebbero essere forniti all'operatore economico al momento della conclusione del contratto o successivamente, ad esempio nel caso in cui il consumatore acconsente a che l'operatore economico utilizzi gli eventuali dati personali caricati o creati dal consumatore» mentre utilizza il contenuto o il servizio digitale.

Dalla lettura del considerando si evincono alcuni punti fondamentali: (i) la presa d'atto da parte del legislatore europeo dell'esistenza di una prassi commerciale nel mondo digitale che prevede la fornitura di dati personali in sostituzione di un prezzo; (ii) i dati personali non sono una merce; (iii) tale situazione deve essere regolata prevedendo rimedi a tutela del consumatore.

In riferimento a questo tema, la disposizione centrale è l'art. 3 della direttiva, recepito dal legislatore italiano nel codice del consumo all'art. 135-*octies*, comma 4.

Il testo dell'art. 3 originariamente proposto contemplava esplicitamente i dati personali come *controprestazione*. Questa impostazione, presente nella proposta originaria, è stata fortemente criticata dal Garante europeo per la protezione dei dati personali con il Parere n. 4 del 2017, [203] il quale ha richiesto al legislatore europeo di non qualificare la

[203] C. Irti, *Consenso "negoziato" e circolazione dei dati personali,* cit., 79. In letteratura si segnala chi, in relazione a tale direttiva, sottolinea che la stessa pone in risalto il fenomeno della patrimonializzazione dei dati personali, sebbene sia difficile da ac-

cessione dei dati personali come una controprestazione contrattuale [204]. Si ritiene che l'intervento del Garante sia servito a porre in salvo quella ideologia secondo la quale i dati personali non possono essere considerati e trattati come merce, benché venga poi ammesso che oggi i dati personali sono trattati come valori economici veri e propri [205].

Il testo definitivo non prevede perciò il termine «corrispettivo» e trova applicazione in riferimento a ogni contratto in cui l'operatore economico fornisce, o si impegna a fornire contenuto digitale (o un servizio) digitale al consumatore con quest'ultimo che corrisponde un prezzo o si impegna a farlo e per quelle ipotesi in cui il professionista fornisce o si impegna a fornire contenuto (o un servizio) digitale al consumatore e quest'ultimo fornisce dati personali al professionista (o si impegna a farlo). Ciò accade sempre se i dati personali forniti dal consumatore non siano trattati esclusivamente dal professionista per fornire il contenuto digitale o il servizio digitale a norma della direttiva o per adempiere all'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti [206].

Con il recepimento dell'art. 3 della direttiva, il legislatore italiano ha

---

cettare (il riferimento è al parere dell'EDPS), non può essere ostracizzato dal sistema giuridico in un'ottica delle più moderne esigenze di mercato. Dunque, occorrerebbe accettare che l'ordinamento non vieti lo scambio dei dati personali anche per finalità economiche e piuttosto lo circondi di garanzie stringenti esigendo che sia frutto di un consenso pieno, libero ed informato; in tal senso C. BASUNTI, *La (perduta) centralità del consenso,* cit., 895.

[204] V. RICCIUTO, *Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali,* cit., 7, spec. 25.

[205] *Ibidem*. Sulla rilevanza economica fattuale dei dati personali si veda anche C. SOLINAS, *La circolazione dei dati personali nell'ottica dello scambio tra diritti,* cit., 111-120.

[206] V. RICCIUTO, *L'equivoco della privacy,* cit., 164-165, rileva come la funzione economica dello scambio del dato personale per un servizio digitale sarebbe quella di realizzare concretamente uno scambio, anche là dove lo schema contrattuale sia apparentemente gratuito. La ragione pratica del contratto risiederebbe, quindi, nel fatto che l'interessato presta il proprio consenso al trattamento per ottenere un servizio digitale da parte dell'operatore economico o un corrispettivo, mentre l'operatore

introdotto una differenza rispetto alla norma europea. Invero, nell'art. 135-*octies*, co. 4, cod. cons., non si fa alcun riferimento ad un *impegno* (come testualmente previsto dalla direttiva), ma ci si riferisce a un *obbligo* da parte del consumatore di fornire dati personali. La previsione di un concetto di obbligazione, quindi, secondo alcuni, confermerebbe il definitivo superamento della «costruzione tradizionale del fenomeno in termini non patrimoniali» [207].

La formulazione normativa della direttiva viene ritenuta un elemento che valorizza la caratteristica di un modello contrattuale che contempla un'operazione economica unitaria con uno schema contrattuale con due momenti negoziali diversi e distinti [208]. Essi creerebbero un doppio procedimento formale e un doppio consenso da parte dell'utente: (i) la conclusione del contratto di fornitura da un lato; (ii) la raccolta del consenso informato sottoposto alle regole del GDPR dall'altro [209].

L'elisione del riferimento al corrispettivo che esclude una diretta sinallagmaticità non farebbe venir meno la circostanza che l'atto unilaterale di autorizzazione al trattamento viene accordato in cambio di un servizio; i dati rilasciati dagli utenti rappresentano l'unico controvalore economico che i fruitori corrispondono al fornitore [210].

Secondo questo filone teorico, il consenso richiesto al consumatore, allorché non sia necessario per il trattamento finalizzato al contratto che si va a concludere, non potrebbe essere considerato oggetto di un vincolo obbligatorio sebbene sia qualcosa senza la quale non si ri-

---

economico fornisce un bene o servizio oppure paga il corrispettivo per sfruttare quella specifica ricchezza patrimonialmente valutabile costituita dai dati personali.

[207] *Ivi*, 151.

[208] C. Irti, *Consenso "negoziato" e circolazione dei dati personali,* cit., 81.

[209] *Ibidem*. L'A. riprende G. Resta, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679*, in *Annuario del contratto*, 2018, 132.

[210] C. Irti, *Consenso "negoziato" e circolazione dei dati personali,* cit., 81.

ceverebbe il servizio digitale. Ciò che manca per farlo rientrare nella obbligatorietà sarebbe la bilateralità del vincolo giuridico.

La prestazione gravante sul consumatore non costituisce una obbligazione giuridicamente coercibile e l'atto di rilascio del consenso al trattamento quale prestazione che grava sull'utente per l'ottenimento del prodotto sarebbe una *prestazione condizionale*[211] che non può essere assicurata da strumenti coattivi di realizzazione. È una prestazione libera, ma pur sempre *necessaria* per la soddisfazione dell'aspettativa connessa allo scambio[212]. In altri termini, se l'utente non acconsente ai *cookie* o comunque al tracciamento, il fornitore non potrebbe agire in giudizio, ma il servizio non verrebbe fornito[213].

In questa operazione, pertanto, viene attribuito un *prezzo*[214] alla libertà della scelta che viene patrimonializzata generando un meccanismo volto a esercitare una forma di controllo sulla scelta autodeterminativa del consumatore, impossibilitato ad avvalersi di strumenti di attuazione coattiva[215]. Con l'art. 135-*octies* cod. cons. viene istituzionalizzata una interdipendenza funzionale tra la fornitura di contenuti digi-

---

[211] *Ivi*, 103.

[212] *Ivi,* 104.

[213] *Ibidem*.

[214] *Ivi*, 105. Con "il prezzo del consenso" l'A. si rifà all'espressione utilizzata da Cass. civ. n. 12433 del 2008 in materia di diritto all'immagine e sfruttamento abusivo atta a sintetizzare l'entità della liquidazione dovuta a chi vanti un diritto al risarcimento per illegittimo sfruttamento della propria immagine.

[215] *Ibidem.* L'A. ritiene che in questi schemi contrattuali vada ritenuta superata quella tesi che esclude la riconducibilità al paradigma dei contratti a prestazioni corrispettive. Infatti, ritiene si debba parlare di interdipendenza (nesso di relazione qualificata) tra le prestazioni per giustificare la corrispettività (non ci sarebbe una reale distinzione tra interdipendenza e corrispettività). Bisognerebbe perciò spostare l'analisi dalla reciprocità del vincolo (sinallagma genetico) a quello della interdipendenza tra le "attribuzioni" (sinallagma funzionale). In tal senso, C. IRTI, *Consenso "negoziato" e circolazione dei dati personali,* cit.*,* 107. Sul sinallagma esistente in queste operazioni si veda anche C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, cit., 88.

tali e la prestazione del consenso [216]. Un consenso che viene definito *remunerato* [217].

I rapporti di cui si discute, secondo la tesi ascrivibile a C. Irti, devono essere inseriti nell'ambito del modello normativo dell'art. 1333 c.c., vista la mancanza di un obbligo facente capo a una delle parti dell'operazione. Da ciò ne conseguirebbe che la promessa potrà dirsi perfetta fin dalla sua proposizione, sebbene la sua esecuzione sia sinallagmaticamente condizionata a una *prestazione* del consumatore [218]. In tal caso si tratterebbe di "promesse condizionate ad una prestazione", mentre nell'ipotesi in cui il contratto si perfezionasse anche in assenza di un consenso del consumatore, si avrebbe un contratto con obbligazioni a carico del solo proponente perché in tal caso il rifiuto al rilascio del consenso non può essere confuso con il rifiuto a ricevere il servizio che viene offerto [219].

---

[216] S. Pagliantini, *L'attuazione minimalista della dir. 2019/770/UE,* cit., 1504-1509. L'A. è piuttosto netto nel negare la configurabilità di un contratto a prestazioni corrispettive poiché i dati non sono riconducibili ad una moneta. Non esisterebbe né un sinallagma né una qualificazione di onerosità, bensì una prestazione gratuita da parte del professionista coeva ad una seconda prestazione gratuita da parte del consumatore. Cfr. sul tema G. Resta, *Contratto e diritti fondamentali*, in G. D'Amico (diretto da), *Enc. Dir., I tematici, Contratto*, Milano, Giuffré, 2021, 304.

[217] S. Pagliantini, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies – 135 vicies ter c.cons.*, cit., 1546. L'A. si esprime nel senso che l'art. 135-*octies* cod. cons. prevede la possibilità di un atto di fornitura strutturato come un consenso al trattamento remunerato. Prosegue poi che «supporre che, *oltre a questo*, l'art. 135 *octies*, comma 4°, configuri *due* attribuzioni che si giustificano vicendevolmente è invece un'*addizione* dell'interprete perché dà per esistente un sinallagma che, nel corpo della norma, *non sta*».

[218] C. Irti*, Consenso "negoziato" e circolazione dei dati personali,* cit.*,* 109.

[219] *Ivi,* 110-111. Ciò, secondo l'A., risolverebbe anche quella discrasia relativa alla diversa età richiesta per consenso dati personali nel GDPR e capacità di agire in materia negoziale. Questo perché essendo contratti unilaterali di cui all'art. 1333 c.c. si pone al centro dell'attenzione il solo consenso negoziale di chi si "obbliga" per il perfezionamento del contratto, mentre l'esecuzione della prestazione condizionale (rilascio consenso) – prestazione evento – resterebbe soggetta alle sole regole speciali della disciplina di settore in punto di capacità, revocabilità ecc. In termini simili, senza alcun

Da ultimo, non può sottacersi la primazia che viene riconosciuta al GDPR rispetto ad altre come quella consumeristica [220]. Ciò avviene con l'art. 135-*novies*, co. 6, cod. cons [221]. Da ciò ne consegue una complementarità incrementante da cui se ne riportano degli esempi: visto che il consenso al trattamento deve essere informato, ne conseguirebbe che quando l'interessato è un consumatore, egli possa eccepire, in caso di informativa incompleta, una pratica ingannevole omissiva (art. 22 cod. cons.) [222].

20. *L'utilizzo secondario dei dati personali e il principio di limitazione della finalità del trattamento*

Un altro profilo sui dati personali - collegato al tema sulla natura e valore intrinseco - riguarda l'utilizzo alternativo o secondario dopo la

---

riferimento all'art. 1333 c.c., sembra porsi S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies – 135 vicies ter c.cons.*, cit., 1537, laddove dopo aver ribadito che la fattispecie prevista dal cod. cons. all'art. 135-*octies*, co. 4, non rientra nell'ambito del contratto a titolo oneroso, rileva che in quei casi in cui il consenso è *opzionale* il modello contrattuale è di una fornitura a titolo gratuito; invece, quando è *condizionale* (il consenso), si tratterebbe di «una *fattispecie complessa* nella quale un negozio dispositivo unilaterale condiziona l'efficacia di una fornitura contrattuale *a struttura gratuita*». Questa previsione normativa, secondo l'A., consente l'estensione di quelle tutele del consumatore in caso di difformità del servizio anche per quelle ipotesi in cui non ci sia stata la previsione e corresponsione di un prezzo.

[220] S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies – 135 vicies ter c.cons.*, cit., 1531.

[221] Il comma in questione prevede infatti che «le disposizioni nazionali e quelle del diritto dell'Unione in materia di protezione dei dati personali, in particolare quanto previsto dal regolamento (UE) 2016/679, nonché dal decreto legislativo del 10 agosto 2018, n. 101 e dal decreto legislativo 30 giugno 2003, n. 196, si applicano a qualsiasi dato personale trattato in relazione ai contratti di cui all'articolo 135 *octies*, comma 3. In caso di conflitto tra le disposizioni del presente capo e quelle del diritto dell'Unione in materia di protezione dei dati personali, prevalgono queste ultime».

[222] *Ibidem*.

loro acquisizione per il perseguimento di scopi differenti rispetto a quelli originari. Si tratta di quelle prassi ove gli operatori, dopo aver raccolto dati per svolgere un determinato servizio all'interno di un mercato, utilizzano quegli stessi dati per svolgere altri servizi in altri mercati. Ciò provocherebbe riflessi simultanei in materia di protezione dei dati personali, in ambito concorrenziale e in materia consumeristica [223].

L'argine per un utilizzo secondario lecito è il principio di limitazione della finalità del trattamento, composto da due corollari. Il primo è rappresentato dal criterio di specificazione delle finalità, secondo cui i dati debbono essere raccolti per finalità determinate, esplicite e legittime. Il secondo è rappresentato dal criterio dell'uso compatibile, secondo cui i dati non possono essere trattati in modo incompatibile con la finalità precedentemente specificata [224].

Per verificare la compatibilità dell'uso secondario, dovrebbe essere effettuata una valutazione in base al caso concreto e in virtù dell'art. 6, par. 4, GDPR e del considerando n. 50 GDPR [225].

---

[223] G. D'Ippolito, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. il caso dell'uso secondario di big data*, in *Diritto dell'informazione e dell'informatica,* vol. 35, n. 6, 2018, 943.

[224] *Ivi*, 951. Il principio di limitazione della finalità può oltrepassare anche il suo ambito naturale e agire in ottica antitrust, ossia, intervenendo in situazioni ove un'azienda dominante abusi della sua posizione, anche a scapito dei consumatori/interessati, agendo in altri settori di mercato rispetto al proprio, alterando la concorrenza nei mercati e sfruttando dati e *asset* strategici già in loro possesso e preclusi ai concorrenti.

[225] A mente dell'art. 6, par. 4, GDPR: là dove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'art. 23, par. 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati rac-

In quest'ultimo considerando, si legge, tra l'altro, che 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».

Il considerando prosegue che l'accertamento di una tale compatibilità dovrebbe tener conto di ogni nesso tra tali finalità e quelle 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.

L'accertamento della compatibilità deve vagliare se le ulteriori finalità siano già chiare o implicite nelle finalità originarie e, successivamente, occorre indagare sull'effetto che tali differenti finalità sono in grado di produrre sull'interessato, sulla percezione da parte di quest'ultimo, in virtù del contesto e di altri elementi caratterizzanti la fattispecie concreta; va verificato se la nuova finalità sia o meno sostitutiva di quella originaria; se il nuovo mercato in cui vengono utilizzati i dati già raccolti sia del tutto separato o anche non concorrente con quello originario.

Quei dati raccolti ed elaborati per finalità incompatibili potrebbero non essere utilizzabili poiché violano il principio di limitazione della finalità del trattamento. Questo risultato potrebbe essere raggiunto in tutti quei casi in cui i due tipi di servizi siano percepiti dagli utenti

---

colti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

in modo molto diverso [226]. Nell'utilizzo degli stessi dati per differenti finalità il titolare del trattamento è comunque tenuto a ottemperare al principio di trasparenza informando tempestivamente, in modo chiaro e preciso, l'interessato [227].

Il tema del "riutilizzo" dei dati, però, oggi deve essere letto anche e soprattutto alla luce del *Data Governance Act* che verrà di seguito analizzato. Inoltre, il "riutilizzo" dei dati personali è spesso consentito grazie a una attività di profilazione dell'utente finale o commerciale.

21. *Le operazioni di «profilazione» dell'utente e il processo decisionale automatizzato (art. 22 GDPR)*

Si è visto nei paragrafi precedenti che la profilazione dell'utente è un'operazione molto frequente nelle prassi degli operatori digitali; perciò, è meritevole di una analisi a sé.

Con «profilazione», secondo l'art. 4 del GDPR, si intende qualsiasi forma di trattamento automatizzato di dati personali consistente in un loro utilizzo volto a valutare specifici aspetti personali inerenti 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.

I contenuti e le comunicazioni pubblicitarie trasmesse all'utente in virtù delle sue preferenze e interessi devono essere accompagnati da una chiara esplicazione delle modalità con cui avviene la personalizza-

---

[226] G. D'Ippolito, *Il principio di limitazione della finalità del trattamento,* cit., 953-954. Secondo l'A. per esempio, al netto delle caratteristiche concrete che possono portare un caso specifico a differire dal modello generale e astratto qui analizzato, dovrebbe in teoria essere precluso per un *social network* o una piattaforma attiva nel commercio elettronico usare gli stessi dati dei suoi utenti per offrire anche servizi finanziari, bancari o assicurativi.

[227] In questo senso depone il considerando n. 61 del GDPR.

zione e da una chiara indicazione delle tecnologie di cui ci si avvale, come i sistemi di intelligenza artificiale o altri mezzi [228].

Una delle sfide che riguardano la profilazione e il trattamento dei dati personali si incentra sui *big data*, ossia sulla possibilità per le grandi aziende tecnologiche di analizzare grandi quantità di dati e comprendere le preferenze degli utenti. Quindi, riguarda la possibilità per questi operatori di elaborare una identità digitale degli utenti da utilizzare per scopi commerciali o politici [229].

Si è già annotato in premessa come si dubiti se l'inoltro di un messaggio pubblicitario mirato - attraverso l'utilizzo di un sistema algoritmico - possa essere considerato alla stregua di una decisione ai fini dell'applicabilità dell'art. 22 GDPR, considerato che questo non produce alcun effetto vincolante e che la stessa pubblicità può essere ignorata [230]. Tuttavia, non manca chi evidenzia come un approccio

---

[228] Ad esempio, nell'informativa di Amazon si legge che «per offrirti pubblicità definita in base agli interessi utilizziamo informazioni quali, ad esempio, le tue interazioni con i siti, i contenuti o i servizi di Amazon. Non usiamo informazioni d'identificazione personale come il nome o l'e-mail per offrire pubblicità definita in base agli interessi. (...) Come è consueto nell'industria pubblicitaria, utilizziamo cookie, pixel e altre tecnologie (congiuntamente, "i cookie"), che ci consentono di comprendere l'efficacia della pubblicità definita in base agli interessi che ti mostriamo valutando su quali annunci viene fatto clic o quali annunci vengono visualizzati, per offrirti la pubblicità a te più utile e pertinente (...)». Nell'informativa di Google, nella sezione dedicata alle basi giuridiche, si legge invece che «chiediamo il tuo consenso per elaborare le tue informazioni per scopi specifici e hai il diritto di revocarlo in qualsiasi momento. Ad esempio, chiediamo il tuo consenso per fornirti servizi personalizzati, come gli annunci basati sui tuoi interessi. Chiediamo inoltre il tuo consenso per raccogliere la tua attività vocale e audio ai fini del riconoscimento vocale. Puoi gestire queste impostazioni dal tuo Account Google».

[229] T. E. FROSINI, *Le sfide attuali del diritto ai dati personali*, in *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, Edizioni scientifiche italiane, 2020, 397.

[230] G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova*, cit., 286; si veda altresì la ricostruzione di E. PELLECCHIA, *Profilazione e decisioni automatizzate,* cit., 1227, secondo cui a fronte di una tesi che sostiene che il fenomeno di *cybermarketing* ha un effetto significativo sulle persone interessate se porta ad una discriminazione ingiusta, le linee guida del *Data Protection Working Party* aggiornate il 6 febbraio 2018 sono

di personalizzazione pubblicitaria potrebbe condurre ad una limitazione della libertà di scelta degli utenti. Questi ultimi, all'interno di "bolle", vedrebbero rivolgersi solo informazioni confacenti alle proprie idee o interessi [231].

In una società *data-driven,* i processi di profilazione e personalizzazione, da un lato, indirizzano le decisioni delle imprese e quelle del consumatore, compromettendo il fondamento dell'autonomia contrattuale di quest'ultimo [232].

Al di là del sopra accennato art. 4, ulteriori disposizioni centrali per il tema in tesi sono gli artt. 13, 14 e 15, nonché l'art. 22 GDPR [233].

---

più caute. Secondo queste ultime, vi possono essere casi in cui la pubblicità basata sulla profilazione non presenta criticità, mentre altri casi in cui vi può essere un impatto significativo, ad esempio per l'invadenza della profilazione, il condizionamento delle aspettative e dei desideri degli interessati, la consapevolezza e lo sfruttamento delle vulnerabilità dei soggetti interessati.

231 E. Pariser, *The filter bubble*, cit.; K. Shaffer, *Data versus Democracy: How big data Alghoritms Shape Opinions and Alter the Course of History*, Colorado, 2019.

232 B. Parenzo, *Sull'importanza dl dire le cose come stanno,* cit., 1476. L'A. espone, p. 1481, alcune delle problematiche derivanti da operazioni di profilazioni estrinsecate nella personalizzazione del prezzo o dei messaggi pubblicitari. Le problematiche derivanti sull'autonomia del consumatore profilato riguardano il disvelamento delle sue vulnerabilità, nell'attuazione di tecniche subliminali che possono sortire migliori effetti per l'impresa. Non solo, p. 1483, vengono esposti anche alcuni effetti di natura discriminatoria.

233 L'art. 22 GDPR prevede, al par. 1, che «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Il par. 2 prosegue prevedendo che «Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato». Il terzo paragrafo aggiunge che: «Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di

Il divieto stabilito nell'art. 22 GDPR contempla due presupposti che hanno generato un acceso dibattito [234]. Il primo è rappresentato da una decisione che dev'essere basata unicamente sul trattamento automatizzato, conducendo quindi all'interrogativo sull'applicabilità del divieto in caso di intervento umano e, in caso positivo, quanto dev'essere marginale tale intervento. Il secondo elemento è rappresentato invece dalla circostanza che la decisione automatizzata produca «effetti giuridici» sull'interessato o «incida in modo analogo significativamente sulla sua persona».

Riguardo al primo elemento alcuni sostengono che il divieto non opera là dove vi sia un qualsiasi intervento umano che contribuisca alla decisione algoritmica, mentre altri sostengono che - affinché il divieto sancito non sia operativo - occorre che vi sia un intervento umano rilevante [235]. In riferimento al secondo elemento, invece, perché quella decisione automatizzata possa incidere su qualcuno in modo si-

---

contestare la decisione». Infine, l'ultimo paragrafo stabilisce che «Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

234 Si è altresì sottolineato come «la costruzione dell'art. 22 non è né semplice né univoca in quanto la sua interpretazione come un "divieto" piuttosto che un "diritto" modifica la natura della protezione che può essere automatica oppure richiesta dall'interessato.» In questo senso L. AMMANNATI, *La circolazione dei dati: dal consumo alla produzione*, in *Rivista Trimestrale di diritto dell'economia*, n. 4, 2020, 663, spec. 683. Sulla interpretazione dell'art. 22 GDPR come un divieto piuttosto che un diritto, alla luce del tenore normativo, si veda altresì A. PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, in *I dati personali nel diritto europeo,* cit., 436. Quando la decisione di inviare un messaggio di pubblicità mirata avviene nell'ambito di applicazione dell'art. 22, l'interessato dovrebbe essere in grado – in virtù del diritto di accesso – di ottenere informazioni sui parametri utilizzati che determinano il contenuto della pubblicità, in questo senso F. GALLI, *La pubblicità mirata al tempo dell'intelligenza artificiale,* cit., 937.

235 Si veda la ricostruzione di E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civili commentate*, n. 5, 2018, 1225.

gnificativo, deve essere in grado di influenzare le circostanze, il comportamento o le scelte delle persone interessate [236].

Tuttavia, come si è già visto in tema di trasparenza, da un lato, v'è chi sostiene che quelle decisioni riguardanti un individuo, assunte da un algoritmo, dovrebbero essere bilanciate dal "diritto di spiegazione" [237], dall'altro lato v'è chi sostiene che l'art. 22 GDPR non contempla alcun diritto dell'interessato ad essere informato sull'utilizzo del procedimento automatizzato [238].

Come si vedrà, la capacità di elaborazione dei dati e di profilazione compone anche il potere dell'operatore digitale. Il potere di mercato aumenta in modo direttamente proporzionale rispetto alla loro capacità di elaborazione dei dati riverberandosi in senso negativo sulla concorrenza in quanto «produce inerzia negli utenti scoraggiandoli dal ricercare alternative in presenza di pesanti costi di *switching*» [239].

Il processo decisionale automatizzato previsto all'art. 22 GDPR è ormai un tema centrale quando si discute di diritto digitale e, infatti, verrà ripreso più volte, soprattutto là dove verrà analizzato il trattamento dei dati personali mediante algoritmo e in relazione ai recenti casi "Schufa" e "Dun & Bradstreet" (*infra*, cap. V, § 9.2).

L'opacità di elaborazione dei dati che si cela nel processo di profilazione, come si evince dal complessivo esame del GDPR, come l'art.

---

[236] *Ivi*, 1226.

[237] C. Tabarrini, *Comprendere la "big mind",* cit., 565; G. Malgeri, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 7, n. 4, 2017, 243.

[238] Si veda G. Simeone, *Machine learning e tutela della Privacy,* cit., 285, il quale riporta quanto espresso dal *Working Party*, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017, nonché S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to explanation of automated decision-making does not exist in the general data protection regulation,* cit., 76.

[239] L. Ammannati, *La circolazione dei dati: dal consumo alla produzione*, in *Algoritmi, Big Data, piattaforme digitali,* cit., 146.

13 ed il considerando n. 60, fa sì che il titolare sia tenuto a precisi e rigidi obblighi di trasparenza [240].

Infatti, occorre precisare che l'attività di profilazione descritta è spesso preliminare all'assunzione di decisioni automatizzate che, in alcuni casi, generano problematiche di opacità, dando vita al c.d. effetto *Black box*.

22. *Il fenomeno del Black Box e l'impatto sul principio di trasparenza*

Le decisioni automatizzate vengono da alcuni denominate *super decisioni* perché ascritte in una categoria a sé stante. Queste seguono un flusso cognitivo quasi impossibile da replicare per la mente umana [241]. Da qui ne deriva la difficoltosa ricostruzione del processo logico-computazionale attraverso cui la macchina giunge ad una determinata decisione; ci si pone innanzi alla problematica del fenomeno della *black box* [242].

L'opacità intellettiva, suddivisibile in intrinseca e intenzionale [243], consente di poter definire i suoi contorni. Con opacità intellettiva in-

---

[240] Sul punto si veda A. PIERUCCI, *Elaborazione dei dati e profilazione delle persone,* cit., 427. In merito all'opacità derivante dalla profilazione l'A. sottolinea, p. 416, come in questo procedimento l'interessato ha a che fare con rappresentazioni proprie, a lui stesso sconosciute, elaborate in base a criteri ignoti che si rivelano solo nel momento in cui la conseguenza si riversa sulla persona. L'intero procedimento si fonda su un forte squilibrio di potere tra il titolare e l'interessato.

[241] C. TABARRINI, *Comprendere la "big mind",* cit., 566.

[242] F. PASQUALE, *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015; T. CERQUITELLI, D. QUERCIA, F. PASQUALE, *Trasparent Data Mining for Big and Small Data*, New York, 2017; R. GUIDOTTI, A. MONREALE, S. RUGGIERI – D. PEDRESCHI, F. TURINI, F. GIANNOTTI, *Local Rule-Based Explanations of Black Box Decision Systems*, 2018, in arXiv:1805.10820; R. GUIDOTTI, A. MONREALE, S. RUGGIERI, D. PEDRESCHI, F. TURINI, F. GIANNOTTI, *Meaningful Explanations of Black Box AI Decision System, Proceedings of the AAAI Conference on Artificial Intelligence, 2019, 33(01), 9780-9784. https://doi.org/10.1609/aaai.v33i01.33019780*

[243] C. TABARRINI, *Comprendere la "big mind",* cit., 566.

trinseca si fa riferimento alla carenza di capacità volta a comprendere il processo di funzionamento algoritmico del sistema utilizzato per un determinato scopo; con quella intenzionale, invece, il riferimento è a quegli ostacoli volontariamente posti dai responsabili del trattamento a tutela di propri interessi, come, a titolo esemplificativo, i diritti di proprietà intellettuale [244].

In tema di intellegibilità dei sistemi tecnologici deputati al conseguimento di determinati scopi o, in senso più generale, ad assumere decisioni è pregevole quella chiave di lettura che, in virtù del fenomeno della *black box*, in uno scenario caratterizzato da "la tirannia dei dati", affronta la questione ponendo all'attenzione la fallacia della trasparenza, ponendo un parallelismo con la c.d. trappola del consenso [245]. Si verrebbe a realizzare una sorta di cortocircuito a causa di quelle informative dirette al consumatore a cui si andrebbero a sommare ulteriori informazioni di natura tecnica riguardanti il funzionamento del *software*. Si verrebbe a determinare un fallimento sistemico dovuto alla percezione delle richieste di consenso come burocratici fardelli, alla frustrazione generata dal tecnicismo linguistico e alla persistente indifferenza a fronte delle richieste di chiarezza, efficacia e sinteticità [246]. Il rischio risiederebbe, quindi, in una consapevolezza degli interessati dell'ampio ventaglio informativo che li dissuaderebbe dall'approfondire il suo significato per via della sensazione di non essere in grado di poter incidere attivamente, rendendo quindi il sistema informativo privo di scopo. Ciò che risulterebbe carente non sarebbe un'informazione sotto un profilo quantitativo, bensì qualitativo [247]. Depone in

---

[244] *Ivi*, 567.

[245] *Ivi*, 568-569.

[246] Sull'effettivo ruolo del consenso ai tempi dall'economia della rete, con l'affermarsi dei modelli di analisi basati sui *Big Data* e l'uso di strumenti predittivi, il quale si riduce ad una pratica astratta, così «che farne oggetto di declamazione di principio sul piano della disciplina positiva rischia di apparire una mera operazione retorica» si è ampiamente e meritoriamente discusso in dottrina. Tra questi, F. Caggia, *Il consenso al trattamento dei dati personali nel diritto europeo,* cit.*,* 410.

[247] *Ibidem*. Sul tema della soglia di attenzione prestata dall'interessata al consenso

questo stesso senso logico chi si focalizza sulla stesura e intellegibilità delle informative *privacy* sottolineando la lunghezza e la complessità del testo [248].

Nell'ottica di una trasparenza e di una corretta informativa da parte del titolare del trattamento, gli artt. 13 e 14 del GDPR costituiscono un elemento essenziale. La lett. f), par. 2, art. 13 GDPR prevede, tra le informazioni che debbono essere trasmesse all'interessato, anche l'esistenza di un processo decisionale automatizzato, compresa la profi-

---

richiesto dagli operatori si veda anche A. PURPURA, *Il consenso nel mercato dei dati personali,* cit., 896, secondo cui l'utente «non ha a che fare con dati dotati di immediata attitudine comunicativa e pertanto egli comprende meno di quanto quei dati possano dire di sé a professionisti del settore. Una disattenta prestazione del consenso è allora frequentemente incoraggiata dalla scarsa dimestichezza con i servizi della società dell'informazione o dalla naturale inaccessibilità del navigatore medio alla comprensione di meccanismi dall'elevato livello di complessità o sofisticazione o, ancora, dalla sensazione che la circolazione in forma aggregata di una vasta mole di dati riesca a maggiorare i vantaggi dei servizi offerti rispetto ai rischi di nocumento alla propria persona».

[248] L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come un rimedio ex ante*, in *Diritto dell'informazione e dell'informatica*, vol. 40, n. 2, 2020, 303. L'A. suggerisce una metodologia improntata sul *legal design*, sottolinea la necessità di una chiarezza delle informazioni ancor maggiore laddove si tratti di dati sensibili ed ha il pregio di non trascurare il tema della trasparenza anche in relazione a quella prassi di alcuni operatori digitali che fa uso dei c.d. *dark pattern*. Si esprime in senso critico sul consenso anche F. GALLI, *La pubblicità mirata al tempo dell'intelligenza artificiale,* cit., 956, rilevando come esso (in particolar modo nell'ambito della pubblicità mirata) non potrebbe mai essere un consenso realmente informato, vista l'elevata complessità delle operazioni di trattamenti e scambio di dati personali. La maggior parte delle volte, peraltro, finisce per essere una scelta non libera dell'utente. Ciò è particolarmente evidente, secondo l'A., allorché il consenso alla pubblicità mirata venga richiesto quale condizione necessaria per l'utilizzo di un servizio e in tutti i casi in cui sia influenzata da pratiche manipolatorie di ottenimento del consenso. Quello che viene suggerito consisterebbe nell'impedire in alcuni casi «che il consenso al trattamento dei dati possa costituire un presupposto sufficiente per la pubblicità mirata, e piuttosto spostare l'attenzione verso altre condizioni di legittimità, come ad esempio, l'effettiva necessità di concludere o eseguire un contratto oppure la presenza di un legittimo interesse».

lazione di cui all'art. 22, par. 1 e 4, GDPR e, almeno in questi casi, informazioni significative sulla logica utilizzata, oltre all'importanza e alle conseguenze previste ad esito di un tale trattamento per l'interessato. Analoga previsione è stabilita nell'art. 14, par. 2, lett. g), GDPR in riferimento a quelle informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.

Le due disposizioni rivestono un rilevante significato poiché si riferiscono più genericamente a ogni «processo decisionale automatizzato», mentre l'art. 22 del Regolamento europeo presuppone una decisione che sia basata «unicamente» sul trattamento automatizzato [249]. Ciò che viene risaltato negli artt. 13 e 14 GDPR non è l'automazione del trattamento, bensì il processo decisionale azionato dai dati personali [250]. Il difetto dell'avverbio «unicamente» farebbe quindi emergere l'esistente necessità di una trasparenza della logica utilizzata dall'algoritmo in ogni ipotesi di trattamento automatizzato di dati personali [251].

---

[249] G. Comandé, *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e responsabilità*, n. 1, 2022, 35.

[250] *Ibidem*.

[251] *Ivi*, 40-41. L'A. muove le proprie considerazioni sulla base della recente pronuncia di Cass., 25 maggio 2021, n. 14381. Viene sottolineato come la leggibilità della logica algoritmica deve essere tale «da dare indicazioni comprensibili all'interessato sulle logiche con cui si inferiscono delle conclusioni e non indicazioni tecniche astruse. Ecco allora che la tensione con la proprietà intellettuale (...) tende a sfumarsi poiché non devono (...) darsi gli ingredienti esatti della ricetta algoritmica difficilmente comprensibile al profano, ma il senso e la logica da essi usati perché se ne possa apprezzare anche la solidità metodologica da parte dell'interessato comprendendo le conseguenze di accettare (o meno) il trattamento dei propri dati personali». Tuttavia, l'a. segnala anche l'altra faccia della medaglia di una trasparenza "eccessiva". Ci si chiede, infatti, se, conoscendo la logica utilizzata dall'algoritmo si possa sfruttare la stessa per un uso distorsivo, oppure si avrebbero «incentivi a fare migliorare il mio rating reputazionale e quindi ho una esternalità sociale positiva?». Ancora: viene segnalato che «per un verso l'algoritmo, la sua logica operazionale, potrebbe non essere conoscibile neppure al titolare del trattamento, mentre per altro verso la piena o anche solo la ampia trasparenza sulle logiche proprio nel senso della leggibilità potrebbe minare la utilità dell'algoritmo stesso». La succitata pronuncia della Cassazione ha stabilito che «In tema di trattamento di dati personali, il consenso è

La corretta attuazione del principio di trasparenza, come si vedrà in pressoché tutti i profili analizzati, costituisce l'elemento cardine che si ripercuote su tutti gli ambiti affrontati.

validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato; ne consegue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire punteggi di affidabilità, il requisito della consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati» (Cass. civ., 25 maggio 2021, n. 14381, *Quotidiano giuridico*, 2021). Sul tema si veda anche F. BRAVO, *Rating reputazionale e trasparenza dell'algoritmo. Il caso «Mevaluate»*, in *diritto dell'informazione e dell'informatica*, vol. 48, n. 6, 2021, 1001.

Capitolo II

LA CIRCOLAZIONE DEI DATI PERSONALI VERSO STATI TERZI

Sommario: 1. Il quadro giuridico europeo in materia di trasferimento dei dati personali verso Stati terzi o organizzazioni internazionali – 2. La nozione di «trasferimento» dei dati personali – 3. Il *Privacy Shield* e il trasferimento dei dati personali verso gli Stati Uniti d'America – 4. I principi europei alla base della sentenza della Corte di Giustizia *Schrems* II – 5. I criteri di valutazione previsti dall'art. 46 del GDPR e il ruolo delle Autorità di controllo secondo la sentenza *Schrems* II – 6. Conseguenze pratiche dopo la sentenza *Schrems* II – 7. La fase transitoria dopo la sentenza *Schrems* II per i trasferimenti dei dati personali verso gli Stati Uniti d'America – 8. Il nuovo quadro giuridico con il *Trans-Atlantic Data Privacy Framework* (DPF) – 8.1 I poteri delle agenzie di *intelligence* secondo il nuovo accordo – 8.2 La supervisione delle attività di *intelligence* – 9. Il parere dell'EDPB sul *Trans-Atlantic Data Privacy Framework* – 10. Il Report dell'EDPB sulla prima revisione della Commissione europea sul *Data Privacy Framework* – 11. Le conseguenze derivanti dal *Trans-Atlantic Data Privacy Framework* – 12. Il trasferimento dei dati personali verso il Regno Unito dopo Brexit – 13. Le altre basi giuridiche previste dal GDPR per i trasferimenti all'estero: la deroga dell'art. 49, lett. a), GDPR – 14. Le norme vincolanti d'impresa (*Binding Corporate Rules*) – 15. Le *standard contractual clauses* (SCC) – 16. Trasferimenti o comunicazioni non autorizzati dal diritto dell'Unione (art. 48 GDPR) – 17. Trasferimento e accesso internazionale ai dati ai sensi del *Data Governance Act* e del *Data Act*

1. *Il quadro giuridico europeo in materia di trasferimento dei dati personali verso Stati terzi o organizzazioni internazionali*

Il GDPR, nel capo V (cfr. artt. 44 – 50), disciplina il trasferimento

dei dati personali verso un paese terzo o organizzazione internazionale [1].

Il legislatore europeo, omettendo una definizione esplicita di "trasferimento" [2], ha previsto un meccanismo *ad hoc* perché possa essere legittima una tale operazione oltre i confini dello Spazio Economico europeo. Il meccanismo è composto da diverse basi giuridiche poste su piani gerarchici differenti.

L'intento legislativo è quello di consentire il flusso transfrontaliero dei dati regolandolo con specifici limiti. La circolazione dei dati personali nei mercati digitali, oggi, non può prescindere dai meccanismi che disciplinano queste operazioni transfrontaliere.

La prima base giuridica che legittima il trasferimento transfronta-

---

[1] Per una ampia dissertazione sulla disciplina si veda l'opera di G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali*, in *Consumatori e mercato*, Roma, Roma-tre press, 2016; si veda altresì: G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Diritto dell'informazione e dell'informatica*, vol. 26, n. 4-5, 2015, 697; M. MASTRACCI, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La comunità internazionale*, n. 4, 2016, 555-579; G. M. RICCIO, F. PEZZA, *Trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali*, in E. TOSI (a cura di) *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019; Y. POULLET, *Transborder Data Flows and Extraterritoriality: The European Position*, in *Journal of International Commercial Law and Technology*, n. 2, 2007, 146; P. BOCCACCINI, *Il flusso transfrontaliero dei dati e le garanzie*, in G- ZICCARDI, P. PERRI (a cura di), *Tecnologia e diritto*, vol. 2, Milano, Giuffré, 2019, 153-166.

[2] Si può ritenere, rifacendoci all'art. 12 della Convenzione 108 «sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale», che si ha "trasferimento" ogni qualvolta in cui un dato personale venga "materialmente" trasferito al di fuori dello Spazio economico europeo. Tuttavia, tale tema ha generato un dibattito, di talché v'è chi ritiene che il GDPR considererebbe solo i flussi dei dati, ma non anche le semplici comunicazioni dei medesimi. Cfr. M.C. MENEGHETTI, *L'adeguatezza dei trasferimenti di dati personali negli USA, anche alla luce del nuovo Regolamento privacy,* in *giustiziacivile.com*, n. 9, 2017. La questione è stata resa più complessa anche per la diffusione dei nuovi mezzi di comunicazione che rendono labile proprio il concetto di trasferimento materiale come financo testimoniato dalla pronuncia della CGUE, C-101/01, 6 novembre 2003, *Lindqvist,* eur-lex.europa.eu.

liero dei dati personali è disciplinata all'art. 45 GDPR e riguarda le ipotesi in cui sia intervenuta la Commissione europea con l'adozione di una decisione di adeguatezza. Siffatto atto, vincolante per tutti gli Stati membri destinatari ai sensi dell'art. 288, par. 4, TFUE [3], presuppone che vi sia stato un esame della normativa del paese terzo in questione e che tale procedimento abbia fornito un esito positivo, nel senso che l'ordinamento giuridico di tale Stato deve offrire un livello di protezione dei dati personali equivalente a quello europeo.

La Commissione europea valuta l'adeguatezza del sistema giuridico del paese terzo alla luce di una serie di elementi enucleati, a titolo esemplificativo, nel secondo paragrafo dell'art. 45 GDPR. Tra tali elementi occorre tener in considerazione lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale, le norme in materia di protezione dei dati, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale. Inoltre, deve essere valutata l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti, nonché gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale, in particolare in relazione alla protezione dei dati personali.

La decisione di adeguatezza prevista nel GDPR deve essere tenuta distinta rispetto a quella prevista dalla direttiva UE 2016/680 [4] riguardante la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di preven-

[3] Ai sensi del par. 4 dell'art. 288 del Trattato «La decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi».

[4] L'art. 36, par. 1, della direttiva prevede che gli Stati membri dispongono che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sia ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

zione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali [5].

Nel caso in cui non sia applicabile l'art. 45 GDPR, entra in gioco il successivo art. 46 che prevede la possibilità di procedere ugualmente al trasferimento dei dati personali qualora siano state adottate adeguate misure volte a garantire una tutela sostanzialmente equivalente a quella europea [6]. In altri termini, le misure in questione devono sopperire a quel *vulnus* di tutela che emerge da una comparazione dei sistemi giuridici tra i due Stati.

Lo stesso articolo elenca una serie di strumenti di trasferimento contenenti «garanzie adeguate» di cui possono avvalersi gli esportatori per trasferire i dati personali verso paesi terzi. Queste garanzie possono essere a loro volta suddivise in due categorie: quelle che non necessitano di autorizzazione da parte del Garante dei dati personali e quelle che, viceversa, necessitano di una preventiva autorizzazione.

Nella prima, rientrano le clausole contrattuali tipo di protezione dei dati [7], le norme vincolanti d'impresa (disciplinate nell'art. 47 GDPR), i

---

[5] Le decisioni di adeguatezza dei LED dovrebbero tenere conto del loro contesto specifico e soprattutto dei diritti fondamentali che intendono proteggere. Perciò, le decisioni di adeguatezza previste dalla direttiva in questione dovrebbero essere adottate con attenzione, non limitandosi a ricalcare lo schema applicato nelle decisioni di adeguatezza del GDPR. Una tale distinzione ha il vantaggio di poter dedicare la giusta rilevanza a questioni di particolare importanza per la protezione dei dati come la presunzione di innocenza e il diritto a un processo equo per l'uso di algoritmi nelle attività di polizia e/o nelle sentenze. Così L. DRECHSLER, *Comparing LED and GDPR Adeguacy: One Standard Two Systems*, in *Global privacy law review*, vol. 1, n. 2, 2020, 103.

[6] Sul test di equivalenza, da effettuare sulla base del principio di proporzionalità, secondo alcuni la Corte di Giustizia dovrebbe fornire parametri più chiari individuando le possibili garanzie attuabili dai responsabili. In tal senso, L. DRECHSLER, I. KAMARA, *Essential equivalence as a benchmark for international data transfers after Schrems II*, in *Research Handbook on EU data protection law*, 2022, 351-352.

[7] Queste vengono adottate dalla Commissione europea con una apposita decisione secondo la procedura d'esame disciplinata all'art. 93, par. 2, del Regolamento. Mentre con la decisione di cui all'art. 45 si deve accertare, con effetto vincolante, e

codici di condotta, i meccanismi di certificazione e gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici. Nella seconda, invece, rientrano le clausole contrattuali *ad hoc* e gli accordi amministrativi tra autorità o organismi pubblici. Queste misure non devono essere intese in senso rigido e automatico. Infatti, l'assetto normativo del paese terzo verso il quale sono trasferiti i dati può comunque richiedere un'integrazione di tali strumenti di trasferimento e le garanzie in essi contenute con misure supplementari volte a garantire un livello di protezione sostanzialmente equivalente [8]. La valutazione delle misure da adottare caso per caso, in virtù del principio di *accountability,* è rimessa in capo al titolare e/o al responsabile del trattamento.

Da ultimo, l'art. 49 del Regolamento stabilisce una serie di ipotesi derogatorie per le quali il titolare (o il responsabile) del trattamento può procedere con il trasferimento dei dati anche in mancanza di una decisione di adeguatezza e dell'adozione di adeguate garanzie previste all'art. 46 GDPR.

Le ipotesi in questione, menzionate dalla lett. a) alla lett. g) del primo paragrafo, riguardano il caso in cui l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate [9]; il caso di un trasferimento necessario all'esecuzione di un contratto concluso

---

previo esame della normativa, che un paese terzo garantisce un livello di protezione adeguato, con la decisione relativa alle clausole tipo, la commissione non è tenuta ad una siffatta valutazione dell'adeguatezza del livello di protezione garantito dai paesi terzi verso i quali potrebbero essere trasferiti i dati personali in base alle clausole adottate.

[8] Si vedano, a tal proposito, le raccomandazioni adottate il 10 novembre 2020 dall'EDPB "*Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE*", consultabile al sito www.edpb.europa.eu

[9] Il consenso deve essere specifico, perciò, secondo l'EDPB, non sarebbe possibile ottenerlo in via preventiva per un trasferimento futuro già all'atto della raccolta dei dati; se ad esempio le circostanze specifiche e il trasferimento stesso non sono noti al momento in cui è richiesto il consenso, non è possibile verificarne l'impatto

tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; il caso di un trasferimento necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato [10]. Le lettere d) ed e) menzionano le ipotesi di un trasferimento necessario per importanti motivi di interesse pubblico, nonché quello volto ad accertare, esercitare o difendere un diritto in sede giudiziaria.

Le ultime due fattispecie, invece, riguardano il trasferimento per la tutela di interessi vitali dell'interessato qualora questi sia in stato di incapacità fisica o giuridica di prestare il proprio consenso e quella di un trasferimento che origini da un registro funzionale a fornire informazioni al pubblico. La disposizione prevede, infine, un'ultima e residuale ipotesi in cui il trasferimento sarebbe consentito qualora si tratti di un flusso necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento. L'operazione non deve essere ripetitiva e può riguardare un numero limitato di interessati.

2. *La nozione di «trasferimento» dei dati personali*

Delineato il quadro normativo che coinvolge il trasferimento dei dati personali al di fuori dello Spazio Economico europeo, è necessario stabilire cosa si intenda per *trasferimento*.

In altri termini, ci si chiede se sia necessario che i dati personali vengano materialmente trasferiti in uno Stato terzo. L'interrogativo sorge dal momento che il legislatore non definisce la nozione di «trasferimento verso un paese terzo»; non lo ha fatto né con la direttiva 95/46, né con il GDPR.

---

sull'interessato. In questo senso le "Linee guida 2/2018 sulle deroghe di cui all'art. 49 del regolamento 2016/679" del 25 maggio 2018 adottate dall'EDPB, 7.

[10] Queste prime tre fattispecie derogatorie, nonché l'ultima riguardante gli interessi legittimi cogenti, non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

Ebbene, per definire la nozione di trasferimento si può ricorrere a una pronuncia della CGUE del 6 novembre 2003, adottata a definizione della C-101/2003. Nel caso di specie si trattava di pubblicazioni effettuate dalla sig.ra Lindqvist su un sito web riguardanti alcune informazioni di persone appartenenti a una associazione. Con la quinta questione, il giudice del rinvio chiedeva se si possa configurare un trasferimento di dati personali verso paesi terzi allorché una persona che si trova in uno Stato membro inserisca in un sito web dati personali rendendoli accessibili a chiunque si colleghi a internet, incluso chi si trova in paesi terzi [11]. In senso affermativo si pronunciava la Commissione europea e il governo svedese, ritenendo che l'inserimento di tali dati su Internet, diventando accessibili a cittadini di paesi tersi, costituiva a tutti gli effetti un trasferimento; di contrario avviso era il governo dei Paesi Bassi e il governo del Regno Unito secondo cui la direttiva 95/64 riguardava i trasferimenti dei dati e non la loro accessibilità; il trasferimento, secondo il governo britannico, implicherebbe la trasmissione di un dato da una persona locata in un luogo preciso a una terza persona che si trova in altro luogo [12].

La Corte di Giustizia - dopo aver ricostruito la fattispecie individuando anche il ruolo del *web hosting provider* - ha stabilito che i dati personali che arrivano a una persona situata in un paese terzo e che provengono da una persona che li ha pubblicati su un sito Internet «non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata» [13]. La CGUE finisce per escludere che operazioni come quelle compiute dalla protagonista della vicenda possano costituire di per sé un trasferimento verso un paese terzo perché se così fosse, il regime speciale previsto dalla normativa europea diverrebbe, per le operazioni online, un regime di applicazione generale [14].

---

[11] Sentenza CGUE, *Lindqvist*, C-101/2001, cit., § 52.
[12] *Ivi*, §55.
[13] *Ivi*, § 61.
[14] *Ivi*, § 69-70.

Dunque, la Corte risolve la questione statuendo che non si configura un trasferimento di dati verso un paese terzo «allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet - caricata presso il suo fornitore di servizi di ospitalità (...) stabilito nello Stato stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi»[15].

Dalla giurisprudenza europea può quindi ricavarsi una nozione di trasferimento legata a un elemento piuttosto pratico, nel senso che non si potrebbe ritenere che vi sia un «trasferimento» per il fatto che un soggetto situato al di fuori dello spazio economico europeo sia in grado di visualizzare o accedere ai dati. Sarebbe, infatti, necessario che questi dati fossero nella disponibilità di tali soggetti. Questi ultimi dovrebbero essere quindi in grado di determinare le finalità e i mezzi del trattamento dei dati personali o comunque di eseguire operazioni al pari di un responsabile del trattamento.

3. *Il Privacy Shield e il trasferimento dei dati personali verso gli Stati Uniti d'America*

Per quanto attiene alla prima base giuridica - ossia quella che prevede l'adozione di una decisione di adeguatezza - la Commissione europea ha adottato, nel corso degli anni, diverse decisioni in riferimento a vari Stati; tuttavia, le decisioni più problematiche hanno riguardato, con ogni evidenza, quelle relative agli Stati Uniti e, recentemente, ha fatto discutere anche quella che concerne il Regno Unito. Per i rapporti esistenti con questi Stati, è doveroso analizzare le vicende occorse e la situazione odierna.

Per quanto riguarda gli Stati Uniti, si è assistito a una sequenza di eventi che hanno condotto alla nota sentenza della Corte di Giustizia

[15] *Ivi*, § 71.

europea C-311/18 del 16 luglio 2020, la cd. *Schrems* II [16] e, da ultimo, al *Trans-Atlantic Data Privacy Framework*.

Però, il travagliato rapporto con gli Stati Uniti in materia di trasferimento dei dati personali ha una origine più risalente poiché, a seguito del ricorso dello stesso Schrems, la Corte di Giustizia era già intervenuta nel 2015 invalidando la precedente decisione di adeguatezza assunta dalla Commissione europea ed emanata sulla base del cd. *Safe Harbour* [17]. Da siffatta pronuncia ne è derivato quindi un successivo

---

[16] Questa decisione è stata sin da subito criticata da alcuni studiosi americani ritenendola un atto di imperialismo giudiziario e di ipocrisia europea: S. Baker, '*How Can the U.S. Respond to Schrems II?*', *Lawfare,* 21 luglio 2020, lawfaremedia.org; altri operatori del settore hanno sostenuto, in modo suggestivo ma fallace, che la decisione della CGUE non costituirebbe un problema in quanto i dati trasferiti in America, siccome provenienti da una società americana situata in Europa, non rientrerebbero nei programmi di sorveglianza di cui all'art. 702 FISA e E.O. 12333; in questo senso, A. C. Raul, *Why Schrems II Might Not Be a problem for EU-U.S. Data transfers*, *Lawfare*, 21 dicembre 2020, lawfaremedia.org.

[17] Già questa prima pronuncia della Corte ha dato ampio spazio a dibattiti e critiche. C. Kuner, *Reality and illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal*, vol. 18, n. 4, 2017, 882-918, si è espresso in senso critico sostenendo che «*EU data protection law (...) maintains the illusion that it can provide seamless, effective protection of EU personal data transferred around the world, a view that the Schrems judgment affirms. This is a beautiful illusion, at least to European eyes, because it envisions a world where the reach of EU data protection law extends globally; where attempts by foreign intelligence agencies to access the data of Europeans are repelled through the use of procedural mechanisms; and where DPAs police the Internet and quash attempts to misuse European data*». Secondo l'A. questa illusione è stata confermata dalla stessa sentenza *Schrems* e da una sua successiva applicazione pratica che si è rivelata "limitata" e che non impedisce quelle conseguenze che invero vuole evitare: «*Procedural mechanisms may satisfy formal requirements of data protection law, but they cannot provide protection against the intelligence surveillance that the Schrems case involved. Data localization attempts to minimize or avoid the transfer of personal data to third countries, but cannot protect data transfers on a broad scale. DPAs have a crucial role to play in the protection of personal data, but have a limited ability and willingness to enforce the law across borders, as shown by the fact that there has been very little enforcement related to the Schrems judgment*»; in riferimento alla dottrina italiana si veda O. Pollicino, M. Bassini, *La carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *diritto dell'informazione e dell'informatica*, vol. 26, n. 4-5, 2015, 741; C. Comella,

accordo, il *Privacy Shield*, in forza del quale la Commissione europea ha adottato la decisione di esecuzione (UE) 2016/1250 del 12 luglio 2016, dichiarata invalida dalla Corte di Giustizia il 16 luglio 2020 proprio con la sopra citata *Schrems* II.

Quest'ultima sentenza è particolarmente importante in materia poiché ha stabilito alcuni dei principi cardine, soprattutto per quanto concerne il profilo relativo all'acquisizione di tali dati da parte di autorità pubbliche del paese terzo [18]. La sentenza della Corte enuncia principi sia per l'ambito di applicazione dell'art. 45 del GDPR, sia per l'ambito di cui all'art. 46, poiché la vicenda giudiziaria è originata quando non era ancora stato raggiunto l'accordo del *Privacy Shield* e la Corte si è quindi pronunciata in merito a più questioni giuridiche.

Come si legge nella sentenza, in base alle informazioni sull'ordinamento giuridico degli Stati Uniti, ivi incluse le dichiarazioni e gli impegni del governo americano, la Commissione aveva ritenuto che «l'ingerenza nei diritti fondamentali della persona i cui dati sono trasferiti dall'Unione verso gli Stati Uniti nell'ambito dello scudo, compiuta dall'autorità pubblica statunitense per esigenze di sicurezza na-

---

Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza "Safe Harbor" della Corte di Giustizia dell'Unione Europea, in *Diritto dell'informazione e dell'informatica*, vol. 26, n. 4-5, 2015, 719; G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems,* in *Diritto dell'informazione e dell'informatica,* vol. 26, n. 4-5, 2015, 779. P. PIRODDI, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati,* in *Diritto dell'informazione e dell'informatica,* vol. 26, n. 4-5, 2015, 827; V. D'ANTONIO, S. SICA, *I Safe Harbor Privacy Principles: genesi, contenuti, criticità,* in *Diritto dell'informazione e dell'informatica,* vol. 26, n. 4-5, 2015, 801; G.G. CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Diritto dell'informazione e dell'informatica,* vol. 26, n. 4-5, 2015, 909.

[18] A seguito della sentenza *Schrems* II l'EDPB, il 10 novembre 2020, ha pubblicato le "raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza". Con tale documento ha quindi coniato le seguenti quattro garanzie: (a) il trattamento deve basarsi su regole chiare, precise e accessibili; (b) devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti; (c) dovrebbe esistere un meccanismo di controllo indipendente; (d) la persona deve poter accedere a mezzi di ricorso efficaci.

zionale, (...) si limitino a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato e che contro le ingerenze di tale natura esiste una tutela giuridica efficace»[19]. Sul punto la Corte di giustizia è stata di contrario avviso, soprattutto in virtù del principio di proporzionalità desumibile dalla Carta UE.

4. *I principi europei alla base della sentenza della Corte di Giustizia Schrems II*

Il *Privacy Shield* è stato dichiarato invalido dalla Corte di giustizia principalmente perché dava origine a una situazione di incompatibilità con la Carta dei diritti fondamentali europea; tra tali principi la Corte fa riferimento anche all'art. 52 della Carta che contempla il principio di proporzionalità. A mente di tale principio, i diritti e le libertà sancite nella Carta possono subire limitazioni solo se sussistono precisi presupposti e solo ove necessari; essi devono rispondere a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere i diritti e le libertà altrui. La limitazione dei diritti al rispetto della vita privata e alla protezione dei dati deve essere perciò sottoposta a una duplice verifica. La prima, riguarda la gravità dell'ingerenza che la limitazione comporta e la seconda, invece, riguarda l'importanza dell'obiettivo di interesse generale perseguito, il quale deve essere proporzionato rispetto al primo elemento[20].

La normativa che pone limitazioni deve prevedere regole chiare e

---

[19] In questo senso la Sentenza *Schrems* II nel punto 140, § 45.

[20] In questo senso la CGUE, C-511/18, C-512/18, C-520/18, 6 ottobre 2020, *La Quadrature du Net e a. contro Premier ministre e a.*, eur-lex.europa.eu. Con tale pronuncia la Corte ha attribuito un significativo valore all'obiettivo di salvaguardia della sicurezza nazionale, ritenendolo uno scopo che legittimerebbe le limitazioni dei diritti fondamentali e, in una scala gerarchica, sarebbe sovraordinato per rilevanza anche all'obiettivo del contrasto alla criminalità. Tuttavia, tale giustificazione varrebbe finché vi siano concrete e valide circostanze che possano far presumere una minaccia grave, reale e attuale alla sicurezza nazionale.

precise che ne disciplinino la portata e l'applicazione della misura; tali regole devono prevedere requisiti minimi in modo che gli interessati dispongano di garanzie sufficienti a proteggere i loro dati personali contro il rischio di abusi. È su questi principi che la Corte ha stabilito che l'ordinamento statunitense non prevedeva un livello di protezione equivalente a quello europeo.

Il *Privacy Shield,* ha rilevato la Corte, prevedeva che l'adesione ai principi stabiliti a protezione dei dati personali, poteva essere limitata per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia. Tali esigenze, dunque, avevano il primato rispetto ai principi stabiliti in materia di protezione dei dati [21].

La Corte, quindi, ha rilevato che una normativa, la quale non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici per accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale a una tutela giurisdizionale effettiva sancito all'art. 47 della Carta UE [22].

---

[21] È così emerso che i programmi di sorveglianza PRISM e UPSTREAM, che si fondano sull'art. 702 FISA e sull'E.O. 12333, non rispettando il principio di proporzionalità, non garantirebbero un livello di protezione equivalente a quello sancito all'art. 52, par. 1, Carta UE. Infatti, l'art. 702 FISA non fa emergere alcuna limitazione all'autorizzazione per l'attuazione dei programmi di sorveglianza ai fini di intelligence esterne, né risultano garanzie per i cittadini stranieri potenzialmente oggetto di tali programmi. Inoltre, la PPD-28 non conferirebbe agli interessati alcun diritto nei confronti delle autorità statunitensi azionabili giudizialmente. Ciò vale anche per i programmi di sorveglianza basati sull'E.O. 12333. La PPD-28 è la *Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities*. Questa direttiva, come si legge dal sito ufficiale del direttore nazionale di *intelligence* USA «*articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes*».

[22] A tal proposito, non è stato ritenuto sufficiente il meccanismo previsto dal *Privacy Shield* consistente nell'istituzione di un mediatore. Siffatta istituzione, infatti, è stata ritenuta priva del requisito fondamentale dell'indipendenza poiché risponderebbe direttamente al Segretario di Stato, il quale provvede altresì alla sua designa-

5. *I criteri di valutazione previsti dall'art. 46 del GDPR e il ruolo delle Autorità di controllo secondo la sentenza Schrems II*

La Corte, sempre nella sentenza *Schrems* II, ha rilevato che il livello di protezione dei diritti fondamentali richiesto dall'art. 46, par. 1, GDPR deve essere determinato alla luce delle disposizioni dello stesso regolamento, lette in virtù dei diritti fondamentali garantiti dalla Carta.

La valutazione richiesta deve considerare tanto le clausole contrattuali tra il titolare del trattamento e il destinatario del trasferimento (del paese terzo) quanto, in caso di un eventuale accesso delle autorità pubbliche del paese terzo, gli elementi rilevanti di quest'ultimo sistema giuridico.

Gli elementi che devono essere considerati per valutare tale sistema giuridico corrispondono a quelli che, in modo non esaustivo, sono enunciati nel par. 2 dell'art. 45 GDPR [23].

La Corte rileva inoltre che l'art. 46 del Regolamento, facendo parte del capo V, deve essere letto in combinato disposto con l'art. 44, il quale delinea il principio generale per il trasferimento dei dati. Secondo tale principio, tutte le disposizioni del capo V devono essere applicate senza pregiudicare il livello di protezione garantito dallo stesso Regolamento. Quindi, la Corte rileva come siffatto livello di protezione debba essere garantito indipendentemente da quale sia la disposi-

---

zione, oltre al fatto che tale organo sarebbe privo di poteri decisori vincolanti nei confronti delle autorità pubbliche.

[23] Come si è già visto, il riferimento è allo stato di diritto, al rispetto dei diritti umani e delle libertà fondamentali, alla pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come all'attuazione di tale legislazione, alle norme in materia di protezione dei dati, alle norme professionali e alle misure di sicurezza (...); all'esistenza e all'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati (...); a gli impegni internazionali assunti dal paese terzo in particolare in relazione alla protezione dei dati personali.

zione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo.

Le clausole tipo di protezione, che sono state fatte proprie dal *Privacy Shield*, avevano una efficacia di natura obbligatoria, quindi vincolanti solo per i contraenti. Non si prospettava alcuna natura vincolante nei confronti delle autorità pubbliche statunitensi e le clausole che vietano l'accesso legittimo ai dati da parte di autorità pubbliche nell'esercizio delle loro funzioni sono nulle [24]. In tal caso, quindi, le circostanze concrete richiederebbero l'adozione di misure supplementari da parte del titolare o del responsabile del trattamento. È lo stesso legislatore europeo che - al considerando n. 109 GDPR - incoraggia i titolari del trattamento a fornire garanzie supplementari che integrino le clausole tipo di protezione dei dati.

In mancanza di una decisione di adeguatezza validamente adottata dalla Commissione, l'Autorità di controllo (ai sensi dell'art. 58, par. 2, lett. f) e j) è tenuta a sospendere il trasferimento dei dati personali qualora sulla base delle circostanze proprie del trasferimento, le clausole non siano o non possano essere rispettate nel paese terzo e se la protezione dei dati non possa essere garantita con altri mezzi.

In presenza di una decisione di adeguatezza, invece, stante la loro natura vincolante (ex art. 288, par. 4, TFUE) per tutti gli stati membri destinatari, finché la Corte non la dichiari invalida, gli Stati e i loro organi non possono adottare misure contrarie. Tuttavia, la decisione di adeguatezza non impedisce al singolo interessato di ricorrere all'autorità nazionale di controllo ai sensi dell'art. 77 GDPR. L'autorità in questione potrebbe quindi adire il Tribunale competente e questo, a sua volta, ricorrere con il rinvio pregiudiziale alla Corte di Giustizia europea.

---

[24] L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettiva,* in *diritto del commercio internazionale*, n.3, 2021, 683.

6. *Conseguenze pratiche dopo la sentenza Schrems II*

La invalidità del *Privacy Shield* ha provocato qualche ripercussione pratica. Tra queste, per quanto riguarda il sistema giuridico italiano, può essere fatta ricomprendere la decisione assunta dal Garante italiano per la protezione dei dati personali (GDPD) con cui è stata accertata l'illiceità del trattamento dei dati personali degli utenti a mezzo di *Google Analytics*[25]. La vicenda ha condotto all'accertamento della violazione degli artt. 5 e 24 GDPR in relazione al principio dell'*accountability*, nonché alla violazione dell'art. 13 GDPR sul principio di trasparenza, ossia all'obbligo di rendere edotti gli interessati dell'intenzione di trasferire dati personali a un paese terzo, oltre all'esistenza delle garanzie appropriate.

Il caso ha visto come protagonista una società che si avvaleva della versione gratuita della piattaforma *Google Analytics* per scopi statistici e per l'ottenimento di informazioni aggregate circa l'attività dei propri utenti nel proprio sito web[26]. Lo scopo dell'utilizzo della piattaforma, invero, consiste nel monitoraggio delle campagne di *marketing* sulla base del comportamento e degli interessi dei singoli utenti[27].

---

[25] Il riferimento è al provvedimento del GPDP del 9 giugno 2022, consultabile su www.garanteprivacy.it

[26] Google Analytics è stato al centro dell'attenzione di diverse Autorità Garanti europee come quella austriaca, francese e danese. A fronte di un'uniformità decisionale da parte delle Autorità citate, nel mese di gennaio 2023 si è pronunciato anche il Garante spagnolo discostandosi dalla linea delle altre Autorità e rigettando il reclamo proposto. Il provvedimento, emesso ad esito del procedimento E/10529/2021, è consultabile al sito www.aepd.es/. Con il provvedimento in questione l'Autorità spagnola ha accertato che il Titolare del trattamento, poco dopo essere venuta a conoscenza della sentenza *Schrems II*, ha cessato di utilizzare lo strumento *Google Analytics*. Il Garante ha altresì accertato che il Titolare non ha mai utilizzato le informazioni allo scopo di identificare gli utenti del suo sito web. In base a quanto accertato e alle informazioni disponibili, il titolare non avrebbe, quindi, utilizzato lo strumento in questione.

[27] Sulle criticità in termini di *privacy* derivanti dall'utilizzo di sistemi come *Google Analytics*, sia nell'ambito dell'ordinamento statunitense, sia in quello europeo, sebbe-

In particolare, il Garante ha accertato che i dati raccolti mediante *cookies* consistevano in «identificatori online unici che consentono sia l'identificazione del browser o del dispositivo dell'utente che visita il sito web, sia del gestore stesso del sito (attraverso l'ID account Google); indirizzo, nome del sito web e dati di navigazione; indirizzo IP del dispositivo utilizzato dall'utente; informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata, nonché a data e ora della visita al sito web». Nel caso in cui l'utente effettui l'accesso mediante l'*account* Google, ai suddetti dati andrebbero aggiunti tutti quelli già contenuti nell'*account* di riferimento.

Il GDPD, quindi, ha accertato che i dati erano oggetto di trasferimento in un paese terzo, ovvero gli Stati Uniti, per il tramite di Google Ireland Limited (responsabile del trattamento) e ha indagato sull'esistenza di adeguate misure supplementari volte ad ottenere una adeguata protezione dei dati personali. A tal proposito, è stato rilevato come le misure supplementari di natura tecnica, nel caso di specie, non fossero adeguate. Infatti, il meccanismo utilizzato consisteva nella cifratura dei dati, la quale però non si dimostrava sufficiente poiché il sistema statunitense consente alle autorità pubbliche l'accesso non so-

---

ne non focalizzandosi nello specifico sulla tematica del trasferimento dei dati personali, si era espressa già nel 2010 parte della dottrina americana: R. LIEBER, K. CHANEY, *Google Analytics*: *Analyzing the Latest Wave of Legal Concerns for Google in the US and the EU*, in *Buffalo Intellectual Property Law Journal*, n. 7, 2010, 135. È stato rilevato come «*the future of web analytics—as a tool and as an industry—will continue to evolve as behavioral targeted marketing and social media become more commonly utilized by companies, organizations, and governments. In addition, Google Analytics's widespread use in the industry will likely continue unabated, thanks in part to its open source status and relative ease of use. But as we have discussed, privacy advocates will continue to raise concerns in the United States, the European Union, and Germany*». Tra le soluzioni proposte, oltre a una sensibilizzazione e formazione dell'utente sull'importanza di un corretto uso dei propri dati personali, vengono fatte proprie anche delle raccomandazioni di organizzazioni statunitensi secondo cui: «(...) *the providers of measurement tools must build their products to higher privacy standards than what currently exists in the commercial sector. Agencies must craft robust policies to ensure that data collected for measurement purposes is adequately safeguarded. And the [] polic[ies] on persistent tracking technologies must be adapted to continue to establish the highest levels of privacy protection while accounting for recent technological advances*».

lo ai dati personali importati, bensì anche alle chiavi crittografiche necessarie alla loro decodificazione.

Pertanto, dal momento che la disponibilità della chiave di cifratura è detenuta dall'importatore Google LLC, le autorità statunitensi sarebbero state in grado di decriptare anche i dati cifrati. Ciò rendeva evidente l'inadeguatezza delle misure attuate dal titolare del trattamento.

L'assenza di idonee misure tecniche, inoltre, ha comportato, secondo il Garante, la conseguente inadeguatezza delle ulteriori misure di natura contrattuale e organizzativa [28].

La decisione del garante è stata dirompente nel mercato delle piattaforme che acquisiscono, elaborano e trasferiscono dati personali e, sebbene limitata specificatamente ad una di tali piattaforme, probabilmente rappresentava – al netto di nuove potenziali decisioni di adeguatezza della Commissione europea – solamente la punta dell'*iceberg* [29].

---

[28] A tal proposito l'Autorità fa rinvio a quanto contenuto nella Raccomandazione EDPB n. 1/2020 relativa alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, 18 giugno 2021, par. 53 secondo cui «le misure contrattuali e organizzative, da sole, non riescono in genere a evitare l'accesso ai dati personali da parte delle autorità pubbliche del paese terzo in forza di una legislazione e/o di prassi problematiche. Vi saranno infatti situazioni in cui solo misure tecniche adeguatamente attuate potrebbero impedire o rendere inefficace l'accesso ai dati personali da parte delle autorità pubbliche dei paesi terzi, in particolare a fini di sorveglianza. In tali situazioni, le misure contrattuali o organizzative possono integrare le misure tecniche e rafforzare il livello generale di protezione dei dati, ad esempio introducendo controlli ed eliminando automatismi in relazione ai tentativi delle autorità pubbliche di accedere ai dati in modo non conforme alle norme dell'Unione».

[29] Basti solo pensare, tra i tanti, ai meccanismi di YouTube: K. B. Anantharamaiah, *YouTube Analytics Using Google Data Studio*, 2020, consultabile su www.ssrn.com

7. *La fase transitoria dopo la sentenza Schrems II per i trasferimenti dei dati personali verso gli Stati Uniti d'America*

A seguito della sentenza *Schrems* II, gli Stati Uniti e l'Unione europea hanno intrapreso trattative per giungere a un valido accordo conforme ai principi giurisprudenziali delineati.

Le critiche mosse dalla dottrina americana all'orientamento giurisprudenziale europeo (già dalla prima sentenza *Schrems*) fanno riferimento a una discutibile discrasia. Si ritiene che l'art. 4, par. 2, TUE, riservando agli stati membri la competenza in materia di sicurezza, renderebbe inapplicabile nei loro confronti la Carta dei diritti fondamentali. Da ciò ne deriverebbe un doppio binario in materia, ossia l'applicabilità di un sistema rigido sul rispetto dei diritti a tutela dei dati per le operazioni statunitensi rispetto a quello previsto per gli Stati membri UE [30].

Tuttavia, è stato d'altra parte rilevato come una corretta interpretazione della fattispecie renderebbe sempre ammissibile un certo potere di controllo europeo sulla legislazione dei singoli Stati membri ogni qualvolta essa comporti deroghe a diritti connessi e disciplinati dal diritto europeo [31]. Secondo tale tesi, quindi, l'ambito di applicazio-

---

[30] C. KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems,* cit., 881.

[31] A. CRISPI, *Sicurezza nazionale e diritti fondamentali alla luce della giurisprudenza UE in materia di tutela dei dati personali*, in *Rivista italiana di diritto pubblico comunitario*, n. 5, 2017, 998. L'A. sulla base di giurisprudenza della stessa CGUE, sostiene, 1004, che, dato che è «lo stesso trattato ad attribuire ai paesi membri la competenza in materia di sicurezza (...) l'adozione da parte di questi ultimi di legislazioni interne in tale materia costituisce proprio l'esercizio di una facoltà attribuita loro direttamente dall'UE ed equivale così all'applicazione di una norma comune, il che rende la Carta applicabile nel contesto in esame. (...) Il fatto che la legislazione adottata dagli Stati membri in settori di competenza esclusiva deroghi al diritto UE o possa incidere su quest'ultimo, condizionandone l'applicazione, costituiscono proprio fattori di connessione utili e sufficienti per l'applicazione della Carta».

ne della Carta non può essere ancorato a parametri puramente di diritto positivo, bensì all'incidenza del diritto UE e ai suoi scopi [32].

La sentenza della CGUE *Schrems* II ha avuto una portata storica, soprattutto alla luce della (inter)dipendenza geopolitica degli stati membri dell'UE rispetto agli U.S.A., la quale "non consentirebbe" la sospensione del trasferimento (reciproco) di dati [33].

Il panorama normativo e giurisprudenziale delineato ha posto domande su quali avrebbero potuto essere le soluzioni, considerato che il sistema composto dalle clausole tipo di protezione non si può ritenere di per sé sufficiente in molti casi [34]. Molti operatori digitali, anche

---

[32] *Ivi.*, 1005; M. Safjan, *Areas of application of the Charter of fundamental rights of the European Union: fields of conflict?,* in *EUI Working Paper*, n. 22, 2012, 5.

[33] M. Zalnieriute, *Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security*, in *Vanderbilt Journal of Transnational Law,* vol. 55, n. 1, 2022, 47. L'A. sottolinea il dilemma attuale che vivono gli esportatori di dati, ovvero se trattare i dati personali all'interno dell'Unione europea oppure sollecitare le istituzioni americane ad attuare riforme strutturali in materia che possano rendere il livello di protezione equivalente a quello europeo.

[34] G. Churches, M. Zalnieriute, *"Contracting Out" Human rights in International Law: Schrems II and The Fundamental Flaws of U.S. Surveillance Law*, in *Harvard International Law Journal Online*, 2020. Una delle soluzioni che veniva rappresentata si fondava sulla riforma della legislazione americana in tema di sorveglianza e di servizi di *intelligence*: B. Propp, P. Swire, *After Schrems II: A Proposal to Meet the Individual Redress Challenge,* 2020, in *www.lawfare.com*, «*after Schrems II, the endgame inevitably will include some modification to U.S. surveillance law and practice, specifically to address the clear concerns expressed by the CJEU about lack of individual redress.* (...) *Any future attempt by the United States to successfully address this perceived deficiency in judicial redress thus must have two dimensions: a credible fact-finding inquiry into classified surveillance activities in order to ensure protection of the individual's rights, and the possibility of appeal to an independent judicial body that can remedy any violation of rights should it occur*». Secondo altri come L. Clarke, *After a Year of Limbo a EU-US Data Privacy Agreement Still Hangs in the Balance*, in *Tech Monitor,* 2021, consultabile al sito www.techmonitor.ai, la riforma della legge statunitense sulla sorveglianza sarebbe difficile, oppure impossibile; in quest'ultimo senso si veda M. Burgess, *Europe's Move Against Google Analytics Is Just the Beginning*, WIRED, 19 gennaio 2022, consultabile su www.wired.com. Una proposta alternativa prevederebbe l'uso di ordini esecutivi, sebbene essi siano deboli e suscettibili di revoca o modifica dallo

a seguito degli interventi della CGUE, hanno persistito con l'utilizzo delle clausole tipo senza adottare alcuna misura supplementare a protezione dei dati personali.

Per altro verso, negli ultimi anni, gli Stati Uniti hanno dato segnali positivi nella direzione di una riforma in materia, dando vita a iniziative per un quadro legislativo che si avvicina all'approccio europeo del GDPR [35].

Alcuni Stati americani, peraltro, stanno tentando di procedere autonomamente con riforme normative in materia di *privacy* [36]. La California è probabilmente lo Stato più attivo e ambizioso che, con il *California Consumer Act* del 2018 - in vigore dal gennaio del 2020 - prevede, ispirandosi al modello del GDPR, alcune rilevanti novità per i diritti ai consumatori. Tra questi, v'è un più pregnante diritto di informazione, il diritto alla cancellazione dei dati personali e il diritto di agire per la tutela dei propri interessi presso il Procuratore Generale della California [37].

I trasferimenti transnazionali di dati sono una delle questioni più complesse nel campo della privacy. Nondimeno, come suggerito da parte della dottrina, si tratta anche di un settore in cui è probabile

---

stesso Presidente o dal suo successore: in questo senso, W. VOSS, *Transatlantic Data Transfer Compliance*, in *Journal of Science & Technology Law*, n. 28, 2022, 177.

[35] D. CALIA, *Schrems II: the EU's influence on U.S. data protection and privacy laws, in Washington University Global Studies Law Review*, n. 21, 2022, 266.

[36] In ordine temporale, l'ultimo Stato americano ad essere intervenuto è il New Jersey con il *Senate Bill* 322. La Commissione Commercio del Senato del New Jersey l'8 gennaio 2024 ha infatti approvato un disegno di legge riguardante la raccolta e la divulgazione di informazioni personali online da parte degli operatori di siti web e servizi online. La legge in questione prevede che gli operatori debbano avvisare gli utenti della raccolta di informazioni personali e di come queste informazioni vengono eventualmente condivise con terze parti. In aggiunta, nel caso in cui l'operatore dovesse divulgare le informazioni personali di un utente a terzi, dovrebbe fornire gratuitamente all'utente stesso l'indirizzo del terzo, le informazioni personali divulgate e i dettagli di contatto del terzo.

[37] E. TEROLLI, *Privacy e protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *Diritto dell'informazione e dell'informatica*, vol. 28, n. 1, 2021, 63-64.

che si verifichino grandi cambiamenti nel medio termine viste le nuove opportunità che saranno dischiuse dalle tecnologie emergenti. Una delle soluzioni è individuata nel "modello dei dati in possesso dell'utente" oltre ad altre opzioni quale ad esempio il progetto europeo di Gaia-X, per «un ecosistema digitale aperto, trasparente e sicuro, in cui i dati e i servizi possono essere resi disponibili, raccolti e condivisi in un ambiente di fiducia» [38]. Vi sono poi altre soluzioni che sono state prospettate dalla dottrina [39]. Ma al di là delle varie opzioni proposte, si è recentemente giunti ad un nuovo accordo.

8. *Il nuovo quadro giuridico con il Trans-Atlantic Data Privacy Framework (DPF)*

Nel corso del 2022 sono state poste le basi per giungere a una nuova decisione di adeguatezza relativa agli Stati Uniti [40]. Il percorso è sta-

---

[38] P. Jurcys, M.C. Compagnucci , M. Fenwick, *The Future of International Data Transfers: Managing New Legal Risk with a 'User-Held' Data Model*, in *The Computer Law and Security Review*, vol. 46, 2022, 25. Il modello dei dati in possesso dell'utente consisterebbe in una architettura tecnologica in cui gli individui possono raccogliere e collegare varie fonti di dati alla propria "nuvola di dati personali". Questi dati possono provenire dagli account online di un individuo o dai dati raccolti da tracker di attività indossabili e dispositivi IoT (come smartwatch, anelli intelligenti, elettrodomestici intelligenti, ecc.). Tale nuvola sarebbe, quindi, un archivio in cui gli individui possono mettere in comune i loro dati paragonabile a un portafoglio digitale in cui è conservata una copia principale dei dati personali. L'accesso alla nuvola di dati personali sarebbe poi consentito solo al singolo consumatore; i terzi potrebbero accedere a specifici frammenti di dati solo previa autorizzazione dell'individuo.

[39] Si veda A. Monterin, *Dell'incertezza nei trasferimenti di dati personali verso gli Stati Uniti*, in *La nuova giurisprudenza civile commentata*, n. 1, 2021, 154; A. Chander, *Is data localization a Solution for Schrems II*?, in *Journal of International Economic Law,* vol. 23, n. 3, 2020; I. Rubinstein, P. Margulies, *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the search for Common Ground*, in *Connecticut Law Review*, vol. 54, n. 4, 2022.

[40] Le più importanti aziende tecnologiche statunitensi insistevano per l'adozione

to intrapreso nel mese di marzo 2022 allorché la presidente della Commissione europea e il Presidente degli Stati uniti hanno annunciato un nuovo accordo, il c.d. *Trans-Atlantic Data Privacy Framework*. L'accordo è stato poi recepito negli Stati Uniti il 7 ottobre 2022 attraverso un ordine esecutivo del Presidente e poi per mezzo dei regolamenti del procuratore generale.

Il 13 dicembre 2022, quindi, è stata pubblicata la bozza di decisione di adeguatezza. A seguito di un vaglio da parte del Parlamento europeo, sarebbe spettato poi alla Commissione decidere se procedere con l'adozione della decisione nella sua formulazione definitiva che sarà sottoposta a revisioni periodiche; la prima, ad un anno dalla sua adozione. Sicché, a seguito del parere dell'EDPB (non del tutto positivo), la Commissione europea il 10 luglio 2023 ha adottato la decisione senza apportare alcuna modifica [41].

In base al nuovo accordo, le società statunitensi vengono sottoposte a una serie di obblighi come la cancellazione dei dati personali quando non sono più necessari per lo scopo per il quale sono stati raccolti, e per garantire la continuità della protezione quando i dati personali sono condivisi con terzi. Vengono garantite ai cittadini dell'UE diverse possibilità di ricorso nel caso di trattamento dei dati personali in violazione dell'accordo quadro dinanzi a organismi indipendenti di risoluzione delle controversie e un collegio arbitrale.

Inoltre, il quadro giuridico statunitense prevederebbe una serie di limitazioni e garanzie riguardanti l'accesso ai dati da parte delle auto-

---

di un nuovo accordo che potesse superare la fase di stallo creatasi a seguito dell'ultimo intervento della CGUE. Si veda in tal senso W. VOSS, *Transatlantic Data Transfer Compliance*, cit., 177. L'A. specifica che «(...) *Google seeks a replacement Privacy Shield agreement, without modifications to U.S. surveillance legislation, even though, paradoxically, it works with Big Tech col- leagues at Amazon, Apple, Dropbox, Evernote, Google, Facebook (Meta), Microsoft, Snap, Inc., Twitter, Yahoo and Zoom in a Reform Government Surveillance (RGS) coalition that "strongly believes that current surveillance laws and practices must be reformed," and be made "consistent with established global norms of privacy, free expression, security, and the rule of law"».*

[41] Gli Stati membri si sono espressi con la votazione del 7 luglio 2023 con 24 voti favorevoli e 3 astensioni.

rità pubbliche, in particolare in materia penale e per finalità di sicurezza nazionale. L'accesso ai dati europei da parte delle agenzie di *intelligence* statunitensi sarebbe perciò limitato a quanto necessario e proporzionato per la protezione della sicurezza nazionale; i cittadini europei hanno la possibilità di ottenere un risarcimento in merito alla raccolta e all'utilizzo dei propri dati da parte delle agenzie di *intelligence* statunitensi dinanzi a un meccanismo di ricorso indipendente e imparziale che comprende un Tribunale di revisione per la protezione dei dati di nuova creazione.

La decisione contempla una particolarità rispetto alle precedenti. È previsto, all'art. 1, che gli Stati Uniti garantiscono un adeguato livello di protezione per i dati personali trasferiti dall'UE alle organizzazioni americane ricomprese nella lista del *Data Privacy Framework* (DPF) [42]. Questo elemento, perciò, sta a significare che solo per quegli enti ricompresi nella lista gestita e pubblicata dal dipartimento del commer-

[42] L'accordo tra UE-USA si fonderebbe su un sistema di certificazione con cui le organizzazioni statunitensi si impegnano a rispettare una serie di principi in materia di *privacy* - i "*EU-U.S. Data Privacy Framework Principles*" adottati dal Dipartimento del Commercio degli Stati Uniti (DoC) e contenuti nell'allegato I della decisione. Per poter ottenere la certificazione, un'organizzazione deve essere soggetta ai poteri d'indagine della *Federal Trade Commission* (FTC) o del *Department of Transportation* (DoT) degli Stati Uniti. Tutte le organizzazioni certificate, inoltre, sono tenute a certificare annualmente la loro adesione ai Principi in questione. Per certificarsi ai sensi del DPF UE-USA, le organizzazioni sono tenute a dichiarare il loro impegno a rispettare i Principi, a rendere disponibili le loro politiche sulla *privacy* e ad attuarle pienamente. Come parte della loro domanda di (ri)certificazione, le organizzazioni devono presentare al DoC informazioni su, *inter alia*, il nome dell'organizzazione in questione, una descrizione degli scopi per i quali l'organizzazione tratterà i dati personali, nonché i dati personali che saranno coperti dalla certificazione, il metodo di verifica prescelto, il relativo meccanismo di ricorso indipendente e l'organismo legale che ha la giurisdizione per far rispettare i Principi. Il DoC è tenuto a monitorare costantemente l'effettivo rispetto dei principi da parte delle organizzazioni DPF UE-USA attraverso diversi meccanismi. In particolare, effettuerà "controlli a campione" su organizzazioni selezionate in modo casuale, così come i controlli ad hoc di organizzazioni specifiche quando vengono segnalati da terzi.

cio degli Stati Uniti (DoC) sarà applicabile la decisione di adeguatezza, mentre per i restanti si dovranno applicare i meccanismi sussidiari di cui agli artt. 46 e ss. del GDPR.

La stessa decisione prescrive che ogni volta che la competente autorità degli Stati membri esercita i poteri previsti dall'art. 58 GDPR in riferimento a quanto previsto dall'art. 1 della decisione, lo Stato membro è tenuto ad informare senza indugio la Commissione europea. Quest'ultima è chiamata a un costante monitoraggio del quadro normativo oggetto della decisione di adeguatezza, incluse le condizioni in cui vengono effettuati i trasferimenti successivi, le modalità di esercizio dei diritti individuali e i casi di accesso da parte delle autorità pubbliche statunitensi ai dati trasferiti.

8.1 *I poteri delle agenzie di* intelligence *secondo il nuovo accordo*

Uno dei profili centrali del nuovo accordo - in considerazione dei principi enunciati dalla Corte di Giustizia europea - riguarda l'accesso e l'utilizzo di dati personali da parte delle autorità pubbliche statunitensi.

Perciò, una prima parte della decisione è dedicata ai poteri e ai limiti delle autorità pubbliche per finalità di polizia e di applicazione della legge penale. La seconda, invece, si focalizza sull'accesso da parte delle autorità pubbliche per motivi di sicurezza nazionale.

La novità rispetto al contesto della *Schrems* II risiede nell'adozione dell'E.O. n. 14086 del 7 ottobre 2022, il quale prevede limitazioni e salvaguardie per tutte le attività di *intelligence* degli Stati Uniti e sostituisce, in larga misura, il PPD-28203 (altra fonte centrale nell'ambito dell'oggetto della *Schrems* II), rafforzando le condizioni, le limitazioni e le salvaguardie che si applicano a tutte le SIGINT, indipendentemente dal luogo in cui si svolgono.

I requisiti stabiliti in questo ordine esecutivo sono vincolanti per l'intera comunità dell'*intelligence*. Essi devono essere ulteriormente attuati attraverso politiche e procedure di agenzia che li traducano in indicazioni concrete per le operazioni quotidiane.

8.2 *La supervisione delle attività di intelligence*

Le attività delle agenzie di *intelligence* statunitensi sono soggette alla supervisione da parte di diversi organismi. L'E.O. n. 14086 richiede anzitutto che ogni agenzia conduca da sé una supervisione periodica delle attività di *intelligence* e che garantisca un rimedio per qualsiasi eventuale violazione. Esse devono fornire ai funzionari preposti l'accesso a tutte le informazioni necessarie per svolgere le loro funzioni di supervisione.

A questi ultimi devono essere garantite le risorse necessarie per adempiere al loro mandato, l'accesso a tutto il materiale e al personale necessario per svolgere le loro funzioni e devono essere informati e consultati sui cambiamenti di politica proposti. I responsabili per la *privacy* e le libertà civili riferiscono periodicamente al Congresso e al PCLOB, anche in merito al numero e alla natura delle denunce ricevute dal dipartimento/agenzia.

Inoltre, ogni agenzia deve prevedere un ispettore generale indipendente con la responsabilità, tra le altre, di supervisionare le attività di *intelligence* estera. Essi hanno accesso a tutti i registri, ai rapporti, alle verifiche, alle revisioni, ai documenti o altro materiale pertinente. Ancora. La *Intelligence Oversight Board* (IOB), istituito all'interno del *President's Intelligence Advisory Board* (PIAB) [43], è deputata a vigilare sul rispetto della Costituzione e di tutte le norme applicabili da parte delle autorità di *intelligence* statunitensi. Come già previsto dall'E.O. n. 12333, i capi di tutte le agenzie sono tenuti a riferire all'IOB qualsiasi attività per la quale vi sia motivo di ritenere che possa essere illegale o contraria a un ordine esecutivo o a una direttiva presidenziale. Per garantire che l'IOB abbia accesso alle informazioni necessarie per svolgere le sue funzioni, l'E.O. n. 13462 dispone che il Direttore dell'*Intelligence*

[43] Organo consultivo dell'Ufficio esecutivo del Presidente, composto da 16 membri, nominati dal Presidente, senza legami con il governo degli Stati Uniti. L'IOB è invece composto da un massimo di cinque membri designati dal Presidente tra i membri del PIAB.

nazionale e i capi delle agenzie di *intelligence* forniscano tutte le informazioni e l'assistenza che l'IOB ritiene necessarie per svolgere le sue funzioni.

L'IOB è a sua volta tenuto a informare il Presidente sulle attività di *intelligence* che ritiene possano violare la legge degli Stati Uniti e che non vengono affrontate adeguatamente dal Procuratore Generale, dal Direttore dell'*Intelligence* Nazionale o dal capo di un'agenzia.

Le agenzie sono soggette anche alla supervisione del PCLOB, un'agenzia indipendente all'interno del ramo esecutivo composta da un Consiglio di cinque membri nominato dal Presidente. Oltre ai meccanismi di supervisione interni al ramo esecutivo, sono previste specifiche commissioni del Congresso degli Stati Uniti che hanno la responsabilità di supervisionare tutte le attività di *intelligence* estera degli Stati Uniti. I membri di queste commissioni hanno accesso a informazioni classificate, nonché a metodi e programmi di *intelligence*.

9. *Il parere dell'EDPB sul Trans-Atlantic Data Privacy Framework*

L'EDPB è intervenuto con un parere sulla bozza di decisione della Commissione europea riguardante gli USA esprimendosi, per alcuni aspetti, in senso critico e, per altri, accogliendo favorevolmente alcune novità apportate dal nuovo accordo [44].

Una prima parte del parere è dedicata agli aspetti generali, una seconda ai profili attinenti alla protezione dei dati personali e una terza all'accesso ai dati da parte delle autorità pubbliche.

Nella prima parte introduttiva, il Comitato ha segnalato che i principi del DPF rimangono sostanzialmente invariati rispetto a quelli del *Privacy Shield* e ha sottolineato la necessità di ricevere maggiori informazioni del contesto normativo americano affinché possa essere

[44] EDPB, Opinion n. 5/2023 *on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, consultabile al sito www.edpb.europa.eu

compreso nel miglior modo l'interazione tra i principi DPF e l'ordinamento statunitense. Inoltre, ha criticato la struttura degli allegati al DPF piuttosto confusa, così come la terminologia utilizzata, sollecitando una maggior coerenza sistematica [45].

Nella parte relativa ai profili riguardanti la protezione dei dati personali e ai principi ivi stabiliti, l'EDPB ha posto una particolare enfasi alle questioni concernenti i diritti degli interessati [46], all'assenza di definizioni chiave, all'incertezza sull'applicazione dei principi del DPF agli incaricati del trattamento. L'EDPB ha ribadito peraltro che il livello di protezione delle persone i cui dati sono trasferiti non deve essere compromesso da trasferimenti successivi da parte del destinatario dei dati.

Ulteriori criticità deriverebbero dalla frammentazione della normativa statunitense in materia di *privacy* a seconda del settore di riferimento; ciò creerebbe differenti livelli di protezione da chiarire. Ancora, per quanto riguarda i processi decisionali automatici, è stato sottolineato come dovrebbero essere stabilite garanzie come il diritto dell'individuo di conoscere la logica decisionale sottostante, il diritto di contestare la decisione e di ottenere un intervento umano quando la decisione incide significativamente sull'interessato.

Nella terza parte, invece, dedicata all'accesso ai dati da parte delle autorità pubbliche americane, il Comitato ha accolto con maggior favore le modifiche apportate, riconoscendo un significativo miglioramento rispetto al quadro precedente. È stato auspicato che l'adozione della decisione sia preceduta dall'adozione di politiche e procedure aggiornate per l'attuazione dell'E.O. n. 14086 da parte di tutte le agenzie di *intelligence* statunitensi e che queste siano valutate, aggiornate e condivise da parte della Commissione europea.

L'EDPB ha salutato con favore l'introduzione dei concetti di necessità e di proporzionalità nel quadro giuridico statunitense su *signals*

---

[45] Il Comitato riporta l'esempio della nozione di *processing*.

[46] A titolo esemplificativo, alcune eccezioni al diritto di accesso e i tempi e le modalità del diritto di opposizione.

intelligence, oltre al nuovo meccanismo di ricorso stabilito, ritenuto notevolmente migliorato rispetto al precedente [47]. Viene riconosciuta positivamente la previsione di diritti e garanzie in precedenza escluse, nonché le maggiori garanzie d'indipendenza del DPRC e l'esistenza di poteri più efficaci per porre rimedio alle violazioni di legge.

Tuttavia, sono stati segnalati una serie di punti che richiederebbero ulteriori chiarimenti. Un primo punto riguarda i cc.dd. *temporary bulk collection*, nonché la conservazione e la diffusione dei dati raccolti in massa. Per questi viene sottolineato che sebbene l'E.O. n. 14086 contenga un elenco di scopi specifici per i quali la raccolta può o non può avvenire, essi potrebbero facilmente essere aggiornati con ulteriori e nuovi obiettivi alla luce di nuovi imperativi di sicurezza nazionale.

Un altro aspetto delicato, secondo il Comitato, riguarderebbe l'ipotesi di raccolta di dati in massa ai sensi dell'E.O. n. 12333, il quale non prevederebbe il requisito dell'autorizzazione preventiva da parte di un'autorità indipendente, come invece richiesto dalla più recente giurisprudenza della Corte europea dei diritti dell'uomo, né tantomeno un riesame sistematico indipendente *ex post* da parte di un tribunale o di un organismo indipendente equivalente. Inoltre, con riferimento all'autorizzazione preventiva e indipendente della sorveglianza ai sensi della Sezione 702 della FISA, l'EDPB si è rammaricato del fatto che quest'ultima non sia chiamata a verificare preventivamente il programma sulla conformità rispetto all'E.O. n. 14086 per quelle ipotesi in cui siano coinvolti individui non statunitensi.

Il parere, quindi, si conclude con richieste di approfondimenti e chiarimenti diretti alla Commissione europea. Quest'ultima, però, ha

[47] L'EDPB saluta con favore anche le garanzie aggiuntive previste dal nuovo meccanismo di ricorso, come il ruolo dei difensori speciali e l'intervento del PCLOB. Le preoccupazioni riguardano l'applicazione generale della risposta standard del DPRC che notifica all'interessato l'assenza di violazioni e la sua non impugnabilità complessivamente considerata. Data l'importanza del meccanismo di ricorso, il Comitato invita la Commissione a monitorare attentamente il suo funzionamento pratico.

adottato la decisione nella sua versione originaria senza apportare alcuna modifica.

10. *Il Report dell'EDPB sulla prima revisione della Commissione europea sul Data Privacy Framework*

Nel suo nuovo report, che segue la prima revisione da parte della Commissione europea, l'EDPB ha accolto con favore gli sforzi compiuti dalle autorità statunitensi e dalla Commissione per l'attuazione del DPF, in particolare per quanto riguarda le vie di ricorso per le persone dell'UE ai sensi dei principi del DPF, nonché per le nomine dei giudici e degli avvocati speciali del DPRC. Tuttavia, durante la prima revisione periodica, l'EDPB ha individuato una serie di punti che richiedono ulteriori chiarimenti, attenzione o preoccupazione [48].

Per quanto riguarda gli aspetti commerciali del DPF, dato che il processo di certificazione nell'ambito del DPF sembra generalmente svolgersi senza problemi, l'EDPB auspica che il DoC aumenti in futuro la sua supervisione d'ufficio e le azioni di applicazione strutturale per quanto riguarda la sostanziale conformità delle organizzazioni certificate a tutti i principi del DPF. Si fa notare nel report che i principi sono rimasti in gran parte invariati rispetto al *Privacy Shield*. La prima revisione periodica del DPF ha evidenziato anche l'assenza dell'attività di monitoraggio sulla conformità sostanziale ai principi in questione, necessaria soprattutto in virtù del basso numero di reclami ricevuti nel primo anno del DPF. L'EDPB sottolinea la necessità che la Commissione monitori attentamente questo aspetto, anche nelle future revisioni del DPF.

Il Comitato sottolinea, inoltre, la necessità di continuare a monitorare attentamente l'aspetto dell'accesso governativo ai dati, anche nelle

---

[48] EDPB, *Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework* – 4 novembre 2024, consultabile al sito www.edpb.europa.eu

future revisioni del DPF. Sebbene gli elementi del meccanismo di ricorso previsto dall'E.O. n. 14086 siano in vigore, il meccanismo di ricorso non è stato ancora messo alla prova nella pratica, poiché al momento della revisione alcun reclamo è stato ancora proposto. L'EDPB invita quindi la Commissione a monitorare il funzionamento pratico delle diverse salvaguardie volte a garantire un livello di protezione sostanzialmente equivalente, tenendo conto delle revisioni del PCLOB in corso sull'attuazione dei requisiti di necessità e proporzionalità e sul funzionamento del meccanismo di ricorso.

Il Comitato sottolinea che deve essere salvaguardato un adeguato livello di protezione anche in riferimento alla acquisizione governativa di dati personali da parte delle agenzie di *intelligence* statunitensi da parte di *broker* di dati e altre entità commerciali, che non è contemplata dall'E.O. n. 14086. La Commissione dovrebbe, perciò, valutare e monitorare questa particolare forma di accesso governativo e i suoi casi d'uso pratici.

11. *Le conseguenze derivanti dal Trans-Atlantic Data Privacy Framework*

Si è visto che la circolazione dei dati ha una notevole rilevanza non solo per questioni riguardanti la sfera domestica o europea, ma anche nella definizione di quei rapporti tra attori geopolitici. La costante evoluzione e la pervasività di questo tema dà la misura del valore sempre più pregnante di ciò che è in argomento [49]. La circolazione tran-

[49] Nel 2013 e 2014 le Nazioni Unite hanno adottato due risoluzioni su questioni riguardanti i dati personali e la tutela della "vita privata". Esse sono "*The right to privacy in the digital age*" ONU, Assemblea generale, A/RES/68/167, New York, 18 dicembre 2013; e ONU, Assemblea generale, "R*evised draft resolution on the right to privacy in the digital age*", A/C.3/69/L.26/Rev.1, New York, 19 novembre 2014, in risposta allo sviluppo di nuove tecnologie e alle rivelazioni sulla sorveglianza di massa effettuata in alcuni Stati (il riferimento è alle rivelazioni di E. Snowden). Queste risoluzioni condannano fermamente la sorveglianza di massa ed evidenziano l'impatto che tale sorveglianza può avere sui diritti fondamentali alla vita privata e alla libertà

sfrontaliera dei dati, caratteristica dominante della società moderna, è una questione che impegna le istituzioni in ogni latitudine del globo [50].

I fattori geopolitici emergono sotto differenti sfaccettature. Ad esempio, è nota la complementarità tra il tema dei dati personali e quello dello sviluppo di sistemi di intelligenza artificiale sempre più all'avanguardia che, in vero, si avvalgono proprio dei dati per il loro funzionamento [51]. I primi costituiscono il carburante dei secondi. Perciò, non desta stupore che il 7 ottobre 2022 gli Stati Uniti hanno, da un lato, adottato l'E.O. n. 14086 - prodromico all'adozione di una nuova e possibile decisione di adeguatezza da parte della Commissione europea - e, dall'altro, hanno provveduto a emanare ulteriori misu-

---

di espressione nonché sul funzionamento di una società democratica. Nei successivi anni sono state adottate altre revisioni delle risoluzioni sul tema: ONU, Assemblea generale, "*Revised draft resolution on the right to privacy in the digital age*", A/C.3/71/L.39/Rev.1, New York, 16 novembre 2016; ONU, Consiglio per i diritti umani, "*The right to privacy in the digital age*", A/HRC/34/L.7/Rev.1, 22 marzo 2017.

[50] In Africa sono attualmente in corso negoziati per un protocollo sul commercio digitale nell'ambito dell'*African Continental Free Trade Area* (AfCFTA) per la creazione di un mercato unico nel continente africano che riguarderà anche i flussi di dati transfrontalieri che potrebbero essere regolamentati da tale Protocollo. Si veda a tal proposito A. Beyleveld, F. Sucker, *Cross-border data flows in Africa: policy considerations for the afcfta protocol on digital trade,* ottobre 2022, consultabile su www.ssrn.com. Per il continente africano, inoltre, è interessante quanto emerge dallo studio di T. Roberts, A. Mohamed Ali, M. Farahat, R. Oloyede, G. Mutung'u, *Surveillance Law in Africa: a Review of Six Countries*, Brighton: *Institute of Development*, 2021, consultabile al sito www.appropriatingtechnology.org: la ricerca si focalizza sulle criticità in materia di trattamento dei dati personali che emergerebbero, in modo particolare, in sei Stati africani tra cui Egitto, Kenya, Nigeria, Senegal, Sudafrica e Sudan. Le criticità sarebbero dovute alla riforma di leggi che estendono i poteri di sorveglianza dello Stato, alla mancanza di chiarezza normativa e protezione per la *privacy* nella legislazione esistente, al diffondersi delle tecnologie di sorveglianza che consentono sorveglianze illegali, alle agenzie statali che condividono regolarmente attività di sorveglianza al di fuori delle leggi, all'impunità per i trasgressori e alla insufficiente capacità della società civile di riconoscere lo Stato come soggetto responsabile.

[51] G. Gröger, *There Is No AI Without Data*, in *Communications of the ACM*, vol. 64, n. 11, 2021, 98-108.

re restrittive volte a limitare l'esportazione verso la Cina di specifici sistemi *hardware* utilizzati per le operazioni e per lo sviluppo di sistemi di intelligenza artificiale [52].

Limitandoci qui ad osservazioni circoscritte al primo tema, si può osservare come la nota sentenza *Schrems* II abbia prodotto risultati incoraggianti e altri più deludenti che si scontrano con le dinamiche di *realpolitik*. Infatti, tra questi ultimi v'è un risultato non troppo positivo in tema di certezza del diritto, ossia che, nonostante il chiaro tenore della sentenza, le dinamiche riguardanti la circolazione transfrontaliera dei dati all'indomani della pronuncia non hanno visto un vero e proprio adeguamento o ridimensionamento pratico; Meta, per citarne una, ha continuato a trasferire dati sulla base delle clausole contrattuali tipo senza alcuna misura supplementare atta a dimostrare una protezione equivalente a quella europea e il DPC irlandese è intervenuto, ma con tempi molto dilatati, ovvero si è adeguato alla pronuncia della CGUE dichiarando che l'ordinamento americano non garantisce un livello di protezione equivalente a quello europeo solo con la decisione del 12 maggio 2023 [53].

Dall'altro lato, la pronuncia della Corte ha portato a risultati positivi di talché negli USA – sebbene con qualche travagliata dinamica tra Stati e amministrazione federale – si è intrapresa un'opera legislativa che si avvicina (molto) timidamente agli *standard* europei, seppure con qualche recente ridimensionamento.

Tutto ciò ha permesso di giungere al nuovo accordo tra UE e USA, e quindi a una nuova decisione di adeguatezza con specifiche

---

[52] Già nel '*Final Report*' del *National Security Commission on Artificial Intelligence* del marzo 2021 si legge che «*we must win the AI competition that is intensifying strategic competition with China. China's plans, resources, and progress should concern all Americans. It is an AI peer in many areas and an AI leader in some applications. We take seriously China's ambition to surpass the United States as the world's AI leader within a decade*».

[53] *Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. Further to an own-volition inquiry under Section 110 of the Data Protection Act 2018*, consultabile al sito www.edpb.europa.eu

peculiarità che ha già impegnato l'EDPB e, si può ipotizzare, un giorno, anche la CGUE. Dagli scenari che si sono venuti a realizzare, l'auspicio è quello di un superamento della fase di stallo, a beneficio della certezza del diritto, delle imprese e degli utenti dei vari servizi, soprattutto nel mercato digitale. È necessario definire anche il margine di operatività dell'attività di *intelligence* estera che alcuni sostengono, in modo controverso, essere inevitabile [54]. A tal proposito, la nuova decisione di adeguatezza per gli U.S.A. non è esente da criticità. Sicché il dibattito potrebbe riguardare differenti profili.

Alcune critiche possono riguardare quelle regole sancite a definizione dei limiti dei diritti e delle libertà degli individui, ovvero, verificando se siano sufficientemente chiare e precise in virtù del principio di proporzionalità. Ci si chiede, dunque, se (nell'ambito dei programmi di sorveglianza) le regole di riferimento siano sufficienti a individuare le categorie di persone potenzialmente destinatarie delle misure; a individuare il limite di durata della misura; a indicare la procedura per l'esame, l'utilizzo e la conservazione dei dati ricavati [55].

Peraltro, l'ordine esecutivo del 7 ottobre 2022, sebbene circoscriva a determinate ragioni e limiti l'attività di *intelligence*, non impedisce di certo l'attività di *Signals Intelligence* e non impedisce la c.d. *bulk collection,* ossia la raccolta massiva di dati personali riguardanti cittadini di Stati stranieri [56]. Tra le ragioni che legittimano la prima attività ve ne sono

---

[54] A. Lubin, *'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,* in *Chicago Journal of International Law*, vol. 18, n. 2, 2018, 502 e ss. sostiene che un diritto universale alla privacy è un falso mito, nonché la legittimità di una distinzione tra norme che prevedono standard di tutela più elevate per I cittadini di uno Stato e meno elevati per chi risiede oltre confine.

[55] CEDU, *Weber and Saravia v. Germany*, 54934/00, consultabile al sito www.hudoc.echr.coe.int

[56] Si pensi alla infrastruttura creata dalla NSA che attraverso i sistemi di Turmoil e Turbine. Si tratta di sistemi attraverso i quali si è in grado di hackerare segretamente i dispositivi su larga scala utilizzando sistemi automatizzati. Essi posizionano e controllano gli impianti con un malware trasmesso in remoto sui singoli dispositivi informatici selezionati o in blocco su decine di migliaia di dispositivi. Sul punto, si

alcune piuttosto vaghe, tanto da far dubitare sulla conformità rispetto a quella proporzionalità a cui si riferisce la CGUE, che rimane un principio concettualmente diverso rispetto a quello oltreoceano. L'ordine esecutivo, a titolo esemplificativo, prevede tra queste ragioni - al fine di proteggere la sicurezza nazionale degli Stati Uniti e dei suoi alleati e *partner* - quello di comprendere o valutare le capacità, le intenzioni o le attività di un governo o esercito straniero, di una regione di una nazione straniera, di un'organizzazione politica con sede all'estero o di un'entità che agisce per conto o sotto il controllo di un governo, di un esercito, di una regione o di un'organizzazione politica straniera [57]; oppure, altrettanto vaga è l'attività volta a comprendere o valutare le minacce transnazionali che hanno un impatto sulla sicurezza globale, tra cui il cambiamento climatico e altri cambiamenti ecologici, i rischi per la salute pubblica, le minacce umanitarie, l'instabilità politica e le rivalità geografiche [58]; oppure, per proteggere dalle minacce al personale degli Stati Uniti o dei suoi alleati o *partner* [59]. Quest'ultimo obiettivo riguarderebbe anche l'attività di *bulk collection*.

Depone proprio in questo senso una direttiva adottata dalla NSA il

---

veda l'articolo *How the NSA Plans to Infect 'Millions' of Computers with Malware,* in *The Intercept*, 12 marzo 2014.

[57] L'ordine esecutivo così testualmente stabilisce: «(*i) Legitimate objectives. (A) Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives: (1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners*».

[58] Si legge testualmente nell'ordine esecutivo: «*Understanding or assessing transnational threats that impact globalsecurity, including climate and other ecological change, public healthrisks, humanitarian threats, political instability, and geographic rivalry*».

[59] L'ordine esecutivo si limita a prevedere: «*protect against threats to the personnel of the United States or its allies or partners*». Con il termine *personnel*, l'ordine esecutivo precisa che deve intendersi qualsiasi membro attuale o ex membro delle Forze Armate degli Stati Uniti, qualsiasi funzionario attuale o precedente del Governo degli Stati Uniti e qualsiasi altra persona attualmente o precedentemente impiegata o che lavora per conto del Governo degli Stati Uniti, nonché qualsiasi membro attuale o ex delle

29 giugno 2023 che fornisce istruzioni su come procedere alle predette attività di *Signals Intelligence* con la precisazione che, però, gli obiettivi stranieri della raccolta di informazioni "dovrebbero essere trattati con dignità e rispetto" [60].

Sebbene l'ordine esecutivo n. 14086 restringa gli scopi per la raccolta di dati in massa, tale sistema rispecchierebbe in larga parte quei limiti e contorni già stabiliti nel PPD-28 che hanno suscitato critiche e condotto alla storica *Schrems* II [61]. Va da sé che, però, l'ordine esecutivo presenta elementi positivi di novità, tra cui la previsione di un medesimo livello di tutela per tutte le persone, precedentemente garantito ai soli cittadini statunitensi.

In tema di conservazione dei dati personali da parte delle agenzie di *intelligence*, l'ordine esecutivo prevede infatti che la conservazione (a) delle informazioni personali di individui non statunitensi, raccolte attraverso l'*intelligence* dei segnali può avvenire solo se la conservazione di informazioni analoghe riguardanti persone statunitensi fosse consentita dalla legge sottoponendo tali informazioni agli stessi periodi di conservazione applicabili a cittadini statunitensi; (b) delle informazioni personali di persone non statunitensi raccolte attraverso l'*intelli-*

Forze Armate, funzionario attuale o ex, o altra persona attualmente o precedentemente impiegata o che lavora per conto di un alleato o partner.

[60] (U) NSA/CSS POLICY 12-3 ANNEX C, *Supplemental procedures for the collection, processing, querying, retention, and dissemination of signals intelligence information and data containing personal information of non-united states persons.*

[61] Con la PPD-28 si prevedeva che l'attività di *bulk collection* potesse avvenire per (1) spionaggio e altre minacce e attività dirette da potenze straniere o dai loro servizi di *intelligence* contro gli Stati Uniti e i loro interessi; (2) minacce agli Stati Uniti e ai loro interessi derivanti dal terrorismo; (3) minacce agli Stati Uniti e ai loro interessi derivanti dallo sviluppo, dal possesso, dalla proliferazione o dall'uso di armi di distruzione di massa; (4) minacce alla sicurezza informatica; (5) minacce alle Forze armate statunitensi o alleate o ad altro personale statunitense o alleato; e (6) minacce transnazionali, compresa la finanza illecita e l'elusione delle sanzioni connesse. In nessun caso *l'intelligence* dei segnali raccolta in massa avrebbe potuto essere utilizzata allo scopo di reprimere o appesantire le critiche o il dissenso; svantaggiare le persone in base alla loro etnia, razza, sesso, orientamento sessuale o religione; offrire un vantaggio competitivo alle aziende statunitensi e ai settori commerciali statunitensi.

gence dei segnali per le quali non è stata presa una decisione definitiva sulla conservazione agli stessi periodi di conservazione temporanea che si applicherebbero a informazioni comparabili riguardanti persone statunitensi; e prevede (c) la cancellazione delle informazioni personali di persone non statunitensi raccolte attraverso l'*intelligence* dei segnali che non possono più essere conservate, al pari della cancellazione di informazioni riguardanti cittadini statunitensi.

Il principio di minimizzazione dei dati e la loro conservazione da parte delle agenzie di *intelligence* nella realtà dei fatti, però, come testimoniato da episodi concreti, richiedono un più difficile controllo [62]. Si può osservare, peraltro, come l'ordine esecutivo in tesi non si applicherebbe a quei dati a cui le autorità pubbliche accedono attraverso altri strumenti come, ad esempio, attraverso il *US Cloud Act* o il *US Patriot Act*, mediante operazioni di tipo commerciale o accordi volontari di condivisione di dati.

Un altro aspetto del nuovo accordo UE-USA potrebbe riguardare la portata vincolante di quei poteri facenti capo agli organi statunitensi chiamati a valutare eventuali violazioni. Su quest'ultimo punto si può osservare come le modifiche apportate potrebbero essere valutate favorevolmente per i soggetti privati che raccolgono i dati personali. Invero, il sistema dell'iscrizione alla lista delle organizzazioni aderenti al DPF come presupposto per l'applicazione della decisione di adeguatezza fa sì che il potere di espellere dalla lista in questione una determinata organizzazione ritenuta "colpevole", unitamente ad altre possibili misure, possa essere di per sé un valido rimedio.

Gli altri temi, molto probabilmente, riguarderanno l'effettiva indipendenza degli organi chiamati a svolgere indagini e pronunciarsi sui ricorsi [63], nonché la natura e la portata del provvedimento che ha in

---

[62] Si veda il '*Memorandum and opinion order'* di *Foreign Intelligence Surveillance Court* del 26 aprile 2017, consultabile al sito www.dni.gov

[63] Molti di questi organi sono stati "proposti" nella già citata letteratura statunitense di cui al § 5.2 che ha segnalato come possibili enti competenti il PCLO e il PCLOB che, sebbene non possiedano le caratteristiche di indipendenza rispetto

gran parte consentito di giungere al nuovo progetto di decisione. In riferimento alla prima questione, sembrerebbero ancora esistenti le criticità sollevate dalla *Schrems* II, considerato che alcuni degli organi presi in considerazione dall'Ordine esecutivo (in particolare il DPRC) appartengono al ramo esecutivo. In riferimento alla seconda questione, invece, l'ordine esecutivo può essere ritenuto *debole*, nel senso che lo stesso non rientra tra le fonti legislative ed è facilmente modificabile o revocabile dallo stesso o da un successivo Presidente. Perciò, l'attività di monitoraggio da parte della Commissione e delle rispettive Autorità garanti degli Stati membri, e i tempi di intervento, giocano un ruolo essenziale.

Quanto appena analizzato riguarda il panorama statunitense che, sebbene sia mutato, presenta ancora sostanziali criticità [64]. D'altro canto, il piano di riforme inglese, invece, sembrerebbe andare nella direzione opposta e, infatti, la decisione riguardante il Regno Unito, con tutte le dinamiche geopolitiche del caso, suscita ampi dibattiti e imponderabili sviluppi, inclusi quelli di natura giurisdizionale. Nella materia in questione il c.d. effetto Bruxelles ha, quindi, generato in molti casi risultati positivi e, in altri – stante la complessità del meccanismo stabilito nel GDPR – ha creato incertezza e *impasse* che devono essere necessariamente superate. Questo risultato può essere ottenuto solo mediante sforzi più profusi tra gli attori geopolitici coinvolti.

---

al potere esecutivo, potrebbero essere sottoposte al vaglio di un giudice federale indipendente come il FISC e il FISCR in caso di impugnazione, per giungere infine alla Corte suprema.

[64] Il sistema si presenta ancora piuttosto fragile rispetto ad un modello di decisione di adeguatezza come quello relativo al Giappone in cui v'è la designazione di un'Autorità indipendente e un meccanismo molto stringente di accesso ai dati per finalità di sicurezza nazionale. USA e Giappone, però, si differenziano in termini di postura strategica.

12. *Il trasferimento dei dati personali verso il Regno Unito dopo Brexit*

La Commissione europea ha adottato una decisione di adeguatezza anche per il Regno Unito a seguito del noto procedimento di recesso dall'UE (*brexit*) [65]. Anche tale decisione ha le sue peculiarità sotto vari aspetti [66]. Da un lato, l'analisi su cui la decisione si fonda si è rivelata più agevole per la Commissione poiché la normativa vigente in quei territori ricalca ancora la normativa europea, tanto da essere denominato il GDPR del Regno Unito. L'ulteriore dato che ha agevolato l'adozione della decisione risiede nell'adesione del Regno Unito alla CEDU e alla convenzione 108 [67], nonché il suo assoggettamento alla giurisdizione della Corte europea dei diritti dell'uomo.

Dall'altro lato, si consideri che sono vari i dibattiti in seno al parlamento inglese sul tema riguardante le modifiche alla disciplina dei dati personali e ciò prelude a importanti riforme. È per tale ragione che la decisione presenta una vera e propria scadenza breve che porta a un'analisi *ex novo* dell'intero assetto normativo da parte della Commissione. A tal proposito, infatti, il Parlamento europeo, con la risoluzione alla bozza di decisione, prendeva atto «della strategia nazionale del Regno Unito in materia di dati (...) che suggerisce un passaggio dalla protezione dei dati personali a un uso e una condivisione maggiori e più ampi dei dati»; rilevando «che tale posizione secondo cui la

---

[65] La decisione di adeguatezza è stata adottata il 28 giugno 2021.

[66] A. CHOROMIDOU, *EU data protection under the TCA: the UK adequacy decision and the twin GDPRS,* in *International Data Privacy Law*, vol. 11, n. 4, 2021, 388.

[67] la Convenzione 108 è vincolante per gli Stati contraenti. Essa non è soggetta al controllo giudiziario della Corte EDU, ma è stata tenuta in considerazione nella giurisprudenza della Corte nel quadro dell'art. 8 della CEDU. Nel 2001 è stato adottato un Protocollo addizionale alla Convenzione 108, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti e l'istituzione obbligatoria delle autorità nazionali di controllo per la protezione dei dati. Tale Convenzione è stata di recente oggetto di un processo di modernizzazione. Questo processo è stato completato il 18 aprile 2018 con l'adozione del protocollo di modifica della Convenzione 108 (Protocollo CETS n. 223).

mancata comunicazione dei dati può avere un impatto negativo sulla società, come enunciata nella strategia, non è compatibile con i principi di minimizzazione dei dati e limitazione della finalità ai sensi dell'RGPD e del diritto primario»[68].

L'altra peculiarità della decisione, sebbene la formulazione sia stata ritenuta troppo vaga dall'EDPB, risiede nel fatto che essa non riguarda i dati personali trasferiti per finalità di controllo dell'immigrazione da parte del Regno Unito o che rientrano nell'ambito di applicazione dell'esenzione rispetto a determinati diritti degli interessati ai fini di mantenimento dell'effettivo controllo dell'immigrazione.

L'altro elemento risaltato riguarda anche qui il profilo delle agenzie di *intelligence*, e quindi, i poteri delle autorità pubbliche per l'accesso ai dati personali finalizzato a motivi di sicurezza nazionale. Le agenzie inglesi, al pari di quelle statunitensi, godono notoriamente di ampi poteri in tal senso e le loro attività sono già state oggetto di importanti pronunce come la sentenza CEDU *Big Brother Watch*[69]. Su questo tema

---

[68] *European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom* (2021/2594(RSP)).

[69] C*ase of Big Brother Watch and Others v. United Kingdom*, *Applications* 58170/13, 62322/14 and 24960/1, *Judgment*. Il 25 maggio 2021 si è pronunciata la Grande Camera stabilendo che «1. La sorveglianza di massa sulle comunicazioni, come disciplinata dal diritto britannico, non è soggetta ad una verifica di necessità e proporzionalità (che assicuri, ad esempio: che le intercettazioni siano soggette all'autorizzazione di un organo indipendente; che l'oggetto e l'ambito di applicazione delle misure di sorveglianza siano ben definite; che vi sia controllo, ex ante ed ex post, da parte di un organismo indipendente). Sebbene gli stati godano di un ampio margine di apprezzamento nel decidere quali misure di sorveglianza siano più adatte a difendere la propria sicurezza nazionale, vi è una violazione dell'art. 8 CEDU. 2. La disciplina britannica che consente lo scambio di informazioni con i servizi di intelligence stranieri non viola l'art. 8 CEDU. Infatti, la supervisione e la possibilità di review da parte di organi indipendenti su queste operazioni appaiono adeguate. 3. La disciplina britannica che governa l'acquisizione dai dati dai service providers viola l'art. 8 CEDU, perché le circostanze che rendono possibile l'acquisizione non sono "stabilite per legge". 4. La disciplina britannica sulla sorveglianza di massa viola l'art. 10 CEDU, nella misura in cui non sono previste garanzie speciali quando viene

la Corte ha sancito importanti principi anche nel caso *Centrum för rättvisa c. Svezia*[70].

Peraltro, anche l'EDPB, nel parere che ha preceduto l'adozione della decisione di adeguatezza, ha avanzato le sue perplessità[71]. Tra le sue varie osservazioni, nell'ambito delle intercettazioni massive di dati da parte delle *intelligence* (i cc.dd. *bulk power*) ha sottolineato come i dati raccolti massivamente, secondo la legislazione inglese, possono essere conservati per lunghi periodi in modo da essere disponibili per un ulteriore e futuro accesso. La disciplina dell'IPA del 2016 – con margini piuttosto ampi – prevede solo la distruzione delle copie dei

---

in gioco materiale che richiede specifica confidenzialità - ad esempio materiale giornalistico confidenziale», consultabile su www.hudoc.echr.coe.int.

[70] Con questa pronuncia del 25 maggio 2021, n. 35252/08, la Corte EDU (Grande Camera), ha stabilito che «1) Alla luce del proliferare delle minacce alla sicurezza nazionale e dell'ampio uso che i terroristi fanno di Internet, agli Stati deve essere riconosciuto un alto margine di apprezzamento nel decidere quali sono le misure migliori per proteggere la sicurezza dei loro cittadini. Pertanto, la scelta di disporre misure di sorveglianza che intercettino le comunicazioni su Internet non è, di per sé, contraria all'art. 8 CEDU. 2) Nondimeno, nel disciplinare le proprie misure di sorveglianza, gli Stati non possono sottrarsi alle basiche garanzie sottese al principio di proporzionalità. Ad esempio, l'intercettazione deve essere soggetta all'autorizzazione di organismi indipendenti; l'oggetto e l'ambito di applicazione delle misure di sorveglianza deve essere ben definito; le operazioni devono essere svolte sotto la supervisione di un organo indipendente e deve esserci possibilità di controllo ex post. 3) Il regime di sorveglianza svedese non rispetta pienamente questi requisiti. In particolare, vi sono tre criticità. Primo, non vi sono regole chiare che riguardino la distruzione del materiale intercettato; secondo, non viene imposto che, quando il materiale intercettato è condiviso con i servizi di intelligence stranieri, debba essere fatta una valutazione anche alla luce delle esigenze della vita privata e famigliare, oltre che di quelle della sicurezza nazionale; terzo, non vi è effettiva possibilità di controllo ex post sulle misure poste in essere». La pronuncia in questione rileva anche perché dichiara legittima l'adozione di un diverso regime giuridico per la sorveglianza domestica e quella straniera. Sentenza consultabile al sito www.hudoc.echr.coe.int.

[71] EDPB, Opinion n. 14/2021, *Regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*.

dati raccolti e solo se la loro conservazione non sia necessaria nell'interesse della sicurezza nazionale o per altri motivi che rientrano nell'ambito di applicazione della sezione 138, par. 2, dell'IPA del 2016. È stato così sottolineato come il riferimento sia rivolto alla distruzione delle sole copie, tralasciando gli originali. Il Comitato, perciò, invitava la Commissione a fornire ulteriori chiarimenti e valutazioni sulle intercettazioni di massa, in particolare sulla loro selezione, per chiarire in che misura l'accesso ai dati personali soddisfi quei principi stabiliti dalla CGUE e quali salvaguardie siano previste per proteggere i diritti fondamentali delle persone i cui dati sono intercettati in questo ambito, anche per ciò che riguarda i periodi di conservazione dei dati.

È ancora più netto il Parlamento europeo là dove nella risoluzione citata si è pronunciato in merito ad alcune attività di *intelligence* britannica tra cui, in particolare, il programma *Tempora* gestito dal *Government Communications Headquarters* (GCHQ – quartier generale delle comunicazioni del governo) del Regno Unito con il quale vengono intercettate le comunicazioni in tempo reale attraverso i cavi in fibra ottica della dorsale internet e si registrano i dati in modo che possano essere trattati e consultati in un momento successivo; un'attività di sorveglianza di massa del contenuto e dei metadati delle comunicazioni che – sottolinea il Parlamento UE – avviene indipendentemente dalla sussistenza di specifici sospetti o di particolari obiettivi [72].

[72] Nella risoluzione si legge, quindi, che il Parlamento: «ritiene inaccettabile che i progetti di decisione di adeguatezza non tengano conto dell'assenza di restrizioni all'utilizzo da parte del Regno Unito dei poteri sui dati in blocco, né dell'effettivo ricorso alle operazioni di sorveglianza del Regno Unito e degli Stati Uniti, come descritto da Edward Snowden, compreso il fatto che: a) l'ICO o gli organi giurisdizionali non effettuano un controllo sostanziale efficace sul ricorso all'esenzione per la sicurezza nazionale prevista dalla legislazione del Regno Unito relativa alla protezione dei dati; b) le restrizioni di utilizzo dei poteri su dati in blocco da parte del Regno Unito non sono previste dalla legge stessa, come richiesto dalla CGUE (ma sono invece lasciate alla discrezione dell'esecutivo soggetta a un "rispettoso" controllo giurisdizionale); c) la descrizione di "dati secondari" (metadati) nei progetti di decisione è gravemente fuorviante e non precisa che tali dati possono contenere molte

Sul tema della sorveglianza, quindi, l'istituzione europea invitava gli Stati membri a concludere accordi di "non spionaggio" con il Regno Unito e invitava la Commissione a utilizzare le sue interlocuzioni con le controparti britanniche per rappresentare che, se le leggi e le pratiche di sorveglianza del Regno Unito non fossero modificate, l'unica opzione percorribile per facilitare le decisioni di adeguatezza sarebbe la conclusione di accordi di "non spionaggio" con gli Stati membri.

Dunque, già lo stato di fatto del quadro normativo inglese genera di per sé perplessità per l'adeguatezza richiesta dal GPDR; a ciò si aggiunga il processo di riforme in discussione proprio in quelle latitudini. Il *Data Protection and Digital Information Bill*, così come proposto nel luglio del 2022, [73] prevedeva importanti modifiche normative che si discostavano dal GDPR, tra cui quelle relative alla definizione di "dati personali" in termini di "identificabilità" dell'interessato, così come relativamente ai processi decisionali automatizzati prevedendo una riduzione dei limiti al ricorso a tali operazioni [74]. Ulteriori modifiche ri-

---

informazioni ed essere altamente invasivi, e che sono soggetti a sofisticate analisi automatizzate (come dichiarato dalla CGUE nella causa *Digital Rights Ireland*) ma che tuttavia, ai sensi della legislazione britannica, i metadati non sono adeguatamente protetti dall'accesso indebito, dalla raccolta in blocco e dall'analisi basata sull'intelligenza artificiale da parte delle agenzie di intelligence del Regno Unito; d) le "Five Eyes Agencies", in particolare il GCHQ e l'Agenzia nazionale per la sicurezza (NSA), condividono nella pratica tutti i dati di intelligence». A ciò si aggiungono anche le recenti dichiarazioni del capo dell'intelligence nazionale australiana, Andrew Shearer, rese nel corso di un evento presso il *Center for Strategic and International Studies* di Washington secondo il quale l'Australia sta costruendo una struttura di archiviazione *cloud* per condividere informazioni con Stati Uniti e Regno Unito proprio nell'ambito dell'alleanza *Five Eyes*.

[73] S. WILKINSON, *UK data protection and digital information bill explained*, in *Journal of Data Protection & Privacy*, vol. 5, n. 3, 2022, 242-253; I. LLOYD, *Moving UK Data Protection Law Away from EU Standards – Legislative Focus Areas in 2022 — New Directions Forward or Steps Backwards in UK Data Protection and Digital Information Bill?*, in *Computer Law Review International,* n. 6, 2022, 180 ss.

[74] In connessione con il tema dei dati personali, peraltro, nel Regno Unito è stato recentemente proposto, per scopi di sicurezza e tutela dei minori, il disegno di legge *Online Safety Bill*, attualmente all'esame del parlamento inglese. Tale disegno

guarderebbero poi proprio l'ambito del trasferimento transnazionale dei dati personali verso un sistema più favorevole a una *circolazione* internazionale dei dati personali. Da ultimo, insieme ad altre modifiche, la riforma avrebbe previsto anche il mutamento – in senso meno restrittivo – del profilo riguardante i *cookie* e altre tecnologie di tracciamento, utilizzabili senza il consenso dell'interessato [75].

A fronte di un piano di riforma sostanzialmente modificativo dell'impianto giuridico in materia di dati personali, più di recente si è assistito ad una sua *sospensione* volta a considerare nuovamente il progetto. Il motivo principale che ha condotto a riconsiderare l'intervento normativo riposa proprio sulla preoccupazione di possibili ripercussioni relative alla decisione di adeguatezza adottata dalla Commissione europea nel 2021 [76]. Pertanto, alcuni membri del governo britannico hanno espresso l'intenzione di riflettere un quadro normativo in materia di *privacy* che possa garantire un'adeguatezza rispetto alla normativa europea al pari di quanto è avvenuto con altri Stati come Giappone, Corea del Sud, Canada e Nuova Zelanda.

---

di legge non è andato esente da critiche, soprattutto da parte di operatori del mercato in tema di comunicazioni private e sicure. Infatti, *Signal* ha recentemente palesato la possibilità di abbandonare il mercato inglese in caso di approvazione di tale disegno di legge poiché, secondo alcuni, indebolirebbe la *privacy* garantita dai sistemi delle piattaforme tramite la nota crittografia *end-to-end*. L'affievolimento delle tutele deriverebbe da un dovere di scansione dei messaggi della rete volte a scovare comunicazioni di matrice pedopornografica e terroristica.

[75] Ciò sarebbe consentito, a titolo esemplificativo, per finalità legate al miglioramento del servizio, sito web o app, oppure per consentire l'adattamento delle funzioni del servizio alle preferenze dell'utente.

[76] L'8 marzo 2023 il governo britannico ha annunciato una nuova versione del *Data Protection and Digital Information Bill* ritenendola una iniziativa legislativa che favorisce le imprese e allo stesso tempo garantisce un'elevata protezione dei dati personali. Fonte normativa consultabile su www.gov.uk

13. *Le altre basi giuridiche previste dal GDPR per i trasferimenti all'estero: la deroga dell'art. 49, lett. a), GDPR*

Molti responsabili del trattamento dei dati vorrebbero utilizzare il consenso degli interessati per trasferire i dati in paesi al di fuori dello Spazio economico europeo [77]. Tuttavia, gli entusiasmi devono essere smorzati. Infatti, nel 2018 l'EDPB ha emanato le linee guida per tutte le ipotesi derogatorie previste dall'art. 49 GDPR, inclusa la deroga del consenso dell'interessato [78]. Ebbene, anche se per il trasferimento dei dati verso un paese terzo fondato sul consenso esplicito e specifico non sia richiesto l'elemento dell'*occasionalità* come nell'ipotesi di un contratto o di motivi giudiziari (art. 49, par. 1, lett. b, c, ed e), il Comitato europeo conclude rilevando che i requisiti richiesti, congiuntamente alla possibilità per l'interessato di revocare il consenso in qualunque momento, fanno sì che il consenso possa rivelarsi una soluzione non applicabile nel lungo periodo per i trasferimenti verso paesi terzi [79].

Nelle stesse linee guida viene specificato che anche «le deroghe non espressamente limitate ai trasferimenti "occasionali" e "non ripetitivi" devono essere interpretate in modo da non contraddire la natura delle deroghe stesse, ossia eccezioni alla regola secondo la quale i dati personali possono essere trasferiti verso paesi terzi soltanto se il

---

[77] S. FABER, *Does the GDPR Allow for the Use of Consent for the International Transfer of Data?,* in *National Law Review,* vol. 9, 2022*,* consultabile al sito www.natlawreview.com. L'A. conclude che sebbene il GDPR sia più permissivo rispetto alla precedente dottrina in termini di utilizzo del consenso come base giuridica per i trasferimenti internazionali di dati, i requisiti per un consenso valido a questo scopo e il diritto di revocare tale consenso generano una situazione complessa e macchinosa. I responsabili e gli incaricati del trattamento dei dati, conclude l'autore, dovrebbero procedere con cautela prima di ricorrere a una "falsa soluzione" e affidandosi quindi al consenso per i trasferimenti internazionali.

[78] EDPB, Linee guida n. 2/2018 sulle deroghe di cui all'art. 49 del regolamento 2016/679.

[79] *Ivi*, 8.

paese di destinazione offre un livello adeguato di protezione dei dati oppure, in alternativa, se sono messe in atto adeguate garanzie»[80].

Si è visto peraltro che il consenso deve essere *esplicito* e *specifico*. Con il primo elemento si intende che dev'essere necessario un elevato livello di controllo individuale dei dati personali come avviene in caso di trattamento di categorie particolari di dati e di decisioni automatizzate. Siffatto elemento fa sì che non sia possibile ottenere un preventivo consenso per un trasferimento futuro al momento in cui avviene la raccolta dei dati[81].

Tra le informazioni che devono essere rese all'interessato per ottenere un valido consenso finalizzato al trasferimento dei dati personali verso Stati terzi occorre: specificare tutti i destinatari o tutte le categorie di destinatari dei dati e tutti i paesi verso i quali sono trasferiti i dati; specificare che il consenso rappresenta il fondamento giuridico per il trasferimento e che il paese terzo verso cui saranno trasferiti i dati non offre un livello adeguato di protezione dei dati sulla base di una decisione della Commissione europea. Come disposto dalla

---

[80] *Ivi*, 5.

[81] *Ivi*, 7. Il Comitato europeo, argomentando il requisito della specificità, puntualizza che se le circostanze specifiche e il trasferimento stesso non fossero noti al momento in cui è richiesto il consenso, non sarebbe possibile verificarne l'impatto sull'interessato. Viene perciò riportato l'esempio «in cui un'azienda UE raccolga i dati dei propri clienti per una finalità specifica (consegna merci) senza prevedere, in quel momento, il trasferimento di tali dati a terzi al di fuori dell'Unione. Si ipotizzi che alcuni anni dopo l'azienda sia rilevata da una società di un paese terzo, che intende trasferire i dati personali dei clienti a un'altra azienda di un paese terzo. Perché il trasferimento sia valido in applicazione della deroga, l'interessato deve prestare il proprio consenso per quel trasferimento specifico al momento in cui si prospetta tale operazione. Il consenso fornito all'atto della raccolta dei dati da parte dell'azienda dell'Unione ai fini della consegna non è sufficiente a giustificare il ricorso a questa deroga ai fini di un trasferimento di dati personali al di fuori dell'UE prospettatosi in un secondo momento. L'esportatore deve quindi assicurarsi di ricevere un consenso specifico prima di mettere in atto il trasferimento, anche se ciò avviene dopo la raccolta dei dati. Tale requisito è correlato alla necessità di un consenso informato».

norma stessa, è necessario fornire informazioni sui possibili rischi per l'interessato derivanti dalla mancanza di un'adeguata protezione nel paese terzo e dall'assenza di garanzie appropriate. Questo avviso «che potrebbe essere standardizzato, deve includere ad esempio una menzione della possibile assenza nel paese terzo di un'autorità di controllo e della possibilità che non siano previsti principi sul trattamento dei dati o diritti dell'interessato» [82].

Nonostante alcuni timidi tentativi in dottrina volti ad ammettere una simile soluzione, dagli orientamenti del principale organismo europeo in materia di dati personali se ne ricava che la base giuridica del consenso - benché non sia limitata a trasferimenti occasionali al pari di altre deroghe normative -, per i precisi e stringenti presupposti richiesti, sarebbe difficilmente utilizzabile per quei trasferimenti massivi di dati ripetuti nel tempo come usualmente avviene da parte delle *big tech*.

14. *Le norme vincolanti d'impresa* (*Binding Corporate Rules*)

Il trasferimento dei dati personali al di fuori dei confini dello Spazio economico europeo, in mancanza di una decisione di adeguatezza della Commissione europea, può avvenire anche previa adozione di adeguate garanzie da parte del titolare o del responsabile del trattamento, tra cui le norme vincolanti d'impresa (BCR) menzionate alla lett. b) dell'art. 46 GDPR e disciplinate nel successivo art. 47 del regolamento [83].

Tali BCR sono sottoposte al vaglio dell'Autorità di controllo competente, la quale è deputata alla loro approvazione. L'autorizzazione

---

[82] *Ivi*, 8.

[83] Sul tema si veda L. BOLOGNINI, *Il trasferimento dei dati verso paesi terzi o organizzazioni internazionali*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il Regolamento privacy europeo*, Milano, Giuffré, 2016, 514-521; G.M. RICCIO, *Model Contractual Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in *Diritto dell'informazione e dell'informatica*, vol. 26, n. 4-5, 2015, 872; P. BOCCACCINI, *Il flusso transfrontaliero dei dati e le garanzie,* cit., 160.

può essere adottata se tali norme sono vincolanti e si applicano a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono una attività comune, se garantiscono diritti azionabili agli interessati e se soddisfano una serie di presupposti contemplati al par. 2 dell'art. 47 GDPR [84].

---

[84] Il par. 2 dell'art. 47 GDPR prevede che le norme vincolanti d'impresa devono almeno specificare: «a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri; b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; c) la loro natura giuridicamente vincolante, a livello sia interno che esterno; d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa; e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa; f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione; g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14; h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 35 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il

La richiesta di autorizzazione viene presentata presso l'Autorità di controllo dello Stato membro nel quale ha sede la società *holding*, oppure presso l'Autorità dove si trova la sede societaria nella quale i dati vengono trattati in via principale. La società che presenta la richiesta è ritenuta responsabile per le violazioni eventualmente commesse dalle altre del gruppo al di fuori dei confini dello Spazio economico europeo.

Si ritiene, però, che lo strumento in parola costituisca un meccanismo oneroso ed elaborato, tendente a scoraggiare gli interessi imprenditoriali (un dato che sarebbe suffragato dal fatto che solo pochi gruppi di imprese se ne avvalgono) e non può essere ritenuto un'alternativa unica agli accordi di adeguatezza, trovando applicazione ai soli rapporti tra società appartenenti allo stesso gruppo [85]. Quindi, in caso

---

controllo della formazione e della gestione dei reclami; i) le procedure di reclamo; j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente; k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo; l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j); m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali».

[85] G.M. RICCIO, *Model Contractual Clauses*, cit., 875.

di trasferimento di dati a società terze rispetto al gruppo, si deve far necessariamente ricorso ai *model contract clauses*[86].

Si può ritenere che le BCR, benché più onerose, presentano una maggiore solidità rispetto alle clausole contrattuali *standard*, in quanto elaborate sulla base delle caratteristiche e delle esigenze del caso concreto, pur tuttavia presentando le stesse criticità dovute al fatto che se le autorità pubbliche dello Stato importatore possiedono ampi poteri di accesso e disponibilità, qualunque BCR o clausola contrattuale *standard* perderebbe il suo valore. Ciò è confermato dal fatto che i principi stabiliti dalla Corte di Giustizia nella sentenza *Schrems* II si estendono pacificamente anche a questi strumenti. Ciò rende necessaria una valutazione d'impatto sul trasferimento, nonché l'adozione di misure tecniche, contrattuali e/o organizzative supplementari idonee a garantire che i dati trasferiti godano di un livello di protezione equivalente a quello europeo.

15. *Le standard contractual clauses (SCC)*

Il 4 giugno 2021 la Commissione Europea ha emanato nuove clausole contrattuali standard, provvedendo all'elaborazione di quattro moduli[87].

Il primo, che disciplina il rapporto tra titolari del trattamento; il secondo, il rapporto tra titolare del trattamento (esportatore) e responsabile del trattamento (importatore); il terzo, riguardante il rapporto e il trasferimento da responsabile del trattamento (esportatore) a responsabile del trattamento (importatore); e il quarto, concernente il

[86] *Ibidem*.

[87] Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio.

trasferimento dal responsabile del trattamento (esportatore) a titolare del trattamento (importatore).

A queste clausole contrattuali si sono affiancate quelle adottate dal Comitato della Convenzione 108 (T-PD) ad esito della sua quarantaquattresima riunione plenaria tenutasi a Strasburgo dal 14 al 16 giugno 2023. È stato adottato il primo modulo delle SCC per i flussi transfrontalieri di dati personali sviluppate sulla base della Convenzione 108 per i flussi di dati da un titolare del trattamento, firmatario della Convenzione, a un altro titolare del trattamento, non firmatario. Le clausole - precisa il Consiglio d'Europa - possono colmare le lacune di quegli strumenti di trasferimento simili (come quelli esistenti negli Stati membri dell'UE, in America Latina e per i Paesi appartenenti all'ASEAN) e contribuire alla convergenza verso adeguati standard di protezione dei dati a livello globale [88].

Lo strumento delle SCC rappresenta quello più diffuso nella prassi in assenza di una decisione di adeguatezza [89]. Con questo meccanismo l'importatore assume alcuni obblighi nei confronti dell'esportatore e in favore dell'interessato (terzo) [90]. Le clausole costituiscono una fonte di integrazione del contratto e agiscono come forma di eterointegrazione della volontà delle parti [91]. In questo caso, però, la volontà legislativa sembrerebbe sostituirsi integralmente a quella delle parti dal momento che - sebbene le parti possano inserire qualunque altra clausola ritenuta pertinente - le SCC della Commissione europea precisano che il contenuto contrattuale non deve essere incompatibile con le clausole tipo e, sostanzialmente, la loro formulazione letterale deve rimanere intatta [92].

La formulazione della clausola presente nell'ultima decisione di

---

[88] Così il comunicato del 27 giugno 2023 del Consiglio d'Europa disponibile sul sito www.coe.int

[89] G.M. RICCIO, *Model Contractual Clauses,* cit., 875.

[90] *Ivi*, 876.

[91] *Ibidem*.

[92] *Ivi*, 876-877.

esecuzione del 2021 - rubricata "Effetto e invariabilità delle clausole" - è parzialmente differente, prevedendo che le clausole «non siano modificate, tranne per selezionare il modulo o i moduli appropriati o per aggiungere o aggiornare informazioni nell'appendice. Ciò non impedisce alle parti di includere le clausole contrattuali tipo» in questione nel contesto di un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Una simile previsione è prescritta anche nelle clausole tipo elaborate nell'ambito della Convenzione 108 (clausola 3). È previsto infatti che non devono essere modificate, se non per aggiungere o aggiornare le informazioni contenute negli allegati o per scegliere un'opzione qualora sia prevista dalla specifica clausola di riferimento. Ciò non impedisce alle Parti di includere tali Clausole in un contratto più ampio e/o di aggiungere altre clausole o garanzie aggiuntive, a condizione che non siano in contrasto, direttamente o indirettamente, con le Clausole tipo, o con la Legge applicabile, o che non pregiudichino i diritti umani e le libertà fondamentali degli interessati riconosciuti nella Convenzione 108.

In tutti i moduli predisposti, sia dalla Commissione europea che dal Consiglio d'Europa, si rintracciano clausole che definiscono il perimetro dei poteri dell'importatore, le limitazioni della finalità di trattamento, i diritti del terzo, le misure di sicurezza che devono essere adottate oltre a quelle supplementari. I moduli in questione presentano anche alcune clausole dedicate agli obblighi dell'importatore in caso di accesso da parte di autorità pubbliche (clausola 15 per le SCC della Commissione e clausola 23 per quelle del Consiglio d'Europa). In entrambi i casi è prevista una procedura di notifica e, successivamente, un riesame della legittimità e minimizzazione dei dati.

A titolo esemplificativo, le SCC della Commissione prevedono (per il modulo 1) che l'importatore è tenuto ad informare prontamente l'esportatore e, ove possibile, l'interessato (se necessario con l'aiuto dell'esportatore) nel caso in cui i) riceve una richiesta giuridicamente vincolante di un'autorità pubblica, comprese le autorità giudiziarie, a nor-

ma della legislazione del paese di destinazione, di comunicare dati personali trasferiti in conformità delle presenti clausole; oppure se ii) viene a conoscenza di qualunque accesso diretto effettuato, conformemente alla legislazione del paese terzo di destinazione, da autorità pubbliche ai dati personali trasferiti in conformità delle presenti clausole; la notifica comprende tutte le informazioni disponibili all'importatore. La clausola prosegue prevedendo che nel caso in cui la legislazione del paese di destinazione vieti all'importatore di informare l'esportatore e/o l'interessato, «l'importatore accetta di fare tutto il possibile per ottenere un'esenzione dal divieto, al fine di comunicare al più presto quante più informazioni possibili. Per poterlo dimostrare su richiesta dell'esportatore, l'importatore accetta di documentare di aver fatto tutto il possibile». Per il riesame della legittimità della richiesta di comunicazione o di accesso è previsto che l'importatore è tenuto a riesaminare la legittimità di tale richiesta, in particolare il fatto che essa rientri o meno nei poteri conferiti all'autorità pubblica richiedente, e di contestarla qualora, dopo un'attenta valutazione, concluda che sussistono fondati motivi per ritenere che essa sia illegittima a norma della legislazione del paese di destinazione, compresi gli obblighi applicabili a norma del diritto internazionale e dei principi di cortesia internazionale. L'importatore è tenuto ad avvalersi delle possibilità di ricorso [93].

Il contenuto delle clausole e il loro scopo sono ambiziosi benché possa suscitare perplessità la loro effettiva valenza e tutela, soprattutto per un controllo pressocché utopistico da parte del terzo interessato sulla loro concreta applicazione.

[93] Il contenuto della clausola 23 elaborata dal T-PD è molto simile, e quindi di significato equivalente, alla clausola 15 delle SCC del 2021 della Commissione europea.

16. *Trasferimenti o comunicazioni non autorizzati dal diritto dell'Unione (art. 48 GDPR)*

L'art. 48 GDPR disciplina un'ipotesi particolare per il trasferimento di dati verso paesi terzi. Si tratta di quei casi in cui il trasferimento o la comunicazione di dati personali sia disposta da una decisione di un'autorità di uno Stato terzo. Si può dar seguito a queste decisioni allorché fondate su un accordo internazionale tra il paese richiedente e l'UE o un suo Stato membro, fatti salvi gli altri presupposti per il trasferimento a norma del capo V del GDPR.

Su questo meccanismo di trasferimento di dati personali è recentemente intervenuto l'EDPB con le linee guida n. 2/2024 [94].

In questo documento il Comitato riferisce che, per i casi in cui non vi sia alcun obbligo legale derivante da un accordo internazionale per il titolare del trattamento, servendosi di una analisi rimessa caso per caso, ci si può avvalere di altre basi legali previste dall'art. 6 GDPR, sempre che vengano soddisfatti i requisiti previsti nel capo V del GDPR [95].

Il consenso potrebbe essere considerato una base giuridica per il trasferimento verso paesi terzi, ma può rilevarsi inappropriato per alcuni settori, soprattutto se il trattamento dei dati si leghi all'esercizio di poteri dell'autorità. L'EDPB sostiene che la base giuridica di cui alla lett. b), art. 6, GDPR (esecuzione di un contratto) non possa costituire la base giuridica appropriata a fronte di una richiesta di trasferimento o divulgazione da parte di un'autorità di un Paese terzo [96].

In quei casi in cui la divulgazione basata su un accordo internazionale non è obbligatoria, ma la cooperazione è consentita dal diritto europeo o degli Stati membri, l'art. 6, par. 1, lett. e), GDPR potrebbe co-

---

[94] EDPB, *Guidelines 02/2024 on Article 48 GDPR*. Le linee guida precisano che la disposizione in questione non è circoscritta ad ambiti e finalità particolari all'interno dei quali i dati possono essere richiesti dall'autorità di uno Stato terzo.

[95] *Ivi*, § 20, 7.

[96] *Ivi*, § 22, 8.

stituire la base giuridica per il trattamento dei dati personali in quanto si potrebbe ritenere "necessario" per l'esecuzione del compito svolto nel pubblico interesse. In circostanze specifiche e consolidate, l'interesse vitale di una persona interessata (art. 6, par. 1, lett. d, GDPR), potrebbe essere citato come base giuridica per un trasferimento a condizione che siano soddisfatte le condizioni stabilite dal diritto internazionale [97].

Invece, ci si potrebbe avvalere della base giuridica del legittimo interesse solo in circostanze eccezionali, previo un necessario bilanciamento nei riguardi degli interessi e dei diritti fondamentali dell'interessato [98].

Differentemente dalle altre disposizioni del Capo V, la disposizione in commento non forma una base per il trasferimento dei dati poiché non contempla garanzie per la protezione dei dati, ma si limita a chiarire che le decisioni o le sentenze delle autorità di paesi terzi non possono essere riconosciute o eseguite se non esiste un accordo internazionale che lo consente. Pertanto, il titolare o il responsabile del trattamento è tenuto a individuare una base applicabile per il trasferimento in un'altra disposizione del capo V del GDPR [99]. Tuttavia, se un accordo internazionale prevede una cooperazione tra il responsabile del trattamento e l'autorità del paese terzo richiedente, può costituire la base per il trasferimento solo se contempli adeguate garanzie come previsto dall'art. 46, par. 2, lett. a), GDPR [100].

17. *Trasferimento e accesso internazionale ai dati ai sensi del Data Governance Act e del Data Act*

Il recente *Data Governance Act,* ossia, il regolamento UE 868/2022 (DGA), che verrà meglio analizzato nel cap. IV, nel suo capo VII, al-

[97] *Ivi*, § 23-24, 8.
[98] *Ivi*, § 25, 8.
[99] *Ivi*, § 29, 9.
[100] *Ivi*, § 30, 10.

l'art. 31, si preoccupa di stabilire regole anche in riferimento all'eventuale richiesta da parte di un'autorità di un paese terzo avente ad oggetto il trasferimento o l'accesso a dati per i quali l'ente pubblico o la persona a cui è stato concesso il riutilizzo dei dati o l'organizzazione per l'altruismo dei dati ne è in possesso.

In linea generale, questi soggetti devono adottare tutte le misure volte a impedire un simile trasferimento o un accesso nel caso in cui ciò confligga con il diritto europeo o il diritto dello Stato membro. Tuttavia, nel caso in cui la richiesta pervenga a seguito di una decisione o sentenza di un'autorità di un paese terzo, queste sono riconosciute solo in presenza di un apposito accordo internazionale tra il paese terzo e l'UE o lo Stato membro.

In difetto di tale accordo, e qualora la richiesta a seguito di sentenza ponga il destinatario in conflitto con il diritto europeo, il trasferimento può avvenire in presenza di tre condizioni. In primo luogo, l'ordinamento del paese terzo deve essere strutturato in modo da esigere l'indicazione dei motivi nella sentenza (o decisione), la quale deve essere conforme al principio di proporzionalità, oltre a richiedere che essa rispetti la caratteristica della specificità. In secondo luogo, una contestazione da parte del destinatario deve essere oggetto di esame da parte di un'autorità giurisdizionale competente nel paese terzo. In terzo luogo, l'autorità giurisdizionale del paese terzo deve avere il potere di considerare gli interessi giuridici di fornitore dei dati tutelati dal diritto europeo o dal rispettivo Stato membro.

Se queste condizioni sono soddisfatte, il fornitore, previa comunicazione al titolare dei dati da effettuare appena viene ricevuta la richiesta (ad eccezione dei casi in cui ciò preclude le attività di ordine pubblico), può fornire quanto richiesto ma in una quantità minima di dati ammissibile sulla base di una ragionevole interpretazione della richiesta pervenuta.

Il *Data Act*, anch'esso oggetto di analisi nel successivo cap. IV, prevede una norma pressocché equivalente all'art. 32 (capo VII). È previsto che i destinatari della richiesta possono essere i fornitori di servizi di trattamento dei dati. In aggiunta a quanto previsto dal DGA, è previsto il possibile intervento di un pertinente organismo o autorità

nazionale competente per la cooperazione giudiziaria internazionale volto ad accertare l'esistenza di quelle condizioni che possano consentire l'accesso ai dati non personali oggetto di richiesta da parte del paese terzo.

Capitolo III

LA PROTEZIONE DEI DATI E IL DIRITTO DELLA CONCORRENZA NEI MERCATI DIGITALI

Sommario: 1. I risvolti anticoncorrenziali della circolazione dei dati personali nei mercati digitali – 2. I *big data* plasmano i mercati – 3. I "nuovi" poteri privati nei mercati digitali – 4. L'abuso di posizione dominante (art. 3 L. n. 287/1990 - art. 102 TFUE) – 4.1 Abusi di sfruttamento e abusi escludenti – 4.2 La pratica dei prezzi dinamici o personalizzati – 4.3 I potenziali e nuovi orizzonti delle pratiche di *self-preferencing* per il tramite degli assistenti vocali – 5. Il trattamento dei dati personali e la sua rilevanza antitrust – 6. L'intervento chiarificatore della Corte di Giustizia europea sul collegamento tra normativa antitrust e normativa in materia di dati personali: la sentenza CGUE C-252/21 – 7. Il recente caso Apple sull'adozione di politiche di privacy differenziate – 8. Il caso Google - Weople sulla portabilità dei dati personali – 9. Il caso del *Norwegian Consumer Council*

1. *I risvolti anticoncorrenziali della circolazione dei dati personali nei mercati digitali*

L'impianto normativo descritto nei precedenti capitoli non può essere circoscritto al solo ambito della protezione dei dati personali e alla loro circolazione, ma deve necessariamente essere esteso e analizzato alla luce delle potenziali ripercussioni nei mercati digitali. La circolazione dei dati, sia all'interno dello spazio economico europeo che transfrontaliero, produce conseguenze anche in termini concorrenziali e, quindi, di competitività tra imprese [1].

[1] Per alcune riflessioni sulle ripercussioni concorrenziali nel mercato transfron-

La *privacy* e il diritto della concorrenza, infatti, sono collegati nelle industrie ad alta tecnologia. È tuttavia difficile immaginare un mondo online in cui gli utenti si preoccupino di proteggere compiutamente la propria privacy, poiché spesso è emerso che essi hanno una limitata (o addirittura nessuna) scelta effettiva [2]. Le aziende dominanti nei mercati digitali, spesso, non si preoccupano di migliorare le loro politiche in materia di trattamento dei dati perché risulta improbabile che gli utenti giungano a rifiutare il servizio [3]. Questo dato è un primo elemento centrale per le argomentazioni che seguiranno.

La violazione delle norme a tutela della privacy conseguente a un uso illecito e a uno sfruttamento dei dati personali può diventare un modo per fare concorrenza sleale e tale comportamento non implica solamente una violazione delle disposizioni contenute nel GDPR, ma finanche delle norme antitrust [4]. Si può sfociare «in un abuso di posizione dominante oppure in una pratica commerciale scorretta, quando, a tale ultimo riguardo, ad essere violati sono i principi di correttezza e trasparenza delle scelte economiche delle parti deboli» [5].

---

taliero dei dati personali si veda G.G. CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transazionale dei dati personali*, in *diritto dell'informazione e dell'informatica*, vol. 26, n. 4-5, 2015, 909, spec. 910-912. L'A., *inter alia*, sottolinea come «la creazione di un "canale preferenziale" di trasferimento di dati tra un paese comunitario ed un paese terzo sfavoriva le imprese unicamente operanti in Europa poiché, di fatto, venivano eluse le normative sulla sicurezza dei dati e la durata del trattamento per scopi di interesse generale (...) e in senso più ampio si creava un vantaggio competitivo in termini di costi di conformazione ai concorrenti con sede sul territorio statunitense».

[2] F. PASQUALE, *Privacy, Antitrust, and Power*, *George Mason Law Review*, vol. 20, n. 4, 2013, 1009, spec. 1022.

[3] *Ibidem*.

[4] C. PERARO, *Quando la violazione della privacy costituisce un illecito antitrust: quali rimedi nell'ordinamento UE?,* in *Eurojus*, n. 3, 2023, 53.

[5] *Ibidem*. Si veda altresì il richiamo a G. MUSCOLO, *Big data e concorrenza: quale rapporto?*, in V. Falce, G. Ghidini, G. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, Giuffrè, 2018, 173-191; W. KERBER, *Digital Markets, data and a privacy: competition law, consumer law and data protection*, in *MAGKS Joint Discussion Paper Series in Economics*, n. 14, 2016, *Philipps-University Marburg, School of Business and*

Uno dei casi in cui si può prospettare una sinergia tra la disciplina antitrust e quella di *data protection*, ad esempio, si ha quando una piattaforma digitale acquisisce un concorrente che, nel proprio patrimonio, possiede una estesa massa di dati e procede quindi a incrociare i dati presenti su entrambi i *network* senza avere informato gli utenti dell'una e dell'altra piattaforma. Il caso emblematico che si è verificato è quello della acquisizione nel 2014 di WhatsApp da parte di Facebook [6].

Un'altra fattispecie che può essere annoverata è quella della collusione algoritmica [7]. Si ipotizza come in alcuni casi gli algoritmi, avvalendosi di sistemi di intelligenza artificiale, riescano a realizzare equilibri collusivi in modo autonomo, spontaneo e tacito [8]. In particolare, lo scenario riguarderebbe alcuni algoritmi progettati per realizzare condotte individuali che massimizzino il profitto, e quindi, non diret-

---

Economics, *Marburgpp*, spec. 3 ss.; A. Canepa, *I mercati digitali*, Torino, Giappichelli, 2020, 118.

[6] C. Peraro, *Quando la violazione della privacy costituisce un illecito antitrust,* cit., 55. L'A. riprende la questione dell'acquisizione WhatsApp/FB rilevando che l'operazione è stata ammessa dalla Commissione per il fatto che l'acquirente e l'impresa *target* erano attivi su mercati rilevanti diversi e non ci sarebbe stata minore disponibilità di dati personali. In quella sede, ossia nell'indagine per verificare la compatibilità con le norme antitrust, l'impatto sulla *privacy* non era stato verificato. Nel 2017, però, FB aggiornando i termini del servizio aveva disposto il collegamento tra i numeri di telefono della chat e i profili del *social network*. Nel 2017, quindi, l'autorità antitrust europea irrogava perciò una sanzione di 110 milioni di euro a FB perché nell'occasione dell'acquisizione ha fornito indicazioni inesatte e fuorvianti per quanto riguarda la possibilità di abbinare automaticamente le ID di FB con il numero mobile di WA. L'A. illustra poi come il caso sia stato oggetto di attenzione anche da parte dell'AGCM italiana e del Garante italiano per la protezione dei dati personali. Quest'ultimo, nel 2018, ha vietato a WhatsApp di comunicare i dati dei propri utenti il cui consenso sia stato ottenuto con modalità illegittime e a FB di effettuarne ogni ulteriore trattamento.

[7] A. Ittoo, N. Petit, *Algorithmic Pricing Agents and Tacit Collusion: A Technological Perspective*, in *L'intelligence artificielle et le droit, Hervé Jacquemin and Alexandre De Streel (eds), Bruxelles: Larcier,* 2017, 241-256.

[8] M. Filippelli, *La collusione algoritmica*, in *orizzonti del Diritto Commerciale*, Fasc. Sp. 2021, 375, spec. 383.

tamente programmati per colludere. Essi, con il giusto supporto tecnologico, sarebbero «in grado di apprendere in modo autonomo (senza supervisione, esplorando l'ambiente di mercato e interagendo con gli altri operatori) e di elaborare processi decisionali autonomi», in modo che lo strumento tenderà a replicare le strategie di successo e a non replicare le altre [9]. Dunque, gli algoritmi agiscono in modo genuinamente tacito e autonomo finendo però per realizzare condotte allineate, con esiti simili a quelli tipici di un cartello; essi individuano la migliore strategia, il migliore livello di prezzo collusivo mantenendolo nel tempo [10].

Dunque, esistono algoritmi di *pricing* molto semplici che si basano su regole predefinite, come quella di allinearsi al prezzo più basso del mercato o di rimanere al di sotto/sopra di una determinata soglia rispetto al prezzo più basso di "mercato" e algoritmi di *pricing* più avanzati, i quali agiscono in forza di modelli predittivi e, grazie a tecniche di *machine learning*, creano autonomamente le strategie ottimali di prezzo al fine di massimizzare i profitti. Come è stato sottolineato dall'AGCM, «la difficoltà di rintracciare l'ingrediente decisivo per una violazione dell'art. 101 TFUE – lo scambio di volontà - in presenza di algoritmi sofisticati, caratterizzati da meccanismi di *machine learning*

---

[9] *Ibidem*.

[10] *Ibidem*. L'A. aggiunge, 385, che fino a qualche anno fa «la possibilità di collusione tacita algoritmica appariva irrealistica: equilibri collusivi stabili – si sosteneva, con argomenti che riprendevano quelli già espressi con riguardo alla collusione tacita in oligopolio – richiedono una qualche forma di comunicazione, un qualche input esterno, cosicché, mentre è realistico che la collusione possa beneficiare del supporto facilitante degli algoritmi, appare irrealistico che un allineamento di condotte, che mima gli effetti tipici di un cartello, sia realizzato direttamente da algoritmi intelligenti, con condotte individuali e non concertate. Oggi, persiste ancora un certo scetticismo di fondo, ma tale possibilità comincia a essere percepita come sempre meno remota e sempre meno irrealistica; e anzi qualcuno non esclude che algoritmi di questo tipo siano già a disposizione delle imprese e già in uso nelle vendite online». L'A. riporta F. BENEKE, M.O. MACKERODT, *Remedies for algorithmic tacit collusion*, in *Journal Antitrust Enforcement*, 2020, 1-3; J.E. HARRINGTON, *Developing Competition Law for Collusion by Autonomous Artificial Agent*, in *Jour. Comp. L. & Econ.*, n. 14, 2018, 331.

è, a dir poco, complicata»[11]. Sulla concreta possibilità di una collusione algoritmica tacita, in realtà, ci sono differenti linee di pensiero; infatti, secondo la tesi oggi maggioritaria, benché i progressi tecnologici abbiano compiuto importanti passi in avanti, non si può ancora parlare di una vera e propria collusione tacita tramite algoritmi[12].

Al di là delle ipotesi di collusione, in letteratura si è tentato di identificare e, in un certo senso, di tipizzare alcune condotte delle imprese cc.dd. *big tech* in grado di ripercuotersi negativamente sugli utenti e di produrre conseguenze anticoncorrenziali. Una di queste può riguardare la modifica arbitraria del *ranking* dell'utente commerciale allorché vi sia una carenza di trasparenza nei parametri che rende impossibile comprendere come migliorare la propria posizione[13].

La piattaforma, inoltre, potrebbe comportarsi come concorrente e applicare le pratiche di *self-preferencing*[14] favorendo, quindi, la propria offerta di acquisto, costituendo una forma di *leveraging*, ossia una espansione del potere di mercato già detenuto rispetto a un determinato bene o servizio verso un differente mercato più o meno contiguo al primo[15].

Da quanto sinora prospettato appare evidente come il soggetto che nel mercato agisce violando o eludendo la normativa in materia di

---

[11] In tal senso si veda AGCM, *Indagine conoscitiva sui big data*, 2020, 113, consultabile al sito www.agcm.it

[12] A. Ittoo, N. Petit, *Algorithmic pricing agents and tacit collusion: A technological perspective*, *TILEC discussion Paper*, vol. 54, 2010, 255-256.

[13] F. Ruggeri, *Poteri privati e mercati digitali*, Roma tre-press, 2023, 122.

[14] Sulle pratiche di *self-preferencing* come illeciti antitrust si veda A. Licastro, *Il* self-preferencing *come illecito antitrust?*, in *Il diritto dell'economia*, vol. 105, n. 2, 2021, 401.

[15] F. Ruggeri, *Poteri privati e mercati digitali*, 124. Questo non sarebbe di per sé un comportamento anticoncorrenziale (cfr. Trib. UE, Grande sezione, 17 settembre 2007, T-201/04). La condotta diventa abusiva solo se produce effetti escludenti di alcuni soggetti o prodotti dal mercato. Sarebbe possibile per la piattaforma allorché riesca a controllare l'accesso alle informazioni e/o il flusso delle stesse, ossia quel capitale informativo che gli garantisce questo ruolo.

protezione dei dati personali sia in grado di trarre un illegittimo vantaggio competitivo e, perciò, sanzionabile.

Le violazioni della normativa sulla protezione dei dati personali possono essere le più varie e non compendiabili in poche battute. Tuttavia, i casi in cui ci si può focalizzare riguardano non solo le ipotesi di violazione del principio di trasparenza, ma anche il diritto alla portabilità dei dati (art. 20 GDPR), soprattutto per impedire la formazione di fenomeni di *lock-in* che costringono l'interessato a rimanere "bloccato" all'interno di un certo servizio [16].

La recente evoluzione dei mercati digitali che si avvalgono di *big data*, perciò, consente di ridefinire la struttura stessa dei mercati digitali.

2. *I big data plasmano i mercati*

I *big data* sono un elemento cruciale nei mercati digitali moderni. Sulla loro definizione non c'è univocità e ciascuno ne ha elaborato una propria [17]. I fattori che maggiormente li identificano sono rappre-

---

[16] *Ivi*, 141. Il diritto alla portabilità dei dati si riferisce ai soli dati personali e se tale diritto non fosse previso o consentito nell'ambito di una relazione tra imprese, si sarebbe di fronte a un comportamento idoneo ad assumere i tratti di un abuso di potere che eccede la lesione del corretto trattamento dei dati personali dell'individuo. Cfr. I. GRAEF, M. HUSOVEC, N. PURTOVA, *Data Portability and Data Control*: *Lessons for an Emerging Concept in EU Law,* in *German Law Journal,* vol. 19, n. 6, 2018, 1359-1398.

[17] B. VAN DER SLOOT, S. VAN SCHENDEL, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, in *Journal of intellectual Property, Information Technology and E-Commerce Law*, vol. 7, n. 2, 2016, 113. Gli AA. riportano gli esempi di alcuni Stati tra cui la Germania: «*in Germany, Big Data is defined as 'das Synonym für den intelligenten Umgang mit solchen großen oder auch heterogenen Datenmengen'(synonymous with the intelligent use of large or heterogeneous datasets*)»; gli Stati Uniti: «*The Podesta Report (United States) builds on the Gartner definition and suggests that there are many definitions of 'Big Data' which may differ depending on whether you are a computer scientist, a financial analyst, or an entrepreneur pitching an idea to a venture capitalist. Most definitions re-*

sentati dalle cc.dd. cinque V, ossia, volume, varietà, velocità, veridicità e valore [18]. In altri termini, si è al cospetto di *set* di dati la cui dimensione o tipologia trascende la capacità dei tradizionali *database* di acquisire, gestire ed elaborare i dati con bassa velocità. Le fonti di dati sono divenute ormai più articolate e complesse rispetto a quelle tradizionali poiché "guidate" da sistemi di intelligenza artificiale (IA) e da dispositivi dell'*Internet of Things* (*IoT*).

I *big data* oggi sono una componente che consente di misurare il potere economico aziendale inteso come capacità per l'impresa di raccogliere e diffondere dati. La loro incidenza in ambito concorrenziale è ormai un elemento sempre più consolidato e indiscusso; il rischio è quello di generare forme di posizioni dominanti proprio in virtù delle quantità di dati raccolti e analizzati [19].

---

flect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data. In other words, 'data is now available faster, has greater coverage and scope, and includes new types of observations and measurements that previously were not available.' More precisely, Big Datasets are 'large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future»; l'Estonia: «*the Estonian DPA describes Big Data as collected and processed open datasets, which are defined by quantity, plurality of data formats, and data origination and processing speed*»; la Francia: «*The French DPA refers to a definition adopted by the French General Commission on terminology and neology (Commission générale de terminologie et de néologie). The official translation of Big Data in French is 'mégadonnées', which stands for data, structured or otherwise, whose very large volume require appropriate analytical tools*».

[18] Con volume ci si riferisce alla mole dei dati; la velocità fa riferimento alla generazione dei dati ma anche alla velocità nell'accesso dei dati e al modo in cui questi vengono elaborati ed analizzati; la varietà si riferisce alla diversità delle informazioni che i dati possono contenere. Le aziende orientate ai dati potrebbero non solo essere interessate alla raccolta di una particolare tipologia di dati fornita dai consumatori bensì mirano potenzialmente a ottenere specifici dati da particolari clienti; il valore sta a significare che i *Big Data* producono ricchezza dal momento che le inferenze derivanti da essi permettono di intraprendere attività commerciali tra loro non mutualmente escludenti; la veridicità, invece sta semplicemente a riferirsi all'attendibilità delle informazioni.

[19] EDPS, Opinion n. 8/2016, *On coherent enforcement of fundamental rights in the age of big data*, 23 Settembre 2016, 16.

In base al grado della loro rilevanza nei processi competitivi si possono operare distinzioni su differenti categorie di mercati [20]. Si possono configurare mercati in cui l'utilizzo dei *big data* ha un rilievo poco significativo nella fornitura del bene o del servizio [21] oppure mercati in cui questo utilizzo è in grado di avere una incidenza sulle condizioni di offerta del servizio in termini di qualità [22]. Esistono, infine, mercati dove l'utilizzo di questi dati costituisce un elemento fondamentale perché da ciò ne discende la funzione propria del bene o servizio di cui si tratta, in specie per l'innovazione e/o la personalizzazione del servizio [23].

La rilevanza dei *big data* - unitamente alla qualità, natura e quantità di dati necessari a competere in un determinato mercato - contribuisce a verificare in quale misura essi possano provocare una distorsione della concorrenza e, quindi, un illecito antitrust creando barriere all'ingresso. Nella prassi, i dati in questione sono detenuti per lo più dalle grandi piattaforme digitali che per la loro capacità di definire il perimetro delle regole del servizio vengono inquadrate come le detentrici di "poteri privati" assimilabili ai poteri pubblici che legiferano.

---

[20] In tal senso si veda AGCM, Indagine conoscitiva sui *big data*, cit., 70.

[21] Si tratta di mercati nei quali i *Big Data* sono parificabili ad altri fattori utilizzati dalle imprese come quelli volti a migliorare la propria efficienza produttiva, senza però incidere in maniera significativa sul processo competitivo.

[22] Questa incidenza in termini di qualità la si può riscontrare nei settori caratterizzati da elevate asimmetrie informative come nei tradizionali mercati in cui c'è già in impatto significativo dei dati, come quelli finanziari, bancari e assicurativi. La raccolta e l'analisi di una quantità sempre maggiore di dati porta a conoscere maggiormente i processi e i clienti, consentendo l'adozione di decisioni che possono favorire positivamente ogni aspetto dell'attività di impresa.

[23] In questo caso, ad esempio, siamo proprio nel campo della pubblicità online personalizzata.

3. *I "nuovi" poteri privati nei mercati digitali*

È ormai conclamato che i mercati digitali sono governati da imponenti piattaforme che creano loro stesse le regole e influenzano le dinamiche tra utenti e operatori grazie alla dominanza di cui godono [24]. Si tratta delle già citate *big tech*, le cc.dd. GAFAM.

Le conseguenze che derivano dalle pratiche di questi giganti del mondo digitale sono varie e in grado di provocare effetti di diversa natura. Nell'ambito della responsabilità civile e nel solo settore dell'*e-commerce* sono stati identificati almeno tre profili di grande interesse: (i) i rapporti con i produttori esterni ai quali la società mette a disposizione la piattaforma per la vendita degli articoli: la distribuzione selettiva può creare disparità di trattamento tra produttori e alterare il gioco della concorrenza; (ii) l'uso del marchio dei fabbricanti di cui la società intermediaria pone in vendita i prodotti; (iii) ed ancora la responsabilità della società per i difetti dei prodotti fabbricati da altre imprese e collocati in vendita sulla sua piattaforma [25].

Queste piattaforme sono state in grado di indebolire le più tradizionali nozioni del diritto antitrust come quella di benessere del consumatore, la definizione di mercato rilevante, di potere di mercato e dello stesso abuso di posizione dominante [26].

---

[24] F. Ruggeri, *Poteri privati e mercati digitali*, cit., 113, ha rilevato come la capacità di alcune piattaforme di creare e imporre le regole più appropriate per il soddisfacimento delle proprie esigenze costituisce espressione dell'affermazione di specifici poteri privati, in questo caso di natura tecnologica che, nell'arco di pochi anni, sono diventati sempre più saldi e meno contendibili. Si veda altresì S. Sileoni, *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Milano, Cedam, 2011, 9, che individua nel cambiamento del ruolo degli attori pubblici le cause dell'emersione di una sempre maggiore tendenza all'autoregolamentazione da parte dei privati; P. Bonini, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in *Federalismi.it*, n. 11, 2020, 265.

[25] G. Alpa, *Amazon in Tribunale*, in *Contratto e impresa*, vol. 40, n 4, 2024, 973, spec. 974.

[26] E. Cremona, *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in *Osservatorio sulle fonti*, n. 2, 2021, 879, spec. 887. L'A. sottolinea co-

Le dinamiche dei mercati digitali hanno messo in discussione lo stesso significato di *speciale responsabilità* dell'impresa in posizione dominante e, quindi, la sua lunga tradizione in materia di concorrenza, portando all'esigenza di prevedere obblighi di protezione più incisivi a carico dei nuovi poteri privati e non solo di mera informazione nei confronti degli utenti [27].

È stato segnalato come i nuovi protagonisti del mondo digitale abbiano portato anche a un cambio di paradigma lessicale nelle condizioni generali di contratto. In altri termini, mentre la prassi contrattuale ha sempre previsto una formulazione che ricalca le espressioni proprie dei testi normativi, nel caso delle *big tech* viene utilizzato un tono colloquiale, persuasivo ed espositivo, come se si rivolgessero direttamente all'utente coinvolgendolo nel discorso [28]. Tra l'altro, gli effetti giuridici di tali condizioni sono dati per scontati e le condizioni «sono presentate come regole del servizio come se esse fossero incorporate nel servizio. Un servizio cioè effettuato sulla base del regolamento privato imposto agli utenti tramite le clausole contrattuali da esse predisposte. Di qui la convinzione del cliente (non giurista) che si rivolge alla piattaforma che le regole siano per così dire "connaturate" al servizio». Non viene percepita alcuna imposizione dall'utente e la piattaforma si presenta come se fosse un cooperatore solidale [29].

Il mercato digitale, perciò, costituisce una sfida per il giurista che si interroga sul rapporto tra tecnologia e regole, chiedendosi "se" e "quale" debba essere la regolamentazione, ovvero se oggetto della re-

---

me questo intervento dirompente sia stato tale che un elevato numero di Autorità di regolazione del mercato ha avviato, nel corso degli ultimi due anni, studi e indagini conoscitive sulla c.d. *digital competition*.

[27] *Ivi*, 904.

[28] G. ALPA, *Sul potere contrattuale delle piattaforme digitali*, in *Contratto e impresa*, vol. 32, n. 3, 2022, 728-729; sulla struttura di questi contratti e sulle condizioni generali di contratto si veda anche E. PODDIGHE, V. ZENO-ZENCOVICH, *La «correttezza» nelle condizioni generali di contratto delle grandi piattaforme online*, in *Comparazione e diritto civile*, n. 1, 2024, 1.

[29] *Ibidem*.

golamentazione debbano essere le piattaforme o gli algoritmi su cui si fondano [30].

La concentrazione del potere di mercato e, soprattutto, l'abuso della posizione dominante, è stata storicamente combattuta per il suo rischio intrinseco di distorcere l'efficace allocazione delle risorse, mentre i prezzi perdono la loro funzione di indicatori della scarsità. Il grande problema posto dalla struttura del mercato digitale è stato il venir meno del prezzo, sostituito da quel concetto di "gratuità", già visto nel cap. I, che in sostituzione del prezzo monetario ha visto un corrispettivo composto da dati personali [31].

Un primo superamento dell'esitazione per un intervento antitrust in caso di prezzi bassi o nulli [32] si è verificato allorché nel 2016 la Commissione europea si è trovata a esaminare la fusione della Piattaforma LinkedIn in Microsoft [33]. In quella sede, si è ravvisato che la tutela dei dati personali, benché non faccia parte in modo diretto del diritto della concorrenza, può avere una incidenza antitrust se i consumatori la percepiscono come «un fattore di qualità del servizio e le imprese concorrano tra loro anche sulla base di tale fattore» [34].

L'espressione del potere delle *big tech* nell'ambito dei mercati di cui si discute può essere sintetizzata con tre modalità di azione:

---

[30] R. Lener, *Tecnologie e attività finanziaria*, in *Il trattamento dei dati tra etica, diritto ed economia, Atti del XIV Convegno nazionale della Società Italiana degli Studiosi del Diritto Civile*, Napoli, Edizioni scientifiche italiane, 2020, 204; Su mercato digitale e finanza, in particolare, si veda P. Lucantoni, *Strumenti digitali e finanza*, in *Banca d'Italia,* in F. Maimeri, M. Mancini (a cura di), *Quaderni di ricerca giuridica n. 87*, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, 2019, 291-310.

[31] Per una chiara esposizione del tema si veda E. Cremona, *L'erompere dei poteri privati,* cit., 888.

[32] S. Mannoni, G. Stazi, *Is Competition a Click Away*?, Napoli, Editoriale Scientifica, 2018, 18.

[33] E. Cremona*, L'erompere dei poteri privati*, 890.

[34] *Ibidem*. L'A. prosegue a pag. 891 rilevando che il *trend* descrive una maturata concezione dei *big data* come viatico per la formazione di monopoli (una sorta di *essential facility*).

a) il *gatekeeper power*, costituivo del controllo del mercato che nasce dal c.d. effetto di rete e dalla conseguente acquisizione di dati;

b) il potere di *leveraging*, che consente all'impresa di avvalersi della propria posizione dominante per ottenere ulteriori benefici da mercati ancillari o separati;

c) lo sfruttamento delle informazioni a disposizione< che consente di discriminare i consumatori o gli utenti commerciali che fruiscono dell'intermediazione della piattaforma per raggiungere i mercati di loro interesse [35].

L'effetto di rete, in particolare, fa sì che il soggetto con più utenti, disponendo di più dati per migliorare il proprio servizio, attira a sua volta più utenti e riesce a creare effetti di rete diretti che, da un lato, generano barriere all'uscita per gli utenti e, dall'altro, introducono barriere in ingresso per nuovi concorrenti [36]. L'elevata qualità e quantità di dati, peraltro, consente di generare effetti di rete indiretti poiché creano valore per gli inserzionisti pubblicitari consentendo di aumentare i ricavi da poter investire nel servizio in termini di qualità.

L'effetto di rete che produce una barriera all'ingresso per potenziali concorrenti fa sì che un nuovo operatore è tenuto a offrire un servizio migliore e convincere tutti gli utenti ad abbandonare il servizio concorrente [37]. L'ulteriore difficoltà di un nuovo operatore riguarda l'accesso ai dati degli utenti. L'effetto di rete infatti ha un ruolo essenziale nella raccolta di dati oltreché nelle economie di scopo. Il primo, perché provoca un aumento del numero utenti, il secondo perché l'aumento del numero della varietà di servizi offerti dalla piattaforma incrementa le fonti e i tipi di dati collezionabili [38].

Tuttavia, si deve qui anticipare che gli effetti di rete non comportano scontate conseguenze anticoncorrenziali, poiché ci sono casi ove

---

[35] RUGGERI, *Poteri privati e mercati digitali,* cit.*,* 113.

[36] P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, in AISDUE, vol. 2, n. 2, 2021, 36.

[37] *Ibidem*.

[38] *Ivi*, 37.

questi costituiscono semplicemente un valore aggiunto della piattaforma per gli utenti (v. *infra* cap. V, § 7).

Nei successivi paragrafi ci si soffermerà in particolare sulla conseguenza relativa all'abuso di posizione dominante e, nel capitolo successivo, alle novità normative dei mercati digitali come il *Digital Markets Act* e il *Digital Services Act*.

4. *L'abuso di posizione dominante (art. 3 L. n. 287/1990 - art. 102 TFUE)*

L'istituto dell'abuso di posizione dominante rappresenta un illecito antitrust con una storia piuttosto articolata dovuta alla difficoltà di individuare parametri oggettivi di applicazione. Si sono avvicendate differenti teorie dottrinali e orientamenti giurisprudenziali con i quali si è tentato di definirne i contorni.

La fonte normativa nazionale che disciplina l'istituto dell'abuso di posizione dominante è rintracciabile nella legge n. 287 del 10 ottobre 1990, la quale, all'art. 3 vieta quelle condotte abusive da parte di una o più imprese in una situazione di posizione dominante all'interno del mercato nazionale o in una sua parte rilevante [39]. La stessa disposizione vieta, in modo specifico, alcune condotte anticoncorrenziali, riprendendo pedissequamente le ipotesi sancite dall'art. 102 TFUE (già art. 82 TCE) che rappresenta la fonte normativa dell'istituto a li-

[39] L'art. 3, Legge n. 287/1990, prevede che: è vietato l'abuso da parte di una o più imprese di una posizione dominante all'interno del mercato nazionale o in una sua parte rilevante, ed inoltre è vietato: a) imporre direttamente o indirettamente prezzi di acquisto, di vendita o altre condizioni contrattuali ingiustificatamente gravose; b) impedire o limitare la produzione, gli sbocchi o gli accessi al mercato, lo sviluppo tecnico o il progresso tecnologico, a danno dei consumatori; c) applicare nei rapporti commerciali con altri contraenti condizioni oggettivamente diverse per prestazioni equivalenti, così da determinare per essi ingiustificati svantaggi nella concorrenza; d) subordinare la conclusione dei contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari che, per loro natura e secondo gli usi commerciali, non abbiano alcuna connessione con l'oggetto dei contratti stessi.

vello europeo [40]. La disciplina che riguarda l'applicazione delle regole di concorrenza, invece, è contenuta nel regolamento (CE) n. 1 del 2003.

Le barriere all'espansione o all'ingresso in un mercato a cui si fa riferimento nelle norme citate possono presentarsi sotto diverse forme, tra cui quelle di natura giuridica come: l'imposizione di tariffe o quote, l'accesso privilegiato a fattori di produzione o risorse naturali essenziali, nonché a tecnologie importanti; oppure, può trattarsi di barriere costituite da costi e altri impedimenti derivanti da effetti di rete, così come lo stesso comportamento dell'impresa dominante. Sostanzialmente, le barriere possono essere di fatto, quando attengono al funzionamento del mercato che si considera, tra cui si possono ricomprendere quelle di tipo tecnico, come le barriere afferenti alla conoscenza, e quelle economiche, afferenti ad esempio all'accesso alle materie prime [41].

Le ipotesi di abuso di posizione dominante, nella maggior parte dei casi, riguardano il lato dell'offerta. Tuttavia, sebbene siano rari, si potrebbero verificare casi di posizione dominante anche dal lato della domanda [42]. In questi casi si parlerebbe di *monopsonio*, facendo riferimento a quei mercati dove opera un solo compratore [43].

---

[40] L'art. 102 TFUE prevede che: è incompatibile con il mercato interno e vietato, nella misura in cui possa essere pregiudizievole al commercio tra Stati membri, lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo. Tali pratiche abusive possono consistere in particolare: a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque; b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori; c) nell'applicare nei rapporti commerciali con gli altri contraenti condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio per la concorrenza; d) nel subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi.

[41] Sentenza C-27/76, *United Brands*.

[42] V. MANGINI, G. OLIVIERI, *Diritto Antitrust*, Torino, Giappichelli, 2000, 51.

[43] *Ivi*, 51-52. Gli AA. segnalano come nell'ipotesi in cui il monopsonio (o i con-

Una prima fase dell'analisi dell'abuso di posizione dominante deve riferirsi all'individuazione del mercato rilevante [44]. È infatti necessario perimetrare il mercato rilevante attraverso l'analisi della sostituibilità della domanda in base ai beni e ai servizi intercambiabili dai consumatori e in considerazione di quelle che sono le loro caratteristiche, i prezzi, le loro abitudini e le loro tendenze [45]. È una valutazione che deve avvenire in riferimento a una specifica area geografica ove sussistano omogenee condizioni di concorrenza [46].

Le quote di mercato detenute dall'impresa rappresentano evidente-

---

sorzi di acquisto) servono a «fronteggiare una posizione dominante dal lato dell'offerta, non daranno luogo a fattispecie lesiva della concorrenza se, e nella misura in cui, i vantaggi derivanti da tale posizione di forza vengano trasferiti sui consumatori finali dei beni».

[44] A. Geraci, *Condotta anticoncorrenziale e perimetrazione del mercato rilevante*, in *Rivista di diritto industriale*, n. 6, 2015, 537, spec. 542. Secondo la giurisprudenza di legittimità «(...) la definizione del "mercato rilevante" costituisce una operazione preliminare per l'accertamento dell'illecito concorrenziale, da effettuare dando applicazione ai principi vigenti nell'Unione europea che informano le norme nazionali in materia di concorrenza, tenendo conto del grado di sostituibilità della domanda (ed eventualmente dell'offerta), in presenza di beni e servizi intercambiabili dal consumatore in ragione dei prezzi e delle caratteristiche oltre che delle sue abitudini e tendenze, con riferimento ad una determinata area geografica nella quale le condizioni di concorrenza sono sufficientemente omogenee», Cass. civ., Sez. I, 12 novembre 2019, n. 29237, CED Cassazione, 2019.

[45] Per un'analisi della definizione di mercato rilevante si veda M. D'Ostuni, M. Beretta, *Il diritto della concorrenza in Italia*, Torino, Giappichelli, 2021, 139 e ss.; sulla sostituibilità in tema di *big data* ne parla F. Di Porto, *La rivoluzione big data. Un'introduzione*, in *Concorrenza. e mercato*, n. 23, 2016, 5.; sui *big data* e sulla definizione del mercato rilevante si veda V. Bagnoli, *The big data relevant market*, in *Concorrenza. e mercato*, n. 23, 2016, 73.

[46] Cass. civ., Sez. I, 04 giugno 2015, n. 11564, nota di Geraci in *diritto industriale*, n. 6, 2015, 537; secondo Cass. civ., Sez. I, 17 maggio 2000, n. 6368, per stabilire se sussista abuso di posizione dominante, procedendo alla ricerca della concorrenza virtuale - e cioè di quella che sarebbe rimasta se la posizione dominante non fosse stata esercitata nel modo che si pretende abusivo - occorre preliminarmente definire il mercato di riferimento, o mercato rilevante, in relazione sia alla sua estensione geografica, sia all'area di sostituibilità dei prodotti e dei servizi in questione.

mente il primo elemento di valutazione da analizzare in virtù delle condizioni di mercato rilevanti e in virtù della dinamica del mercato e del grado di differenziazione dei prodotti. Esse costituiscono un importante indicatore, poiché quote di mercato modeste generalmente comportano, presuntivamente, l'assenza di un considerevole potere di mercato [47].

Anche la Commissione europea, con la comunicazione del 2009 riguardante gli "Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti", [48] ha posto in risalto il presupposto della posizione dominante quale base di partenza per accertare l'applicabilità dell'art. 82 TCE (oggi art. 102 TFUE). Perciò, la Commissione definisce la posizione dominante «come una situazione di potere economico grazie alla quale l'impresa che la detiene è in grado di ostacolare il persistere di una concorrenza effettiva sul mercato in questione e di agire in maniera significativamente indipendente rispetto ai suoi concorrenti, ai suoi clienti e, in ultima analisi, ai consumatori».

Dal canto suo, la giurisprudenza europea nelle sue prime pronunce in materia (anni '70 e '80) ha fornito una definizione di posizione dominante identificandola come una *sostanziale indipendenza* di una determinata impresa rispetto alle possibili reazioni di concorrenti, fornitori e clienti alle proprie condotte; perciò, è stata elaborata la formula della *speciale responsabilità* facente capo all'impresa dominante [49]. Per il suo potere di mercato, quell'impresa è tenuta a comportarsi in maniera tale da non impedire la sussistenza di una concorrenza effettiva nel mercato di riferimento. Dunque, si configurerebbe un abuso allorché ven-

---

[47] Sul tema delle quote di mercato si veda CGUE, C-85/76, 13 febbraio 1979, *Hoffmann-La Roche*, Racc. 1979, 461, § 39-41, eur-lex.europa.eu.

[48] Comunicazione Commissione europea 2009/C45/02.

[49] M. LIBERTINI, *Abuso del diritto e abuso di posizione dominante*, in *orizzonti del diritto commerciale*, n. 3, 2018, 7.

ga violato il dovere di comportarsi secondo criteri di *speciale responsabilità* [50].

Dalla formula in questione ne deriva un importante principio consistente nel fatto che non rileva se la condotta di una impresa sia qualificata come lecita da una norma di diritto privato o di diritto amministrativo, o costituisca l'esercizio di un diritto; ciò non impedisce che la condotta possa essere qualificata come restrittiva della concorrenza e quindi abusiva, benché formalmente lecita [51].

Nella casistica giurisprudenziale, le prime sentenze europee succedutesi fino alla Comunicazione della Commissione del 2009 si incentravano su un approccio di tipo economico, di tendenza statunitense. Veniva riconosciuta una particolare centralità ai cc.dd. abusi escludenti (ancora oggi predominanti) [52] e la condotta avrebbe dovuto considerarsi illecita solo se induceva a una esclusione dal mercato dei concorrenti generando una riduzione del benessere del consumatore [53]. Ma, stando a una impostazione di tal fatta, non tutti i comportamenti escludenti sarebbero di per sé illeciti dal momento che il successo di un'impresa può essere conquistato attraverso innovazioni di successo o mediante riduzioni di prezzi dovute a una maggiore efficienza produttiva [54].

In buona sostanza, la particolare efficienza dell'impresa in posizio-

---

[50] Questa formula viene ancora oggi utilizzata dalla Commissione europea e ripresa dalle pronunce della Corte di giustizia europea come CGUE, C-413/14, 6 settembre 2017, *Intel Corp. Inc.*, curia.europa.eu.

[51] M. Libertini, *Abuso del diritto e abuso di posizione dominante,* cit., 8.

[52] In realtà, come testimoniato da una rassegna delle istruttorie avviate e concluse negli ultimi anni dell'AGCM, v'è una predominanza delle istruttorie relative a condotte escludenti. Si veda a tal proposito N. M. Naso, *Abusi di posizione dominante (Anno 2021)*, in *Concorrenza e mercato*, n. 1, 2022, 291, spec. 292 e 300.

[53] M. Libertini, *Abuso del diritto e abuso di posizione dominante,* cit., 9.

[54] *Ibidem*. L'A. sottolinea però che in quei casi in cui le ragioni del successo non possono essere ricostruite in modo lineare, la Commissione tende ad ammettere presuntivamente il carattere abusivo dell'effetto escludente e a porre sull'impresa dominante l'onere di provare i guadagni di efficienza e di benessere del consumatore, prodotti dalla sua condotta.

ne dominante, così come la sua peculiarità in termini di innovazione, non può di per sé essere associata al concetto di barriera all'espansione o all'ingresso nel mercato, rimanendo solamente una mera indicazione dell'elemento di dominanza [55].

Quindi, il criterio di definizione delle condotte abusive che si è venuto a sviluppare nelle più recenti elaborazioni della Corte di giustizia è quello della concorrenza basata sui meriti [56].

Quest'ultima viene intesa come meritevolezza dell'impresa per il successo conseguito grazie alla qualità delle proprie offerte commerciali valutate dalla *libera scelta* dei consumatori. Nel corso degli anni, si è tentato di elaborare un test idoneo a condurre a conclusioni tecnicamente verificabili di questo criterio come il benessere dei consumatori [57]. Il tentativo è stato effettuato nonostante la difficoltà di costruire un test affidabile per misurare tale benessere, soprattutto considerando che i bisogni dei consumatori non sono definibili staticamente e

---

[55] Si veda la sentenza CGUE C-27/76, 14 febbraio 1978, *United Brands*, § 125, eur-lex.europa.eu.

[56] CGUE, C-202/07, 2 aprile 2009, *France Télécom*, § 109, eur-lex.europa.eu; CGUE, C-280/08, 14 ottobre 2010, *Deutsche Telekom*, § 177; CGUE, C-457/10, 6 dicembre 2012, *Astra Zeneca*, § 75; CGUE, Grande Sez., C-209/10, 27 marzo 2012, *Post Danmark*, § 25; CGUE, Grande Sez C-413/14, 6 settembre 2017, *Intel*, § 136, eur-lex.europa.eu, riprese da M. LIBERTINI, *Abuso del diritto e abuso di posizione dominante,* cit., 10. Ulteriori e precedenti criteri utilizzati erano quello del c.d. *equally efficient competitor text* secondo il quale una condotta deve qualificarsi come abusiva se un concorrente dell'impresa dominante, altrettanto efficiente di questa, non sia in grado di replicarne autonomamente le offerte commerciali, in quanto privo di alcuni vantaggi competitivi di cui l'impresa dominante gode in via esclusiva. L'altro criterio è quello del c.d. *reasonably efficient competitor test* che valuta la struttura dei costi di un'impresa efficiente che decida di entrare oggi *ex novo* nel mercato. Tale ultimo criterio è relegato dalla Commissione a livello sussidiario.

[57] È stato osservato, in Enc. del diritto, *abuso di posizione dominante-vertici internazionali*, annali V, Milano, 2012, 7, come un'applicazione rigorosa della teoria incentrata sul benessere dei consumatori potrebbe «condannare ogni comportamento che danneggia il consumatore pur non toccando assolutamente il mercato (...) ovvero assolvere una condotta chiaramente anticoncorrenziale (...) che tuttavia non comporta almeno nel breve termine alcun danno diretto per il consumatore».

dipendono dell'evoluzione dell'offerta delle imprese, a sua volta mediata dall'innovazione tecnologica [58].

Si può notare che la tutela della libertà di scelta degli acquirenti costituisce il presupposto che accomuna e che collega le diverse decisioni dei giudici europei in materia. Se si conclude che la concorrenza basata sui meriti è quella situazione in cui il profitto dell'impresa dipende dalle libere scelte dei consumatori, allora si dovrebbe altrettanto concludere che una siffatta situazione viene meno allorché i consumatori:

(a) siano ingannati da false informazioni o da costrizione psicologica (in tal senso le pratiche commerciali scorrette) [59];

(b) siano costretti a compiere scelte per mancanza di alternative o per l'esistenza di vincoli giuridici pregressi e non per libera scelta (clausole leganti e simili);

(c) vengano privati di alternative di mercato potenzialmente interessanti (pratiche escludenti) [60].

Un criterio alternativo a quello del benessere del consumatore, rintracciabile anch'esso in vari interventi giurisprudenziali, è quello che si

---

[58] M. Libertini, *Abuso del diritto e abuso di posizione dominante,* cit., 11-12; si veda altresì, sulla difficoltà di utilizzare la massimizzazione del benessere del consumatore quale parametro dell'efficienza, F. Denozza, *Il progetto teorico dell'analisi economica del diritto antitrust e il suo fallimento,* in C. Rabitti Bedogni, P. Barucci (a cura di), *20 anni di antitrust – L'evoluzione dell'Autorità Garante della Concorrenza e del Mercato*, Torino, Giappichelli, 2010, 137 ss.

[59] Ancora una volta, quindi, si può notare la centralità del principio di trasparenza.

[60] Si veda sempre M. Libertini, *Abuso del diritto e abuso di posizione dominante,* cit., 12. L'A., inoltre, p. 19, soffermandosi su una sintesi dell'illecito in discussione rileva come esso possa attenere allo «svolgimento di un'attività e può realizzarsi solo all'interno della stessa. Le condotte rilevanti possono consistere in atti negoziali come anche in comportamenti di fatto o ancora in pure omissioni o in particolari declinazioni della prassi o delle strategie aziendali (p.e. l'adozione di un piano di investimenti che limita artificiosamente la creazione di capacità produttiva addizionale, quando su di essa vi sarebbe diritto di accesso dei concorrenti operanti nei mercati a valle)».

incentra sulla struttura del mercato. La Corte di Giustizia, in una sua pronuncia del 2009, ha specificato che gli interessi dei consumatori non sono gli unici a essere tutelati dal diritto della concorrenza, bensì la struttura del mercato e la concorrenza in quanto tale sono gli interessi che vengono protetti dalle regole antitrust e, perché si possa manifestare un illecito concorrenziale, non sarebbe necessaria la verificazione di un danno ai consumatori [61].

---

[61] Corte di Giustizia CE, C-501/06 P, C-513/06 P, C-515/06 P e C-519/06P, 06 ottobre 2009, curia.europa.eu. Tale pronuncia riprende quanto già affermato dalla stessa Corte di Giustizia in un caso riguardante *British Airways*, causa C-95/04 P, in cui veniva statuito espressamente che l'istituto dell'abuso di posizione dominante riguardava quei comportamenti che sono atti ad influire sulla struttura di un mercato. In particolare, in quest'ultima pronuncia si legge che «L'art. 82 CE non riguarda soltanto le pratiche di natura tale da causare direttamente un danno ai consumatori, bensì anche quelle che arrecano loro pregiudizio compromettendo un regime di concorrenza effettiva, quale quello di cui all'art. 3, n. 1, lett. g, CE. Ne consegue che, per valutare l'eventuale carattere abusivo di un comportamento di un'impresa in posizione dominante, non è necessario accertare se esso ha causato un danno ai consumatori ai sensi dell'art. 82, secondo comma, lett. b, CE, ma basta verificare se esso ha avuto un effetto restrittivo sulla concorrenza». La stessa pronuncia prosegue statuendo che: «Lo specifico divieto di discriminazione di cui all'art. 82, secondo comma, lett. c, CE fa parte del regime che garantisce, in conformità all'art. 3, n. 1, lett. g, CE, che la concorrenza non sia falsata nel mercato interno. Il comportamento commerciale dell'impresa in posizione dominante non deve falsare la concorrenza sul mercato situato a monte o a valle, cioè la concorrenza tra fornitori o tra clienti della detta impresa. Le controparti commerciali di tale impresa non devono essere favorite o sfavorite sul terreno della concorrenza che praticano reciprocamente. È conseguentemente importante, perché ricorrano le condizioni di applicazione dell'art. 82, secondo comma, lett. c, CE, constatare che il comportamento dell'impresa in posizione dominante su un mercato non soltanto sia discriminatorio, ma anche che esso tenda a falsare tale relazione concorrenziale, cioè ad ostacolare la posizione concorrenziale di una parte delle controparti commerciali di tale impresa rispetto alle altre. Al riguardo nulla osta a che la discriminazione delle controparti commerciali che si trovano in una relazione concorrenziale possa essere considerata abusiva dal momento in cui il comportamento dell'impresa in posizione dominante tende a condurre, alla luce dell'insieme delle circostanze della fattispecie, ad una distorsione della concorrenza fra tali controparti commerciali. In simile situazione,

Tuttavia, dagli stessi principi elaborati dalla giurisprudenza europea se ne può ricavare che i due criteri del benessere dei consumatori e della struttura del mercato non sono l'uno in contrasto con l'altro, ma possono essere in un rapporto alternativo tra loro, ovvero di complementarità [62].

Per completare il quadro, peraltro, va rilevato che, come statuito dalla giurisprudenza europea e nazionale, il giudizio sull'abuso di posizione dominante prescinde dalla liceità della condotta alla luce delle singole normative di riferimento [63].

L'illecito antitrust in questione, perciò, benché sia stato spesso attivato negli ultimi anni nell'ambito dei mercati digitali [64], presenta una struttura complessa e si caratterizza per una applicazione *ex post* rispetto a una condotta anticoncorrenziale realizzata da quelli che sono ormai considerati i detentori del potere privato nel mercato digitale.

---

non si può esigere che sia anche fornita la prova di un deterioramento effettivo, esattamente valutabile, della posizione concorrenziale delle dette controparti commerciali considerate individualmente».

[62] Ciò può essere ricavato dalla Corte di giustizia CE, C-85/76, 13 febbraio 1979, *Hoffmann-La Roche & Co. AG*, eur-lex.eu

[63] In questo senso, Tar Lazio, sez. I, 01 agosto 2017, n. 9140 e 9141 in cui vengono riprese le pronunce della Corte di giustizia CE, C-457/10, 06 dicembre 2012, Astrazeneca, curia.europa.eu; Cons. di Stato, VI, 15 maggio 2015, n. 2479 e 12 febbraio 2014, n. 693, Foro It., 2014: «la giurisprudenza ha pure osservato come il carattere abusivo di un comportamento alla luce dell'art. 102 TFUE non ha relazione con la sua conformità ad altre normative, giacché gli abusi di posizione dominante consistono, per lo più, proprio in comportamenti leciti alla luce di altri settori dell'ordinamento, diversi dal diritto alla concorrenza. (...) Ne consegue che, pur in presenza di comportamenti leciti alla luce di singole normative settoriali, l'interprete potrà ravvisare la sussistenza dell'illecito anticoncorrenziale laddove la combinazione degli stessi sia espressiva di un intento escludente, da accertare indiziariamente come un *quid pluris* che si aggiunge alla sommatoria di comportamenti altrimenti leciti».

[64] I procedimenti dell'AGCM conclusi nel 2021 si connotano per una spiccata attenzione ai mercati digitali e alle cc.dd. *multi-sided platform*; in tal senso, N. M. Naso, *Abusi di posizione dominante*, cit., 296-299, ove risalta la complessità di definizione del mercato rilevante per alcune istruttorie che riguardano gli operatori digitali.

Per completezza, va precisato che il soggetto leso da una condotta anticoncorrenziale è legittimato ad agire in via risarcitoria in forza di una normativa *ad hoc*. Con il D.lgs. del 19 gennaio 2017, n. 3, è stata data attuazione alla direttiva 2014/104 (UE) e sono state introdotte disposizioni relative ad alcuni importanti aspetti delle azioni volte ad ottenere il risarcimento del danno provocato da condotte contrastanti con il diritto della concorrenza [65].

4.1 *Abusi di sfruttamento e abusi escludenti*

Nell'ambito dell'illecito antitrust di cui all'art. 102 TFUE viene sovente operata una dicotomia tra i tipi di abuso. Da un lato, gli abusi di sfruttamento, consistenti in quelle ipotesi di iniquo sfruttamento da parte di un'impresa del proprio potere di mercato volto a ricavare «profitti sovra competitivi». Sono condotte abusive a prescindere dall'impatto che hanno sulla struttura concorrenziale del mercato [66].

Questi abusi possono originare proprio dal potere di mercato che

---

[65] Secondo pronunce anteriori alla vigenza della richiamata normativa, il danno cagionato mediante abuso di posizione dominante non è *in re ipsa*, ma, in quanto conseguenza diversa ed ulteriore rispetto alla distorsione delle regole della concorrenza, deve autonomamente provarsi secondo i principi generali in tema di responsabilità aquiliana. In tal senso, Cass. civ., Sez. I, 10 settembre 2013, n. 20695, CED Cassazione, 2013. Il legislatore, con il citato D.lgs. n. 3/2017, all'art. 14, ha previsto che «il risarcimento del danno causato da una violazione del diritto della concorrenza dovuto al soggetto danneggiato si deve determinare secondo le disposizioni degli articoli 1223, 1226 e 1227 del codice civile. 2. L'esistenza del danno cagionato da una violazione del diritto alla concorrenza consistente in un cartello si presume, salva prova contraria dell'autore della violazione. 3. Il giudice può chiedere assistenza all'autorità garante della concorrenza formulando specifiche richieste sugli orientamenti che riguardano la quantificazione del danno. Salvo che l'assistenza risulti non appropriata in relazione alle esigenze di salvaguardare l'efficacia dell'applicazione a livello pubblicistico del diritto della concorrenza, l'autorità garante presta l'assistenza richiesta nelle forme e con le modalità che il giudice indica sentita l'autorità medesima».

[66] In tal senso, F. RUGGERI, *Poteri privati e mercati digitali,* cit.,175.

alcuni operatori detengono nei cc.dd. mercati "senza prezzo" e dalle modalità con cui vengono acquisiti i dati degli utenti [67].

Dall'altro lato, invece, si collocano gli abusi escludenti, che si traducono in quelle condotte tese a ridurre o eliminare «la capacità competitiva delle imprese concorrenti per poter, di contro, (tendere a) monopolizzare il mercato e godere dei profitti che tale posizione consente di conseguire» [68]. Peraltro, possono verificarsi anche ipotesi di abusi escludenti per mezzo di condotte di sfruttamento [69].

Quelli escludenti sono gli abusi più diffusi nella prassi e nel corso della verifica della condotta non sarebbe determinante l'elemento soggettivo [70].

---

[67] AGCM, *Indagine conoscitiva sui Big data,* cit., 109. Nel documento si legge che tali abusi benché «costituiscano una dimensione residuale dell'enforcement antitrust "tradizionale", il loro rilievo nei mercati digitali appare potenzialmente più esteso».

[68] F. Ruggeri, *Poteri privati e mercati digitali,* cit.,175. Con una recente pronuncia, la cassazione ha ravvisato un caso di abuso escludente realizzato attraverso l'applicazione da parte del soggetto in posizione dominante nel mercato all'ingrosso di condizioni economiche più onerose nei confronti delle imprese concorrenti rispetto a quelle applicate alle proprie divisioni commerciali. È stato accertato che la condotta provocherebbe una contrazione degli utili (*margin squeeze*) nell'impresa danneggiata, sicché il danno da quest'ultima subito ricomprende il mancato guadagno che si determina per effetto dell'assorbimento del maggior costo sostenuto e, in assenza di altri elementi rappresentativi, può essere liquidato in tale misura. Il caso riguardava un abuso escludente da parte di un gestore del servizio di telecomunicazione che si trovava in posizione dominante nei mercati all'ingrosso della terminazione delle chiamate su rete mobile. Cass. Civ., Sez. I, 26 aprile 2022, n. 13073, CED Cassazione, 2022. In riferimento al suddetto *margin squeeze*, era già stato specificato dalla giurisprudenza di merito che sussiste un'abusiva compressione dei margini, praticata da un'impresa dominante, allorché la concorrenza da posizioni asimmetriche consenta a chi può vantare un costo minore di acquisire un vantaggio competitivo riducendo il profitto di chi sopporti un costo maggiore. In questo senso, Corte d'Appello Milano, 02 gennaio 2017, *Foro Italiano*, vol. 1, n. 9, 2017, 1, 2839.

[69] V. Morozovaite, *The future of anticompetitive self-preferencing: analysis of hypernudging by voice assistant under article 102 TFEU*, in *European Competition Journal*, vol 19, n. 3, 2023, 410, spec. 433.

[70] F. Ruggeri, *Poteri privati e mercati digitali,* cit.,176. Sull'elemento soggettivo in

Su quest'ultimo tema, però, occorre tener presente un'ordinanza di rimessione alla Corte di Giustizia con cui il Consiglio di stato ha posto cinque quesiti interpretativi inerenti alla corretta identificazione delle condotte che si sostanziano in abusi di posizione dominante. Tra i quesiti il giudice *a quo* chiede se l'abuso di posizione dominante debba valutarsi soltanto per i suoi effetti (anche soltanto potenziali) sul mercato, senza alcun riguardo al movente soggettivo dell'agente; oppure, se la dimostrazione dell'intento restrittivo costituisca un parametro utilizzabile - anche in via esclusiva - per valutare l'abusività del comportamento dell'impresa dominante; oppure ancora se tale dimostrazione dell'elemento soggettivo valga soltanto in un'ottica di inversione dell'onere della prova in capo all'impresa dominante, la quale sarebbe onerata di fornire la prova che l'effetto escludente non sussisteva [71].

L'accertamento di un abuso non è una operazione banale. A fronte di una prima individuazione di un certo standard di condotta ne segue un confronto con quella osservata in concreto dall'impresa dominante [72]. L'esito di tale complessa operazione potrebbe fornire una risposta sulla sussistenza dell'abuso in questione [73]. Tuttavia, per quei mercati caratterizzati da innovazione tecnologica questo accertamento su

---

materia concorrenziale, il Consiglio di Stato ha stabilito, aderendo ad un orientamento già consolidato in materia che, ai fini della sanzionabilità di un illecito antitrust, sotto il profilo dell'elemento soggettivo non è necessaria la consapevolezza di trasgredire un puntuale divieto normativo, essendo sufficiente la consapevolezza dell'esito anticoncorrenziale delle condotte. In tal senso, Consiglio di Stato, Sez. VI, 16 marzo 2006, n. 1397, *Rassegna di diritto di Farmaceutico e della salute*, n. 1, 2007, 53.

[71] Consiglio di Stato, Sez. VI, 20 luglio 2020, n. 4646, in *Diritto dei Servizi Pubblici.it*, 2020.

[72] La giurisprudenza ha statuito che in tema di abuso di posizione dominante, la valutazione delle attività d'impresa deve avvenire in rapporto all'utilità economica sostanziale che esse perseguono. Quindi, condotte consentite da un punto di vista settoriale possono per altro verso risultare illecite. Nel caso di specie è stato riconosciuto il carattere di strumentalità e di emulatività dei comportamenti dell'impresa in posizione dominante, volti ad ostacolare l'ingresso nel mercato da parte del concorrente. Cons. Stato, Sez. VI, 08 aprile 2014, n. 1673, in *Foro Italiano*, 2014.

[73] F. RUGGERI, *Poteri privati e mercati digitali,* cit.*,* 176.

come sarebbe stato il mercato se la presunta condotta abusiva non avesse avuto luogo è irta di difficoltà vista la scarsità di dati storici nel settore e la carenza di pratiche commerciali consolidate [74].

Su questo tema è necessario dare atto che la Commissione europea ha recentemente adottato una nuova comunicazione che modifica i precedenti orientamenti sugli abusi preclusivi. Il documento chiarisce che nei mercati caratterizzati da effetti di rete o da altre barriere all'ingresso la Commissione può indagare sulle pratiche di un'impresa dominante in grado di pregiudicare i concorrenti che non sono (ancora) efficienti come l'impresa dominante. Essa può indagare sui casi in cui un'impresa dominante impone condizioni di accesso inique in relazione a un determinato fattore di produzione (il cosiddetto "rifiuto costruttivo di fornitura"), anche laddove non vi sono prove che il fattore di produzione in questione sia indispensabile [75].

Oltre ai casi pratici che si riporteranno nei paragrafi successivi, occorre segnalare come negli ultimi anni la Commissione europea sia intervenuta più volte con procedimenti che hanno condotto a sanzioni per pratiche escludenti. Nei soli confronti di Google sono stati conclusi tre procedimenti per abusi di posizione dominante aventi ad oggetto pratiche escludenti nei mercati delle ricerche generiche sul web e nel settore dell'intermediazione pubblicitaria. Tutte pratiche che hanno consentito all'impresa di rafforzare la propria posizione nei mercati interessati e di raccogliere una mole sempre più rilevante di dati degli utenti, utili per le sue attività di ricerca e di pubblicità online [76].

---

[74] M. Rato, N. Petit, *Abuse of Dominance in Technologyenabled Markets: Established Standards Reconsidered?,* in *European Competition Journal*, vol. 9, n. 1, 2013, 1, spec. 21.

[75] Comunicazione Commissione europea, 27 marzo 2023, C (2023) 1923 final, "*Amendments to the Communication from the Commission Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings*".

[76] AGCM, *indagine conoscitiva sui Big data,* cit., 107. Uno degli ultimi procedimenti è stato: Commissione Europea (2019), "*AT.40411 Google Search (AdSense)*". In questo procedimento è stato accertato che molti contratti tra Google e i siti *publisher* più rilevanti prevedevano clausole di esclusiva; i *publisher* avevano il divieto di mostrare

4.2 *La pratica dei prezzi dinamici o personalizzati*

Tra le pratiche diffuse nelle prassi di alcuni operatori digitali occorre menzionare anche quella dei prezzi differenziati (*dynamic pricing*) o dei prezzi personalizzati. Questa pratica si traduce nella determinazione di un prezzo del prodotto o servizio a seconda delle caratteristiche del singolo utente, ovvero della sua propensione al consumo e, quindi, della attitudine ad acquistare un prodotto a un determinato prezzo [77]. È un'altra pratica che, con ogni evidenza, viene attuata grazie all'acquisizione sistematica di dati personali dell'interessato.

Per adattare il prezzo in base alla disponibilità del singolo consumatore vengono elaborate, tramite algoritmi, informazioni provenienti dal mercato, dal singolo prodotto e dal singolo potenziale acquirente [78]. Viene giustamente sottolineato in letteratura che la disponibilità "a pagare" indica la misura di utilità di un bene, per il singolo consumatore, espressa in termini monetari e viene definita, per distinguerla dal prezzo effettivamente pagato, "prezzo di riserva" [79].

Si tratta di una pratica suscettibile di produrre trattamenti discriminatori. In letteratura viene differenziata la discriminazione di prezzo

---

sulle pagine dei risultati di ricerca annunci pubblicitari collegati alla ricerca dei concorrenti; successivamente, Google ha gradualmente iniziato a sostituire le clausole di esclusiva con le cosiddette clausole di "posizionamento premium", che imponevano ai *publisher* di riservare lo spazio più redditizio sulle pagine dei risultati di ricerca agli annunci di Google e di prevedere un numero minimo di annunci di Google; infine, Google ha previsto clausole che imponevano ai *publisher* a ottenere l'autorizzazione scritta da parte di Google prima di modificare le modalità di visualizzazione dei messaggi pubblicitari dei concorrenti. Gli altri procedimenti sono stati: Commissione Europea (2018), "*AT.40099 Google Android*" e Commissione Europea (2017), "*AT.39740 Google Search (Shopping)*".

[77] A. MILLER, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, in *Journal of technology law & policy*, vol. 19, n. 1, 2014, 41 ss.

[78] R. WEISS, A. K. MEHROTRA, *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, in *Virginia Journal of Law and Technology.*, vol. 6, 11, 2001, 1.

[79] L. A. CALOIARO, *Il prezzo personalizzato, il consumatore e le insidie del mercato digitale*, Torino, Giappichelli, 2024, 6-7.

sulla base di tre gradi. Nel primo grado, verrebbe applicato per ogni cliente il prezzo massimo che egli è disposto a pagare per ogni unità di prodotto; con quella di secondo grado, verrebbero applicati distinti prezzi unitari in virtù della quantità consumata di un prodotto; con quella di terzo grado, invece, il venditore, possedendo informazioni sui comportamenti dei consumatori, riuscirebbe a stabilire prezzi differenti in base alle loro caratteristiche personali. Con quest'ultima modalità viene operata una segmentazione in forza dell'appartenenza a un determinato gruppo. Tra gli elementi di riferimento per tale segmentazione può essere annoverata la localizzazione geografica, l'età dell'acquirente e la sua occupazione [80].

Qualora la discriminazione si riferisca alle caratteristiche soggettive del consumatore, si parla di "discriminazione intersoggettiva del prezzo"; nel caso, invece, di discriminazione attuata sulla base del comportamento osservato dal consumatore, si parla di "discriminazione comportamentale" [81].

In un'ottica strutturale, alcuni autori ricostruiscono il fenomeno riconducendolo sotto il suo profilo concorrenziale [82], mentre altri sotto l'aspetto etico [83].

---

[80] La classificazione in questione andrebbe attribuita all'economista inglese Arthur Cecil Pigou.

[81] L. A. Caloiaro, *Il prezzo personalizzato,* cit., 18. La discriminazione intersoggettiva viene a sua volta distinta in perfetta, quando si riferisce al singolo consumatore, o imperfetta, quando si riferisce a una classe di soggetti. Si parla di "prezzo personalizzato" proprio in riferimento alla prima, ossia a una discriminazione intersoggettiva perfetta. L'A., 69, sottolinea come la pratica di una discriminazione intersoggettiva "imperfetta" appaia suscettibile di essere vietata ai sensi dell'art. 43, co. 2, lett. b, d.lgs. 25 luglio 1998, n. 286, mentre appare più complessa la fattispecie della discriminazione "perfetta".

[82] R. Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, in *University of Pennsylvania Law Review*, vol. 163, 2015, 1311, 1330; N. Newman, *Search, Antitrust, and the Economics of the Control of User Data*, in *Yale Journal on Regulation*, vol. 31, 2014, 401-405.

[83] A. J. Schmitz, *Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots"*, in *Michigan State Law Review*, n. 5, 2014, 1411, spec. 1414-1415.

Da un punto di vista concorrenziale si è affermato che, visto che uno degli scopi della legislazione antitrust è quello di salvaguardare il benessere dei consumatori, a questi deve essere garantito un mercato con la più ampia scelta possibile al livello di prezzo più basso [84]. Nella dottrina statunitense, in particolare, si è sostenuto che le attuali pratiche di discriminazione dei prezzi potrebbero generare problematiche anticoncorrenziali in quanto potenzialmente produttive di inefficienza, al punto che dovrebbero essere vietate anche nei casi in cui non limitino la concorrenza [85].

La dottrina domestica, invece, sempre in tema di discriminazioni di prezzo, ha rilevato la possibilità di accertare, sulla base di una valutazione caso per caso, una ipotesi di abuso di sfruttamento allorché si rechi un pregiudizio al commercio tra Stati membri o all'interno del mercato rilevante di riferimento. L'abuso in questione potrebbe tradursi nell'appropriazione del *surplus* del consumatore, con incremento del sovrapprezzo, realizzata dall'impresa "discriminante" e in posizione dominante [86].

Peraltro, in ambito nazionale, occorre tenere in considerazione che il codice del consumo, all'art. 49, co. 1, lett. e-*bis*), prevede che il professionista sia tenuto a comunicare al consumatore l'informazione sul prezzo personalizzato prima che quest'ultimo sia vincolato da un contratto a distanza o negoziato fuori dei locali commerciali.

Il mancato assolvimento dell'onere di chiarezza e comprensibilità non comporterebbe l'attivazione di particolari rimedi, ma renderebbe la clausola dubbia, quindi suscettibile di plurime interpreta-

---

[84] S. C. SALOP, *Question: What is the Real and Proper Antitrust Welfare Standard? Answer: The True Consumer Welfare Standard*, in *Loyola Consumer Law Review*, vol 22, 2010, 336.

[85] D. M. KOCHELEK, *Data Mining and Antitrust*, *Harvard Journal Law & Tech.*, vol, 22, 2009, 515-535.

[86] L. A. CALOIARO, *Il prezzo personalizzato*, cit., 130-131; Sul tema si veda altresì F. DI PORTO, *La rivoluzione big data*, cit., 5 ss.; per una tesi tendente ad escludere l'illecito antitrust per ipotesi di questo genere si veda M. MAGGIOLINO, *I big data e il diritto antitrust*, Milano, Egea, 2018, 318.

zioni [87]. V'è chi ritiene che, sotto un profilo di diritto contrattuale, l'omessa informazione sulla personalizzazione del prezzo implichi un inadempimento di un obbligo d'informazione suscettibile di provocare una fattispecie di responsabilità precontrattuale [88].

4.3 *I potenziali e nuovi orizzonti delle pratiche di self-preferencing per il tramite degli assistenti vocali*

È stato recentemente osservato in dottrina che si potrebbero aprire le porte di fattispecie anticoncorrenziali provenienti dall'utilizzo dei nuovi (e sempre più diffusi) strumenti tecnologici quali gli assistenti vocali.

In particolare, tramite tecniche di *hyper-nudging* [89], si potrebbero realizzare pratiche di *self-preferencing* capaci di incidere in termini di concorrenza. È stato segnalato, infatti, come i sistemi tecnologici odierni - grazie alla disponibilità di una grande quantità di dati - sarebbero in grado di consigliare un prodotto o un servizio in base a quelle che sono le esigenze riconosciute in relazione al singolo consumatore, adattando le proprie raccomandazioni in base all'umore di quest'ultimo e riconoscendo il momento adeguato per la proposta a un determinato acquisto.

In questo modo, il sistema riuscirebbe a orientare le scelte del consumatore in una logica di profitto che potrebbe non riflettere gli interessi e le preferenze del singolo rendendo più difficile (se

---

[87] L. A. Caloiaro, *il prezzo personalizzato,* cit., 98.

[88] *Ivi*, 110.

[89] Con *nudge* si fa riferimento a tecniche proprie della scienza comportamentale che, senza creare alcun obbligo o divieto, riescono a influenzare il comportamento e le scelte delle persone. Con *hyper-nudging* ci si riferisce, invece, a *nudge* capaci di adattarsi e cambiare nel tempo in base ai *feedback* che giungono dall'interessato. Su questo tema si veda l'interessante scritto di S. Mills, *Finding the 'nudge' in hypernudge*, in *Technology in Society*, vol. 71, n. 1, 2022, 102, spec. 122.

non impossibile) identificare pratiche scorrette rispetto a quelle tradizionali [90].

È stata altresì osservata la differenza esistente fra le pratiche attuabili mediante assistenti vocali e quelle per il tramite delle piattaforme di base. In quest'ultimo caso, il consumatore si trova esposto a più offerte in contemporanea, una in primo piano e le altre in base ai criteri di ricerca sul web o sull'interfaccia dell'applicazione, creando quindi una certa utilità ai fini decisionali; per gli assistenti vocali, invece, lo scenario muta perché ai consumatori viene suggerito un solo prodotto per volta, senza alcun margine visivo e con scarse informazioni [91].

Il rischio, dunque, sarebbe quello di influenzare il comportamento del singolo in senso negativo in termini di competitività, verificandosi un'ipotesi di sfruttamento che porta a effetti escludenti [92]. Sostanzialmente, secondo la tesi in questione, in mercati digitali sempre più incentrati sul consumatore occorrerebbe considerare anche quelle pratiche che si avvalgono dell'*hyper-nudging*, le quali possono mirare all'esperienza dell'utente/consumatore come mezzo per escludere i concorrenti [93]. Si tratta di scenari nuovi e suggestivi che, in ogni caso, richiedono un adattamento nei processi di accertamento della condotta ai fini antitrust e finanche ai fini dell'applicabilità del DMA.

5. *Il trattamento dei dati personali e la sua rilevanza antitrust*

La portata del tema inerente al trattamento dei dati personali e la sua connessione anche con le dinamiche concorrenziali è ormai un dato pressocché pacifico. Lo dimostrano i casi in cui le competenti

---

[90] V. MOROZOVAITE, *The future of anticompetitive self-preferencing,* cit., 433. L'A. osserva che attraverso queste tecniche ci sarebbe il rischio che le migliori offerte per il consumatore verrebbero taciute con conseguente perdita di benessere per i consumatori e di profitti per i concorrenti.

[91] *Ivi*, 437.

[92] *Ibidem*.

[93] *Ivi*., 444.

autorità di vari Stati si sono attivate, soprattutto nel settore della pubblicità. Uno dei casi più recenti è stato quello della *Competition and Markets Authority* inglese che ha aperto una indagine per abuso di posizione dominante in merito ad alcune pratiche di Google [94].

Invero, si è visto che tra gli elementi chiave del mercato digitale la pubblicità costituisce una delle fonti dalle quali le aziende traggono i maggiori profitti. Si è già visto inoltre che questi ultimi vengono ricavati grazie a una maggiore qualità del servizio reso mediante la profilazione degli utenti ottenuta per mezzo di una massiva acquisizione di dati personali (e non personali) che consentono di individuare gli interessi concreti dei potenziali acquirenti; quindi, le loro preferenze e la loro personalità. Ciò accade spesso, come si è già visto, quando nelle *privacy policy* viene indicata, tra le finalità del trattamento, quella del *marketing* [95].

È stato rilevato come gli inserzionisti, nel settore in esame, grazie

---

[94] Il settore delle tecnologie pubblicitarie digitali viene comunemente denominato *ad tech stack*. La procedura a cui si fa riferimento è quella avviata dalla *Competition and Markets Authority* il 6 settembre 2024, consultabile al sito www.gov.uk

[95] La domanda e l'offerta in questi mercati si incontrano tramite le cc.dd. *ad exchange* automatizzate che costituiscono un luogo virtuale ove avviene un'asta in tempo reale degli spazi pubblicitari. Si realizza un processo attraverso il quale la piattaforma di *programmatic* (*advertising*) segnala ai potenziali inserzionisti le caratteristiche dell'utente al quale potrebbe essere indirizzato un determinato messaggio, tra cui la stima dell'età, eventuali figli ed interessi particolari; l'inserzionista interessato, partecipa quindi all'asta, aderendo alla c.d. *Real Time Bidding* (RTB), ovvero all'offerta in tempo reale. Tutte le singole esigenze di *marketing* dell'inserzionista possono essere potenzialmente soddisfatte in forza di determinati parametri, tra i quali l'area geografica di riferimento dell'utente, l'età anagrafica, gli interessi particolari, l'attività lavorativa etc. Gli editori, che costituiscono i venditori degli spazi pubblicitari del mercato digitale in cui potranno essere inserite le comunicazioni commerciali dei compratori, possono essere rappresentati da agenzie pubblicitarie o dalle stesse aziende titolari del *brand*. Si aderisce, perciò, ad un vero e proprio mercato virtuale in cui si incontrano domanda ed offerta, realizzando ogni singola operazione in un arco temporale brevissimo grazie ai *bots*, ovvero ai più avanzati strumenti tecnologici esistenti che si avvalgono di sistemi di intelligenza artificiale.

ai *big data*, si avvalgono di un imponente laboratorio volto alla conduzione di ricerche sui consumatori e alla creazione di contatti, dando vita alla c.d. *lead generation*[96].

La pubblicità online per indirizzare messaggi promozionali mirati agli utenti deve essere suddivisa in due mercati rilevanti distinti: l'uno rappresentato da quello della pubblicità *search online* e, l'altro, da quello della pubblicità non *search online*[97].

Il mercato in questione, nel suo insieme, e negli ultimi tempi, ha assistito ad una rilevante concentrazione di aziende e ha prospettato finanche ipotesi di restrizioni anticoncorrenziali. Perciò, il tema delle nuove tecnologie, che si esprime attraverso le piattaforme di raccolta dei dati, quello della pubblicità e della concorrenza, si intessono dando vita a questioni che meritano particolare attenzione.

In un parere del 2016 elaborato dalla *European Data Protection Supervisor* (EDPS) - stesso anno dell'analisi della fusione LinkedIn/Microsoft -, è stata sottolineata la capacità delle piattaforme di acquisire una massiva quantità di dati che gli consente di trarre importanti introiti economici grazie alla pubblicità e di precludere l'ingresso di nuove imprese nel mercato digitale. Questo, secondo l'EDPS, comporterebbe un pregiudizio ai consumatori, i quali vedrebbero ridursi la possibilità di scelta e l'innalzamento del prezzo dei servizi, un prezzo che i con-

---

[96] C. O'NEIL, "*Weapons of math destruction: How Big Data Increases Inequality and Threatens Democracy*", Crown, 2016, 103. Secondo l'a., attraverso l'avvento di Internet «le persone di tutto il mondo hanno prodotto milioni di miliardi di parole sulla nostra vita e il nostro lavoro, le nostre abitudini di acquisto, le nostre amicizie. Così facendo, abbiamo costruito senza saperlo il più gigantesco corpus di apprendimento immaginabile per le macchine che elaborano il linguaggio naturale. (...) Un programma pubblicitario potrebbe partire dai soliti dati demografici e geografici. Ma nel corso delle settimane e dei mesi, comincia ad acquisire i modelli di comportamento delle persone su cui focalizza l'attenzione e a fare previsioni circa le loro prossime mosse. Impara a conoscerle. E se il programma è predatorio, ne misura debolezze e vulnerabilità, cercando di individuare il percorso più efficiente per sfruttarle».

[97] Si veda la decisione della Commissione europea del 20 marzo 2019, AT. 404411 – *Google Search* (*AdSense*). Così come Commissione europea M.5727 – *Microsoft/Yahoo!Search Business.*

sumatori pagano proprio con la concessione dei propri dati personali [98]. Di qui, l'elemento chiave, già trattato nei precedenti capitoli, ossia, la concessione dei dati personali come prezzo del servizio erogato.

Secondo l'EDPS, la rilevanza dei dati personali è tale da essere inseriti tra le "materie prime" delle aziende digitali. Viene specificato nel parere che la *privacy* e gli standard di protezione dei dati costituiscono parametri per valutare la qualità di un prodotto o di un servizio. Qualora il grado di protezione fosse basso, ciò produrrebbe un danno al consumatore che si riverserebbe finanche nel settore concorrenziale.

Le imprese che agiscono in una posizione dominante sarebbero in grado di escludere nuovi concorrenti che offrono servizi maggiormente rispettosi della privacy, come coloro che non tracciano le attività online degli individui, ad eccezione, va da sé, dei casi in cui ciò fosse necessario per fornire il relativo servizio; quindi, quei casi in cui tale tracciamento sia funzionale al servizio stesso.

Per determinare se sussistano ipotesi di abuso di posizione dominante ai sensi dell'art. 102 TFUE, *rectius*, fattispecie di esclusione di nuove imprese dal mercato, un parametro fondamentale, secondo l'EDPS, sarebbe costituito proprio dalle norme sulla protezione dei dati e dei consumatori. Ebbene, l'analisi descritta ha aperto le porte a una riflessione sulla configurabilità di ipotesi anticoncorrenziali, in particolare di abuso di posizione dominante derivanti dall'acquisizione e dal trattamento di informazioni da parte di quelle imprese che nel mercato digitale godono di una dominanza, con lo scopo di profilare l'utenza, di indirizzare loro la più congeniale pubblicità commerciale, con il relativo incremento dei profitti, a danno del benessere dei consumatori che si vedono ridurre le possibilità di scelta tra differenti

---

[98] S. Martinelli, *Il parere dell'EDPS sulla tutela dei diritti fondamentali nell'era dei Big Data*, in *Quotidiano Giuridico,* n. 11, 2018; EDPS, Opinion n. 8/2016, *On coherent enforcement of fundamental rights in the age of big data*, consultabile al sito edps.europa.eu. Il parere mostra come le pratiche di acquisizione e utilizzo dei dati personali, nell'ottica di tutela della *privacy*, possano produrre un danno ai consumatori e quindi, di riflesso, comportare ipotesi di condotte anticoncorrenziali.

operatori concorrenti a causa della preclusione di ingresso di nuove imprese in quel determinato mercato.

Invero, un mercato viene considerato competitivo allorché i consumatori vengano posti nella posizione di poter scegliere fra una gamma di prodotti con caratteristiche simili e i fornitori non incontrano particolari ostacoli all'accesso [99]. Tuttavia, benché possibile, rimane difficoltoso, nei mercati digitali, accertare un'ipotesi di abuso di posizione dominante. La difficoltà e complessità della questione risiede nel fatto che gli elementi che comportano un innalzamento di barriere all'ingresso (e quindi un effetto escludente) per l'accesso prioritario all'infrastruttura di riferimento (dati personali e sistemi tecnologici) può significare «una propensione di tale peculiare mercato» di riferimento e non l'esito di premeditate condotte abusive di chi ha una posizione dominante [100].

La portata della regolazione dei dati personali in termini concorrenziali deve essere oggetto di particolare attenzione soprattutto là dove abbia un effetto differenziale, ossia da una parte avvantaggiando le imprese dominanti, che dispongono tipicamente dei dati ottenuti dalla relazione diretta con i propri utenti, e dell'altra, andando a svantaggio dei potenziali nuovi entranti, i quali potrebbero avere l'esigenza di acquisire con altre modalità i dati rilevanti per entrare e crescere nel mercato [101]. L'incidenza della normativa privacy sugli aspetti concorrenziali dovrebbe essere una valutazione rimessa al caso concreto poiché i dati personali possono anche generare effetti pro-competitivi [102].

---

[99] G. GUZZARDI, *L'abuso di posizione dominante nel mercato dei servizi digitali*, in *Nuova giurisprudenza civile commentata*, n. 2, 2023, 309, spec. 310.

[100] *Ivi*, 317. Perciò l'A. sottolinea come il peculiare dinamismo del mercato digitale acuisce le difficoltà di demarcazione di quella sottile linea di confine tra il legittimo godimento di una posizione dominante acquisita con merito negli anni e l'abuso della stessa, vietato, innanzitutto, dall'art. 102 TFUE.

[101] AGCM, *Indagine conoscitiva big data,* cit., 75.

[102] Z. M. MAZUR, *Il dato personale nella disciplina del mercato e della concorrenza l'esperienza tedesca*, in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali,* cit*.,* 229, spec. 245.

L'indagine conoscitiva sui *big data* dell'AGCM ha posto in risalto l'impatto che l'utilizzo dei dati può avere sull'offerta di beni e servizi facendo venire in rilievo differenti scenari riguardanti il rapporto tra *big data* e il benessere dei consumatori [103]. Nell'indagine vengono riportati alcuni casi pratici.

Viene segnalata l'ipotesi in cui l'utilizzo dei dati personali può comportare una riduzione del benessere dei singoli consumatori. Viene riportato il caso del tracciamento di una attività di ricerca online in cui l'utente non perfeziona l'acquisto di un determinato prodotto. Questa attività tracciata può essere sfruttata per proporre al consumatore, in un secondo momento, lo stesso prodotto o servizio a un prezzo incrementato. Perciò, a fronte di un incremento del *surplus* delle imprese, si realizza un peggioramento delle condizioni economiche dei consumatori [104].

Un'altra ipotesi può invece riguardare l'uso dei dati personali che aumenta il benessere dei consumatori individualmente intesi. Ad esempio, viene riportato il caso della raccolta e dell'elaborazione dei dati sulla geolocalizzazione degli utenti che ha permesso lo sviluppo di servizi che forniscono in tempo reale informazioni sul traffico. Questo servizio non sarebbe possibile senza un accesso ai dati relativi ai singoli utenti. È la condivisione dei dati personali a costituire in questo caso il presupposto per lo sviluppo del servizio [105].

Infine, nel documento dell'AGCM viene posta in risalto l'ipotesi in cui si viene a creare un incremento del benessere del singolo consumatore a fronte, però, di una riduzione del benessere sociale a causa di esternalità negative. Viene riportato l'esempio della personalizzazione dei contenuti giornalistici proposti agli utenti dalle piattaforme digitali che può essere apprezzata dal singolo utente, il quale accede a contenuti di interesse e in linea con le proprie idee, ma può non essere gradita da altre compagini sociali «nella misura in cui riduce il grado di

---

[103] *Ivi*, 87.
[104] *Ibidem*.
[105] *Ibidem*.

pluralismo nel consumo dei contenuti giornalistici con un impatto sulla sfera politica e sociale»[106].

Si può affermare, quindi, che il diritto della concorrenza e la normativa a tutela dei dati personali, in molti casi, sono contesti giuridici complementari, come suffragato dalla recente attività delle Autorità competenti di vari Stati membri. Infatti, si può registrare un dato di fatto: le Autorità a tutela della concorrenza che tendono - in modo sempre più insistente - a ritenere le condizioni di trattamento dei dati personali come uno degli elementi per accertare un abuso di posizione dominante, e dall'altro, invece, le Autorità a tutela dei dati personali che nella definizione di "libero consenso" si rifanno allo sfruttamento del potere di mercato indirizzando lo sguardo sull'effetto *lock-in*[107].

6. *L'intervento chiarificatore della Corte di Giustizia europea sul collegamento tra normativa antitrust e normativa in materia di dati personali: la sentenza CGUE C-252/21*

Come si è già accennato nel primo capitolo, il 4 luglio 2023 la Corte di Giustizia europea ha emesso una pronuncia fondamentale con la quale è stata fornita una risposta chiara alla possibilità per le Autorità antitrust di pronunciarsi su dinamiche concorrenziali anche laddove si sia verificata una violazione della normativa in materia di dati personali[108].

---

[106] *Ibidem*.

[107] A. DAVOLA, G. MALGIERI, *Data-Powerful. Un'indagine sulla nozione di potere e il suo rapporto con la vulnerabilità nel mercato digitale*, in *Concorrenza e mercato*, n. 1, 2022, 67, spec. 91. Gli AA. rilevano successivamente le differenze di approccio delle due normative. Quella antitrust che analizza il potere attraverso un approccio reattivo, a posteriori e strutturale, considerando quindi in modo marginale le vulnerabilità dei singoli coinvolti. La normativa in materia di *privacy*, invece si focalizza sulla posizione dei singoli interessati, con necessità di controllo *ex ante*, ma non è sovente capace di inserire le singole violazioni nell'ambito di un contesto sistemico e strutturale.

[108] Per un primo commento cfr. G. D'IPPOLITO, *Data economy: la Corte di giustizia*

La Corte ha, invero, specificato che «nessuna disposizione (...) vieta alle autorità nazionali garanti della concorrenza di constatare, nell'ambito dell'esercizio delle loro funzioni, la non conformità» al GDPR di un trattamento di dati effettuato da un'impresa in posizione dominante e tale da costituire un abuso di tale posizione [109].

L'autorità garante della concorrenza è tenuta a valutare se il comportamento di una impresa in posizione dominante (ricorrendo a mezzi diversi da quelli su cui si impernia la concorrenza normale tra prodotti o servizi) possa ostacolare, la conservazione del grado di concorrenza esistente sul mercato o lo sviluppo di detta concorrenza [110]. La conformità o non conformità di detto comportamento alle disposizioni del GDPR può costituire un importante indizio fra quelle che sono le circostanze rilevanti e per valutare le conseguenze di una determinata pratica sul mercato o per i consumatori [111]. Tutto ciò perché - sottolinea la Corte di Giustizia - «l'accesso ai dati personali e la possibilità di trattamento di tali dati sono diventati un parametro significativo della concorrenza fra imprese dell'economia digitale» [112].

Un'altra questione rilevante per questi fini, e decisa dalla Corte con la sentenza in esame, riguarda il consenso prestato dall'utente di un'impresa (*social network*, nel caso di specie) in posizione dominante. In particolare, se il consenso possa ritenersi valido in termini di libertà ai sensi dell'art. 4, n. 11, GDPR.

Ebbene, il ragionamento della Corte muove dall'assunto che la posizione dominante dell'impresa, idonea a creare uno squilibrio eviden-

---

precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata, in *Media Laws*, n. 2, 2023, 323.

[109] CGUE, C-252/21, *Meta*, cit., § 43.

[110] CGUE, C-152/19, 25 marzo 2021, *Deutsche Telekom*, § 41 e 42, curia.europa.eu.

[111] CGUE, C-252/21, cit., § 47.

[112] Ivi, § 51, là dove aggiunge che «(...) escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione».

te tra l'interessato e il titolare del trattamento, favorirebbe l'imposizione di condizioni che non sono strettamente necessarie all'esecuzione del contratto. Tutto questo fa sì che deve essere garantita agli utenti la possibilità di rifiutarsi individualmente di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza che tale rifiuto comporti la rinuncia alla integrale fruizione del servizio offerto dall'impresa. Agli utenti, quindi, deve essere proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente che non preveda simili operazioni di trattamento dei dati personali [113]. Tale passaggio costituisce il fulcro della questione sul *pay or consent* oggetto di una controversia pendente (v. infra, cap. V, § 6).

La CGUE ha perciò dichiarato, nella sua interpretazione dell'art. 6, par. 1, co. 1, lett. a), e dell'art. 9, par. 2, lett. a), GDPR, che «la circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'art. 4, punto 11, di detto regolamento, al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare».

Tra l'altro, in considerazione della portata del trattamento di cui sopra, e del suo notevole impatto sugli utenti, oltre al fatto che gli utenti non possano ragionevolmente attendersi che dati diversi da quelli relativi al loro comportamento all'interno della piattaforma siano trattati dall'operatore di quest'ultima, è opportuno che venga prestato un consenso separato «per il trattamento di questi ultimi dati, da un lato, e dei dati off Facebook, dall'altro». Il giudice è chiamato ad accertare l'esistenza di una simile possibilità in difetto della quale il consenso degli utenti al trattamento dei dati raccolti fuori dalla piattaforma deve

[113] *Ivi*, § 150.

presumersi non sia stato prestato liberamente e sarebbe, quindi, non lecito [114].

7. *Il recente caso Apple sull'adozione di politiche di privacy differenziate*

Il caso di Meta Platform oggetto della sentenza CGUE del 4 luglio 2023 costituisce un precedente giurisprudenziale importante nel campo della interazione tra la disciplina dei dati personali e quella della concorrenza. Tuttavia, vi sono altri recenti casi (anche nazionali), come quelli che seguono, meritevoli di attenzione.

Il 2 maggio 2023 l'Autorità garante della concorrenza e del mercato italiana ha adottato un provvedimento con cui è stata avviata una istruttoria ai sensi dell'art. 14 della legge n. 287 del 1990 nei confronti della società Apple Inc. per accertare l'esistenza di violazioni della concorrenza ex art. 102 TFUE [115].

Il fulcro dell'istruttoria avviata dall'Autorità è rappresentato da presunte politiche discriminatorie (o *self preferencing*) inerenti al trattamento dei dati personali tra Apple e suoi concorrenti.

I fatti risalgono al 2021 quando Apple ha imposto ai suoi concorrenti sviluppatori di applicazioni per *smartphone* (che si avvalgono del suo negozio "App Store") una differente politica sul trattamento dei

---

[114] *Ivi*, § 151. Nel successivo § 154 la Corte stabilisce che «l'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a), del RGPD devono essere interpretati nel senso che la circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, di detto regolamento, al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare».

[115] Provvedimento del 02 maggio 2023 AGCM n. 30620, procedimento A561 - *App tracking transparency* di Apple.

dati personali con regole più restrittive rispetto a quelle previste per sé stessa. La nuova politica per i concorrenti è stata denominata *App Tracking Transparency policy,* o ATT *policy.*

Le differenze ricadono sulle caratteristiche della "finestra a scomparsa" che viene mostrata agli utenti per l'acquisizione del consenso al tracciamento dei dati di navigazione che, per i concorrenti pone in risalto l'ipotesi della negazione del consenso e prevede l'espressione inerente al consenso a «tenere traccia delle attività svolte nelle app e sui siti di altre aziende» senza alcun chiarimento in merito al significato di "tenere traccia"; inoltre, nulla dice sui vantaggi per gli utenti in relazione alla pubblicità personalizzata. La politica, invece, per le app di Apple è differente poiché si pone in risalto la prestazione del consenso e l'oggetto di quest'ultimo diventerebbero i "servizi personalizzati" in luogo di "tenere traccia" dell'attività degli utenti.

Peraltro, per le app concorrenti sarebbe previsto il doppio consenso esplicito che prevede il consenso al tracciamento per ogni accesso alle diverse app anche se sono tra loro collegate. Quindi, lo sviluppatore concorrente non potrà condividere i dati per consentire la personalizzazione e la misurazione dell'efficacia degli annunci su un'altra app neppure se vi è stato un consenso iniziale da parte dell'utente. Questo doppio consenso esplicito non è invece previsto per le app di Apple.

Ulteriori differenze riguardano la politica privacy sull'attività di misurazione degli effetti delle campagne pubblicitarie. Questo accadrebbe perché, per gli sviluppatori concorrenti, l'accesso ai "dati di conversione" - ossia, le azioni eseguite dagli utenti come *feedback* agli annunci o messaggi che gli vengono mostrati - è ritardato, mentre per Apple è immediato. Inoltre, i dati sarebbero limitati ed eccessivamente aggregati, a differenza di quelli disponibili per Apple.

Ebbene, secondo l'AGCM, con l'adozione di questa differente politica ne sarebbe derivata una minor capacità di profilazione degli utenti e un aumento del costo medio per azione «dell'acquisto da parte degli inserzionisti di spazi pubblicitari sulle app dei concorrenti di Apple. In particolare, per ogni azione di conversione effettuata dagli utenti» tale costo sarebbe aumentato con una media di oltre il 150% in

Italia [116]. Da ciò ne è derivata una riduzione dei ricavi degli sviluppatori concorrenti e, viceversa, un aumento di quelli di Apple [117].

Sicché, stando al provvedimento dell'Autorità, la società in questione adotterebbe una politica discriminatoria che produce una riduzione dei proventi per gli inserzionisti terzi a suo esclusivo favore, oltre che a ridurre l'ingresso o impedire la permanenza dei concorrenti sul mercato dello sviluppo e distribuzione di applicazioni, avvantaggiando così le applicazioni Apple. È per questo motivo che il dato rilevante non è rappresentato dal livello di privacy scelto da Apple, bensì dalla scelta di adottare politiche differenziate in tema di trattamento dei dati tra sé stessa e i concorrenti [118].

Tra l'altro, l'AGCM sostiene che un'ulteriore conseguenza sarebbe quella di indurre i concorrenti ad abbandonare quel modello di monetizzazione basato sulla pubblicità verso un modello a pagamento, riducendo così il loro livello di competitività rispetto agli sviluppatori Apple. Con ciò portando anche a un pregiudizio per i consumatori «per i quali si riduce la possibilità di scegliere app gratuite o a più basso prezzo offerte» dagli sviluppatori concorrenti [119]. In realtà, benché il ragionamento dell'Autorità sia chiaro e lineare, sarebbe preferibile - per tutte le ragioni già viste - parlare di scelta tra due modelli di pagamento differenti, l'uno monetario e l'altro per mezzo del trasferimento e della concessione di utilizzo dei dati personali dell'utente.

Il provvedimento conclude che, oltre a non incentivare lo sviluppo di applicazioni maggiormente innovative, la posizione di svantaggio delle applicazioni di terzi derivante dalla differente politica adottata indurrebbe i consumatori ad avvalersi sempre di più di dispositivi Apple, ostacolando il loro passaggio verso apparati dotati del concorrente sistema operativo.

---

[116] *Ivi*, 7.

[117] Secondo i dati dell'AGCM vi sarebbero stati mancati ricavi nel 2022 stimati di oltre il 50% per un ammontare di 10 miliardi di dollari.

[118] *Ivi*, 12.

[119] In tal senso §50, provvedimento AGCM, cit., 13.

8. *Il caso Google - Weople sulla portabilità dei dati personali*

Si è visto nei capitoli precedenti l'importanza del diritto alla portabilità dei dati; esso, come si vedrà, è previsto in differenti atti normativi. Tale diritto rileva non solo per ragioni di controllo dei dati da parte dell'interessato, ma ha ripercussioni anche a livello concorrenziale. Un recente caso ne ha messo in luce quest'ultimo aspetto.

Infatti, il 5 luglio 2022 l'autorità italiana Antitrust ha avviato un'istruttoria ai sensi della Legge n. 287 del 10 ottobre 1990 nei confronti di Google, ipotizzando un abuso di posizione dominante in violazione dell'art. 102 TFUE. Il caso si è concluso con un accordo, ma è utile ripercorrere la vicenda per la sua rilevanza e portata.

Il procedimento è stato avviato a seguito della segnalazione presentata dalla società Hoda S.r.l. Ciò che veniva discusso riguardava il fatto che Google avrebbe frapposto ostacoli all'individuazione di meccanismi di interoperabilità idonei a rendere i dati presenti nella propria piattaforma disponibili a piattaforme alternative; l'ostacolo derivava da una presunta complessità per gli utenti di esportare i propri dati all'app sviluppata da Hoda, denominata *Weople*.

La contestazione che veniva mossa a Google ruotava sul fatto che trasferisse i dati solo se la richiesta avveniva tramite un'utenza Google. Una scelta che, secondo la società istante, poneva chiaramente ostacoli alla sua attività, consistente nel consentire ai propri utenti di raccogliere in un'unica "cassaforte digitale" i dati raccolti da altre aziende (come le piattaforme digitali) e monetizzarli [120]. L'idea di fondo, rela-

[120] Weople è un servizio di infomediazione che si riferisce a quei modelli di business basati sull'offerta di servizi di intermediazione per ciò che concerne il trattamento e la protezione dei dati personali. In particolare, le new infomediaries si propongono di agire in favore e per conto degli interessati, offrendo loro un servizio che mira ad instaurare rapporti commerciali ai fini della condivisione degli stessi. Una volta trasferiti nella propria cassetta di sicurezza, i dati possono essere monetizzati attraverso la funzione "salvadanaio personale". In esso, infatti, l'app Weople promette di versare quanto le aziende pagheranno per mandare all'interessato una pubblicità e/o un'offerta di prodotti o servizi personalizzati.

tiva al servizio *Weople*, è quella di costituire la prima banca per investire e recuperare valore dai propri dati.

Pertanto, mediante l'apertura di un *account* sulla piattaforma *Weople*, l'interessato può delegare l'infomediario a richiedere una copia dei dati personali già trattati da altri fornitori così che tali informazioni possano essere concentrate nel *caveau*. Come si vedrà, è ciò che è stato ormai istituzionalizzato con il DGA.

Il procedimento si è concluso con l'assunzione di tre impegni da parte di Google, il quale è chiamato a realizzare una serie di strumenti per la portabilità dei dati. Gli impegni assunti consistono nell'agevolare la portabilità dei dati degli utenti; nel migliorare l'utilità dei dati esportati e condivisi dagli utenti con operatori terzi; nell'accelerare l'effettiva adozione di una nuova soluzione di portabilità diretta dei dati da servizio a servizio che Google metterà a disposizione di operatori terzi autorizzati da un utente finale i cui dati siano oggetto della richiesta di portabilità relativa a taluni prodotti di Google.

Nel valutare la sussistenza di una posizione di dominanza da parte di Google, l'Autorità nota come la piattaforma in esame metta a disposizione dell'utente una pluralità di servizi, tra loro interconnessi. Tali servizi, in quanto parti dell'ecosistema Google, diventano fonti di estrazione dei dati di ciascun utente e permettono al gigante del web di disporre di una mole di informazioni pressoché illimitata. A fronte di ciò, essa definisce quali mercati rilevanti, l'insieme delle attività che consentono a Google di accumulare, custodire ed elaborare i dati degli utenti finali, e riconosce come, in ciascuno di essi, la piatta-

---

A tale servizio poi, si affianca anche la funzione di gestione dei diritti dell'interessato, come il diritto di revoca del consenso o di rettifica. Weople infatti, in questo caso, agisce da intermediario, veicolando le richieste verso le aziende nei confronti delle quali l'interessato decide di agire. Tale servizio, in conclusione, consente di mettere a disposizione dell'interessato il patrimonio di dati personali a lui appartenenti, permettendogli di essere reso edotto della quantità di informazioni che fino a quel momento ha diffuso, con la possibilità, tra l'altro, di trarne un guadagno. Sul tema si veda F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act,* cit., 213 ss.

forma in esame detenga una quota di mercato superiore al 50%, ritenendo dunque comprovata la sussistenza della sua posizione dominante.

Per il comportamento abusivo, vengono rilevati due distinti caratteri restrittivi della concorrenza conseguenti alla condotta posta in essere da Google:

il primo, consistente nell'assenza di meccanismi di interoperabilità che pregiudica l'esercizio, da parte dell'utente finale, del diritto alla portabilità dei dati, cui consegue un indebito sfruttamento dell'utente da parte di Google, essendo esso privato dei benefici che potrebbe trarre dalla valorizzazione, anche economica, dei propri dati personali.

Il secondo, consistente nel fatto che tale condotta limiterebbe la possibilità di operatori alternativi a Google di sviluppare forme innovative di utilizzo di tali informazioni.

Quindi, Google negando l'applicazione di meccanismi di interoperabilità, sarebbe in grado di preservare la propria posizione dominante, ostacolando lo sviluppo di modalità alternative di valorizzazione delle informazioni detenute e, perciò, la realizzazione di una concorrenza basata sul merito.

A ciò l'Autorità aggiunge la duplice valenza concorrenziale che, nei mercati digitali, ha la portabilità dei dati, così come disciplinata dall'art. 20 del GDPR. Un corretto esercizio di tale diritto infatti, permetterebbe, da una parte di rafforzare la possibilità di esercitare pressione su operatori commerciali come Google, e dall'altra, offrirebbe agli utenti la possibilità di conseguire il massimo potenziale economico conseguente all'utilizzo dei dati personali.

Sulla base di tali presupposti, quindi, l'AGCM ha deciso di avviare una istruttoria per abuso di posizione dominante. Con l'avvio del procedimento in questione, il diritto alla portabilità dei dati è divenuto il mezzo - non solo per un rafforzamento del controllo sui propri dati - ma anche per poter garantire all'interessato la possibilità di sfruttare economicamente le informazioni che genera.

Il diritto di cui all'art. 20 GDPR - soprattutto se esteso anche ai dati non personali - può assurgere a diritto da proteggere, oltre che da promuovere, non solo in quanto *species* del diritto di ogni persona

a un giusto trattamento dei dati personali, ma anche perché cruciale per il corretto ed efficiente funzionamento del mercato digitale, «nella misura in cui la sua violazione implica un pregiudizio al sistema concorrenziale, al benessere dei consumatori e alla libertà d'impresa» [121]. Il rifiuto alla richiesta di trasmissione dei dati, opposto da parte di un'impresa che si colloca in una posizione dominante, è astrattamente in grado di costituire una forma di rifiuto a contrarre. Tale comportamento, «di per sé ammesso, diviene però abusivo laddove manchi di una giustificazione oggettiva, ovvero nel caso in cui non risulti alcun contemperamento» tra i diversi interessi all'esercizio dell'autonomia privata e alla tutela del mercato [122].

Con la riduzione dei costi di *switching* dell'utente da una piattaforma all'altra, la portabilità dei dati può incidere, infatti, sulla mobilità degli utenti. La circolazione dei dati e la riduzione dei costi di *switching* possono contribuire a far sì che i dati non costituiscano una barriera all'ingresso, riducendo possibili rischi di *lock-in*, e che la mobilità degli utenti riduca gli effetti di rete connaturati all'attività delle piattaforme [123].

Il diritto alla portabilità dei dati così come è concepito, però, presenterebbe alcune criticità secondo parte della dottrina. È stato sottolineato un potenziale conflitto di interessi in capo alle società infomediarie che, interagendo con le *data companies* e altri terzi, potrebbero essere indotte a sacrificare le logiche di tutela dei diritti a beneficio degli interessi economici propri e della propria clientela, legati all'incremento di redditività, oltre al raggiungimento degli obiettivi della clientela *business* della società stessa, a cui vengono forniti i servizi a valore aggiunto [124]. Per questo nel DGA, al considerando n. 30, si legge che - per quei fornitori di servizi di intermediazione dei dati il cui obiettivo

---

[121] F. Ruggeri*, Poteri privati e mercati digitali,* cit.,183.

[122] *Ivi*, 184.

[123] AGCM, *Indagine conoscitiva sui big data,* cit., 75.

[124] F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act,* cit.*,* 230.

è quello di rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano - «(...) è importante che il [loro] modello commerciale garantisca che non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano» rispetto a quanto non sia nel loro stesso interesse.

9. *Il caso del Norwegian Consumer Council*

Un altro caso interessante, benché meno noto, è stato quello promosso dall'organismo norvegese che ha portato sette organizzazioni europee a interessare le rispettive autorità di regolazione nazionali [125]. La questione riguardava alcune pratiche realizzate da Google che, secondo l'Ente, violerebbero la privacy degli utenti e, si aggiunge qui, potrebbero produrre ripercussioni in materia di concorrenza al pari di altri casi.

Il rapporto norvegese si incentra in particolare sui dispositivi Android e, si legge anche in questo documento che la maggior parte dei servizi forniti da Google non prevede alcun compenso da parte dell'utente poiché il corrispettivo sarebbe rappresentato dalla raccolta dei dati e delle informazioni sul comportamento degli utenti, poi monetizzato mediante i servizi di pubblicità.

Il documento si basa sostanzialmente su due principali linee direttrici che si esprimono attraverso alcune pratiche rinvenibili nei dispositivi in esame, ossia la (costante) localizzazione della posizione dell'utente e i cc.dd. *dark patterns*.

Nella relazione viene dato risalto alla localizzazione quale dato utile per profilare un determinato utente, citando studi secondo cui sareb-

[125] La relazione dal titolo *every step you take. How deceptive design lets Google track users 24/7*, del 27 novembre 2018, è consultabile sul sito www.fil.forbrukerradet.no; anche se sono state interessate varie Autorità, ad oggi, non sembra esserci stato un qualche sviluppo ufficiale.

bero sufficienti quattro punti di localizzazione per identificare un individuo, giungendo a dedurre altresì dati sensibili, tra cui, opinioni religiose, posizioni politiche e informazioni sulla salute.

Le informazioni che possono essere raccolte tramite la localizzazione rilevano le abitudini e la personalità dell'utente, consentendo così di procedere indirizzando una pubblicità mirata e, in alcuni casi, dando vita a pratiche discriminatorie. La geolocalizzazione si combina con altri dati che vengono raccolti, come la cronologia di navigazione, le preferenze e i *social network*, generando in tal modo la pratica del c.d. *closing the loop*.

I *dark patterns*, invece, costituiscono delle pratiche ingannevoli che risiedono nella struttura e nella progettazione grafica di determinati dispositivi. Essi inducono l'utente a effettuare delle scelte a favore del fornitore dei servizi e contro i propri interessi. Tra queste pratiche si menzionano l'utilizzo di un determinato colore, la visibilità, il carattere di un testo; tutti elementi che orientano gli utenti verso una determinata opzione, portando spesso a travisare le conseguenze che derivano da una scelta anziché l'altra. Trattandosi in molti casi di dispositivi mobili, nella relazione si sottolinea che, spesso, la scelta dell'utente va a favore dell'opzione che consente di accedere nel minor tempo possibile ad un determinato servizio. L'esempio che si riporta è quello del pulsante "continua", che nei dispositivi Android è sempre blu ed è posizionato nell'angolo destro; tuttavia, in alcuni casi, tale pulsante blu comporta anche l'abilitazione di funzionalità "extra", che possono essere attivate se l'utente non presta la massima attenzione in ogni singola fase. In questo modo, prosegue la relazione, si finisce per occultare informazioni rilevanti, confondendo l'utente su ciò che le impostazioni effettivamente svolgono, impendendogli perciò di effettuare scelte consapevoli.

In riferimento alla pratica della localizzazione, il *report* suddivide l'analisi sulle due differenti impostazioni per la localizzazione dell'utente: la cronologia delle posizioni e la *Web & App Activity*.

La prima, è un'impostazione dell'*account* che registra continuamente la posizione dell'utente. Stando a quanto riferito dall'azienda, l'impostazione è necessaria per aiutare l'utente a ottenere risultati migliori e

consigli sui prodotti forniti, tra i quali i consigli basati sui luoghi che l'utente ha visitato con dispositivi sui quali ha effettuato l'accesso o le previsioni sul traffico. Tali dati sulla posizione possono tra l'altro essere raccolti sia quando l'utente si trova all'interno, sia quando si trova all'esterno di un edificio, poiché le modalità di tracciamento si svolgono attraverso il GPS, Wi-fi e Bluetooth.

Questa impostazione raccoglie una serie di dati dell'utente, inclusa la modalità di trasporto con cui effettua i suoi spostamenti, l'altitudine, le informazioni sul wi-fi, le coordinate GPS e il livello di batteria del dispositivo; questi vengono trasmessi alla società e memorizzate. Mentre alcuni di questi dati sono disponibili sull'*account* dell'utente (posizione, percorso, modalità di trasporto), altri (altitudine, hotspot Wi-fi, bluetooth e livello della batteria) non sono visibili e vengono raccolti in *background*.

In base a quanto riferito sul sito, *Web My Account* dell'azienda, questi dati, raccolti mediante questa impostazione, sono utilizzati anche per gli annunci pubblicitari mirati. Viene specificato che l'impostazione è volontaria e che gli utenti devono attivarla prima che essa possa funzionare.

Il *report* prosegue affermando che al momento dell'attivazione di un nuovo *account*, viene mostrata all'utente una versione monca e limitata di politica sulla *privacy*, e si possono accertare ulteriori informazioni e impostazioni solamente procedendo, ossia accedendo, su "altre opzioni". Invero, per sapere che i dati raccolti mediante la cronologia delle posizioni vengono utilizzati per scopi pubblicitari è necessario precedere accedendo all'area "ulteriori informazioni".

Tra le altre pratiche viene richiamata la prassi di richiesta di abilitazione dell'impostazione in momenti successivi rispetto all'attivazione dell'account. In altri termini, se l'utente non provvede all'attivazione durante il primo accesso, la richiesta viene rinnovata in successivi passaggi, come nel caso del primo accesso all'applicazione "Maps" in cui viene riferito all'utente che tale abilitazione è necessaria per ricevere consigli su percorsi, su orari per la visita di luoghi, o per salvare i luoghi visitati; anche in questo caso, per conoscere lo scopo pubblicitario, è necessario accedere a un'altra schermata, procedendo con un

clic su una freccia grigia poco visibile. La richiesta viene nuovamente inoltrata quando si accede per la prima volta sull'applicazione "foto", specificando che l'attivazione occorre per visualizzare le foto in base al luogo in cui si trova l'utente. In questo caso, alla richiesta di attivazione non appare alcuna informazione relativa alla cronologia delle posizioni prima che venga attivato il servizio. Viene rilevato che la ripetuta richiesta di attivare l'impostazione aumenta le possibilità che gli utenti attivino la stessa sia per errore, sia perché ritengono che altrimenti i servizi non funzioneranno nel modo più ottimale.

La pratica che porta all'automatica attivazione della cronologia delle posizioni per usufruire di alcuni servizi come quelli di cui sopra porterebbe alla assenza di granularità nella scelta, in quanto, come nel caso delle foto, l'utente che vuole fruire di tale servizio lo può ricevere solo accettando il rilevamento della posizione a fini pubblicitari. Stessa circostanza si verifica nel caso dell'assistente vocale, senza che l'utente sappia che tale servizio può funzionare anche se in seguito l'utente sospenda la cronologia delle posizioni.

La granularità è assente anche nel momento in cui gli utenti sono posti innanzi a un unico binario di scelta; ossia possono optare per un consenso all'attivazione di questa impostazione, che raccoglierà quindi i dati in qualsiasi momento, oppure debbono rifiutare l'impostazione nella sua interezza, bloccando così i servizi che richiedono la sua attivazione. L'applicazione, dunque, registra la posizione dell'utente anche quando la rispettiva applicazione di rilevamento non è in uso.

Ulteriori argomentazioni, poi, riguardano la sospensione dell'impostazione e l'assenza di una vera e propria disattivazione.

In merito alla *Web & App Activity,* [126] gli utenti possono visualizzare i dati raccolti sul loro profilo, in una raccolta separata rispetto a quella riguardante la cronologia delle posizioni.

---

[126] Questa viene presentata come un'altra impostazione che raccoglie una serie di dati dell'utente la cui funzione è quella di salvare le ricerche dell'utente, la cronologia di navigazione e le attività di siti e applicazioni, per ottenere migliori risultati di ricerca, suggerimenti e personalizzazione per tutti i servizi offerti.

Questa, a differenza della precedente, è attiva automaticamente, come impostazione predefinita quando viene attivato un *account* dell'azienda e i dati raccolti vengono, anche in questo caso, utilizzati per personalizzare la pubblicità. Si legge che quando viene attivato un *account*, non viene menzionato l'uso di questi dati ai fini pubblicitari, neppure dopo aver fatto accesso su "Ulteriori informazioni". Questa informazione avviene in alcuni contesti specifici e limitati, come l'ipotesi in cui l'impostazione venga disattivata dall'utente; in questo caso, quando lo stesso utente procede alla sua riattivazione, viene informato sugli scopi pubblicitari.

Infine, il *report* analizza l'applicazione dell'assistente vocale, la cui abilitazione comporta l'attivazione della cronologia delle posizioni. In tale schermata, ci si limita a riferire agli utenti che la cronologia delle posizioni «salva dove vai con i tuoi dispositivi» e solo procedendo con l'accesso ad altra schermata tramite il *clic* su una freccia grigia si espande una più ampia descrizione che include l'utilizzo dei dati per scopi pubblicitari. Da tutto quanto descritto, l'istituzione norvegese ne ricava violazioni della privacy [127].

Secondo il *NCC* la richiesta del consenso sopra descritta non consentirebbe all'utente di essere pienamente consapevole delle sue scelte; dunque, in suo difetto, il consenso non potrebbe essere considerato libero. Sarebbe carente anche il requisito della granularità come previsto nel considerando n. 32 GDPR.

Viene poi messo in dubbio che le informazioni rese siano sufficienti e tali da rendere la volontà espressa «specifica e informata». Ciò perché l'utente, per ricevere informazioni più dettagliate, deve accedere ad altre sezioni e anche in questo caso, secondo il *report*, è possibile che molti utenti non possano comprendere fino a che punto

[127] Considerato che la cronologia delle posizioni, per essere attivata, abbisognava del consenso dell'utente, secondo il NCC se ne evince che il trattamento di questi dati sia basato sul consenso; per converso, la fattispecie della *Web & App Activity*, essendo attivata in via predefinita, non può fondarsi sul consenso, bensì sull'interesse legittimo.

vengono elaborati i propri dati sulla posizione, che essi vengono archiviati definitivamente e che verranno utilizzati per fini pubblicitari. Peraltro, l'induzione di *clic* ingannevoli e informazioni nascoste, metterebbero in dubbio anche l'univocità della volontà espressa.

Le situazioni come quella appena analizzata potrebbero generare conseguenze anche in termini di concorrenza. Questo proprio per quello che si è visto nei precedenti paragrafi: gli standard di protezione dei dati personali costituiscono parametri utili a verificare la qualità di un determinato prodotto o servizio offerto. Minore è il grado di protezione garantito, maggiore sarà il pregiudizio per il consumatore.

Si è altresì visto che il diritto della concorrenza non salvaguarda esclusivamente gli interessi delle imprese, ma, anzi, ampia la tutela ai consumatori consentendo a questi di compiere *scelte libere* e consapevoli, garantendo così l'efficienza del sistema di economia del mercato.

Nel caso di specie, oltre a un'incidenza in termini di competitività, si potrebbe verificare un'ipotesi di pregiudizio al benessere dei consumatori aprendo le porte alla fattispecie sancita dell'art. 102 TFUE.

L'efficienza di un sistema di un'economia di mercato viene preservata tutelando anche le scelte dei consumatori affinché queste possano essere, si ribadisce, libere e consapevoli, senza alcun inganno nei loro confronti.

In un sistema concorrenziale, ovvero in un'economia di mercato, il mancato rispetto delle norme poste a tutela dei dati personali potrebbero danneggiare quelle imprese concorrenti che garantiscono il grado ed il livello di tutela previsti dalla legge. È utile rimarcare, peraltro, che le pratiche manipolative non impongono solo costi al singolo interessato. Esse minano anche il processo concorrenziale e il suo indebolimento si verifica sia nel mercato iniziale - quello in cui vengono raccolte le informazioni personali - sia nei mercati in cui le informazioni personali vengono successivamente utilizzate in modo contrario a quelle che sono le ragionevoli aspettative del consumatore.

Il giudizio diventa più netto allorché le modalità di trattamento delle informazioni acquisite dall'impresa non siano necessarie per l'erogazione del servizio offerto. Ogni qualvolta che un'impresa in posizio-

ne dominante impone ai consumatori una scarsa tutela della privacy, realizza un potenziale abuso della sua posizione a scapito dei consumatori [128].

[128] Sul tema si veda H. A. SHELANSKI, *Information, Innovation, and Competition Policy for the Internet,* in *University of Pennsylvania Law Review*, vol. 161, n. 6, 2013, 1663, spec. 1687.

Capitolo IV

IL NUOVO QUADRO REGOLATORIO EUROPEO IN TEMA DI MERCATI DIGITALI E LA VALORIZZAZIONE DEI DATI

Sommario: 1. Il regolamento europeo *Platform-to-Business* (P2B - Reg. UE 2019/1150) e gli altri interventi normativi che regolano i mercati digitali – 2. Il *Digital Markets Act* (DMA - Reg. UE 2022/1925) – 3. Il *ne bis in idem*. La necessità di coordinare la disciplina antitrust tradizionale e il DMA – 4. I *gatekeeper* secondo il *Digital Markets Act* – 5. Le pratiche sleali o limitative della contendibilità (artt. 5 - 7 DMA): gli obblighi e i divieti – 6. I poteri della Commissione europea – 7. I primi casi applicativi del DMA – 8. Il *Digital Services Act* (DSA – Reg. UE 2022/2065) – 9. Scopo e applicazione del *Digital Services Act* – 10. Il quadro di esenzione da responsabilità dei prestatori di servizi intermediari – 11. Gli obblighi per i prestatori di servizi intermediari nel DSA – 11.1 Obblighi applicabili a tutti i prestatori – 11.2. Obblighi applicabili ai prestatori di servizi di memorizzazione di informazioni – 11.3 I poteri dei fornitori di piattaforme online e i relativi obblighi – 11.4 Obblighi supplementari per i fornitori di piattaforme online (VLOP) e di motori di ricerca online di dimensioni molto grandi (VLOSE) – 12. I primi casi applicativi del DSA – 13. La nuova figura di «utente commerciale» e di «operatore commerciale» nei mercati digitali – 14. La creazione dei servizi di intermediazione nella strategia europea per i dati con il *Data Governance Act* (DGA – Reg. UE 2022/868) – 15. La circolazione dei dati nel sistema dell'*Internet of Things* con il *Data Act* (Reg. UE 2023/2854)

1. *Il regolamento europeo Platform-to-Business (P2B - Reg. UE 2019/1150) e gli altri interventi normativi che regolano i mercati digitali*

Nel corso degli ultimi anni il legislatore europeo è intervenuto più volte con l'obiettivo di disciplinare i mercati digitali [1].

È intervenuto con il *Digital Markets Act* che, da un lato, si occupa di prevedere regole *ex ante* volte a regolare le grandi piattaforme, prescrivendo obblighi e divieti precisi, accentrando importanti poteri e competenze in capo alla Commissione europea.

È intervenuto con il *Digital Services Act* che, dall'altro, mira a stabilire le regole valenti per vari operatori nei mercati digitali a seconda dell'attività svolta e si incentra, in particolare, nel regolare i flussi informativi che circolano nel web, con l'obiettivo di eliminare i contenuti illegali.

Prima ancora di questi regolamenti, però, il legislatore era già intervenuto con il regolamento *Platform-to-Business* (P2B - Reg. UE 2019/1150), il quale promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.

Questi interventi legislativi sono stati stimolati dal fatto che le regole sulla concorrenza "tradizionali", previsti per quelli che sono i mercati *off-line*, presentano alcuni limiti applicativi. È stato rilevato che, per un verso, la velocità e il dinamismo di questi mercati digitali renda la tutela *ex post* inadeguata ad assicurare rimedi efficaci e tempestivi. D'altro canto, risulta difficoltoso individuare i parametri con i quali valutare le condotte che si presumono illecite, considerato che queste si mostrano in una loro duplice natura [2].

In dottrina è stato sottolineato che «in una chiave di "efficienza statica" e di breve periodo (e scontando l'impatto sui dati personali),

---

[1] Non mancano le critiche a quella ipertrofia normativa che sembra caratterizzare gli ultimi anni. Si veda M. AINIS, *L'Autorità Antitrust alla prova dei mercati digitali*, in *Diritto dell'informazione e dell'informatica*, vol. 41, n. 1, 2022, 1.

[2] M.W. MONTEROSSI, *La tutela dell'utente commerciale nei mercati digitali*, in *Contratto e impresa*, vol. 28, n. 3, 2021, 920, spec. 928.

queste pratiche possono rivelarsi, per certi versi, fonte di benefici per i consumatori finali; rendendo, in ogni caso, complessa la definizione degli effetti negativi sui mercati interessati (...). Tuttavia, ove a prevalere sia una lettura improntata all'efficienza dinamica» alcune pratiche realizzate dalle piattaforme digitali manifestano il loro potenziale anticompetitivo [3]. Tali pratiche sono in grado di «minare tanto la fiducia degli utenti commerciali che operano all'interno della piattaforma (concorrenza *intra-platform*), perché incapaci di controllare i fattori che portano alla remunerazione dei propri investimenti; tanto quella delle piccole e medie imprese, desiderose di affermarsi nel mercato delle piattaforme (concorrenza *inter-platforms*), perché prive dei fattori di produzione necessari per esercitare l'attività economica in modo redditizio. L'uno e l'altro fattore contribuiscono così all'attribuzione di un potere di decisione sul se e come innovare in capo a pochi *big players*» [4].

L'obiettivo perseguito con il regolamento P2B è quello di assicurare la trasparenza e l'equità del contenuto contrattuale che i fornitori del servizio possono imporre agli utenti commerciali. Il regolamento delinea una serie di obblighi che, contrariamente a quanto accade per il DMA, sono previsti per tutte le imprese che gestiscono piattaforme online, a prescindere dalle loro dimensioni o dal loro potere di mercato [5]. Il regolamento P2B prevede una serie di prescrizioni generali volte a garantire la conoscibilità del contenuto contrattuale all'utente, il quale deve soddisfare i requisiti della semplicità e comprensibilità, oltre a essere facilmente reperibile all'interno del sistema digitale di cui trattasi. A questi si aggiungono obblighi di trasparenza più specifici per i fornitori di servizi di intermediazione [6]. Se il contratto non rispetta i requisiti di trasparenza richiesti, è previsto il rimedio della nullità all'art. 3 del P2B.

---

[3] *Ivi*, 929.
[4] *Ibidem*.
[5] *Ivi*, 934.
[6] *Ivi*, 936.

Siffatto regolamento, quindi, deve necessariamente coordinarsi con gli altri due regolamenti del DMA e DSA. Questi ultimi due regolamenti, come è stato già rilevato in letteratura, devono trovare un loro coordinamento, stante anche una integrazione con l'*Artificial intelligence act* (AIA) che, allo stato, non pare sufficiente [7].

In un quadro ancora più ampio, si può dire che questi ultimi regolamenti si inseriscono nel complesso quadro normativo inerente ai prestatori dei servizi nella rete. Il quadro in questione si compone di una base normativa individuabile nella dir. 2000/31/CE dell'8 giugno 2000 (direttiva sul commercio elettronico), recepita nell'ordinamento italiano con il d.lgs. 9 aprile 2003, n. 70. Infine, oltre al DMA e DSA, l'impianto normativo in tema di attività degli intermediari deve menzionare anche la dir. 2019/790/UE sul diritto d'autore e i diritti connessi nel mercato unico digitale recepita in Italia col d.lgs. dell'8 novembre 2021, n. 177 [8].

Il DMA e il DSA sono ancora in una fase applicativa iniziale e le varie impugnazioni avanzate in sede giurisdizionale europea da parte di molte importanti piattaforme digitali costituiscono il preludio di una fase complessa in cui la prassi assumerà un ruolo rilevante [9].

2. *Il Digital Markets Act (DMA - Reg. UE 2022/1925)*

Il DMA intende contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate con l'obiettivo di garantire a tutte le imprese che i mercati nel settore digitale nei quali sono presen-

---

[7] In questo senso, A. IANNOTTI DELLA VALLE, *Il Digital Markets Act e il ruolo dell'unione europea verso un costituzionalismo digitale*, in *Giurisprudenza costituzionale*, vol. 67, n. 3, 2022, 1867, spec. 1876-1877.

[8] F. PIRAINO, *La responsabilità dei prestatori di servizi di condivisione di contenuti online*, in *Nuove leggi civili commentate*, n. 1, 2023, 146, spec. 147.

[9] M. MIDIRI, *I Signori del Tech e la sfida sulle regole: il caso Amazon,* in *federalismi.it,* n. 28, 2023, 100, spec. 105.

ti *gatekeeper* siano equi e contendibili a vantaggio degli utenti commerciali e degli utenti finali [10].

Infatti, nel considerando n. 7 del regolamento si legge proprio che la finalità della normativa è quella di contribuire «al corretto funzionamento del mercato interno stabilendo norme volte a garantire la contendibilità e l'equità per i mercati nel settore digitale in generale e per gli utenti commerciali e gli utenti finali dei servizi di piattaforma di base forniti dai *gatekeeper* in particolare».

Con il considerando n. 13 il legislatore è ancora più specifico là dove segnala la centralità di quelle imprese che fungono (principalmente) da intermediari diretti tra utenti commerciali e utenti finali in quei mercati dove prevalgono «caratteristiche quali economie di scala estreme, effetti di rete molto forti, abilità di connettere molti utenti commerciali con molti utenti finali tramite la multilateralità di tali servizi, effetti di *lock-in*, indisponibilità del *multihoming* o integrazione verticale» e che oggi sono in grado «di stabilire agevolmente condizioni e modalità commerciali in maniera unilaterale e pregiudizievole per i loro utenti commerciali e finali» [11].

Sostanzialmente, è utile ripeterlo, il legislatore sarebbe intervenuto con lo scopo dichiarato di porre un freno all'immenso potere acquisito da alcune piattaforme, a beneficio della contendibilità del mercato e, quindi, a favore di piccole e medie imprese che intendano parteciparvi.

---

[10] Sul concetto di "contendibilità" ed "equità" inseriti nell'art. 1 DMA e nei considerando nn. 32 e 33, nonché sul percorso che ha portato all'adozione finale del testo legislativo, si veda A. R. Martìnez, *The DMA's Ithaca: Contestable and Fair Markets*, in *World Competition*, vol. 46, n. 4, 2023, 1-30; sul tema si veda anche G. Olivieri, *Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali*, in *Orizzonti del Diritto Commerciale*, fasc. sp., 2021, 359.

[11] Con *multi-homing*, ai fini del DMA, si intende la possibilità per l'utente commerciale di vendere i suoi prodotti o servizi attraverso piattaforme concorrenti, oppure per il tramite di un proprio canale diretto di vendita. G. Afferni, *Gli obblighi dei gatekeeper*, in L. Bolognini, E. Pelino, M. Scialdone (a cura di), *Digital Services Act e Digital Markets Act*, Milano, Giuffrè Francis Lefebvre, 2023, 320.

All'art. 1, par. 2, DMA è prevista una disposizione dell'ambito di applicazione territoriale simile a quanto è previsto nel GDPR. Invero, è stabilito che il regolamento trova applicazione ai servizi di piattaforma di base forniti o offerti dai *gatekeeper* a utenti commerciali stabiliti nell'Unione o a utenti finali stabiliti o situati nell'Unione, a prescindere dal luogo di stabilimento o di residenza dei *gatekeeper* e dalla normativa altrimenti applicabile alla fornitura del servizio.

Con questo regolamento sui mercati digitali il legislatore è intervenuto prescrivendo una serie di obblighi (*rectius*, divieti) in capo alle piattaforme digitali che dominano i mercati in questione definendoli *gatekeeper*[12]. In realtà, benché il legislatore stesso (dagli artt. 5 e ss.) li definisca genericamente "obblighi", la maggior parte delle prescrizioni costituiscono più propriamente dei divieti che di seguito si tenterà di ordinare[13].

Il DMA è stato elaborato anche per far fronte alla difficoltà di applicare gli illeciti antitrust nell'ambito dei mercati digitali e perché questi ultimi, come si è visto, avendo una applicazione *ex post*, presentano un effetto tardivo e culminano in sanzioni facilmente assorbibili dalle imprese *big tech*[14].

---

[12] G. GUZZARDI, *L'abuso di posizione dominante nel mercato dei servizi digitali,* cit., 318, sottolinea che mentre gli artt. 101 e 102 TFUE sono in grado di intervenire solo *ex post* ad esito di lunghe e complesse indagini, il DMA pur se applicabile solo dalla Commissione, consente mirati interventi *ex ante* volti a limitare l'utilizzo dei dati personali sensibili per la pubblicità mirata ed evitare il consolidarsi di posizioni anticoncorrenziali.

[13] Anche nella versione inglese e francese si parla di *obligations* e in quella tedesca di *Verpflichtungen*.

[14] Con il considerando n. 5 del DMA viene infatti affermato che «(...) spesso i processi di mercato non sono in grado di garantire risultati economici equi per quanto riguarda i servizi di piattaforma di base. Sebbene gli articoli 101 e 102 del trattato sul funzionamento dell'Unione europea (TFUE) si applichino al comportamento dei gatekeeper, l'ambito di applicazione di tali disposizioni è limitato a talune tipologie di potere di mercato, per esempio una posizione dominante in mercati specifici e di comportamento anticoncorrenziale, e la loro applicazione avviene ex post e richiede un'indagine approfondita, caso per caso, di fatti spesso molto complessi.

È, quindi, un regolamento che nasce dalla debolezza dell'efficienza dinamica dei mercati digitali. Il numero di *startup* è in diminuzione, così come si va attenuando l'innovazione; si hanno quindi mercati in cui il comportamento delle piattaforme non è trasparente e la manipolazione dei dati degli utenti è prassi comune [15]. Oggi si assiste a una progressiva copertura, da parte del diritto concorrenziale, di quelle fattispecie rilevanti ai sensi del DMA. Ciò è avvenuto a seguito di una progressiva affermazione di interpretazioni estensive della norma sul divieto di abuso di posizione dominante che non è avvenuto in precedenza, non solo perché le norme antitrust si limitavano a specifici mercati e a specifiche condotte anticoncorrenziali, ma anche ad una sorta di inerzia delle autorità nei mercati digitali dovuto a una qualche forma di deferenza per l'innovazione; con la convinzione della piena apertura dei mercati digitali [16].

Le nuove regolazioni sono, quindi, idealmente incentrate sull'idea di controllo del potere di mercato, e si pongono in continuità ideale con il divieto di abuso di posizione dominante del diritto antitrust europeo [17].

Prima di analizzare l'interazione tra la tradizionale normativa in materia di concorrenza e la normativa regolamentare del DMA, è necessario accennare al fatto che, il 17 aprile 2023, la Commissione europea ha adottato anche il regolamento di esecuzione (UE) 2023/814

Inoltre, il diritto vigente dell'Unione non affronta, o non affronta in maniera efficace, i problemi per quanto concerne l'efficiente funzionamento del mercato interno, imputabili al comportamento dei gatekeeper che non dispongono necessariamente di una posizione dominante in termini di diritto della concorrenza». Sul punto si veda anche M. Midiri, *I Signori del Tech e la sfida sulle regole,* cit.*,* 103.

[15] M. Libertini, *Digital markets and competition policy. Some remarks on the suitability on the antitrust toolkit*, in *Orizzonti del Diritto Commerciale*, fasc. Sp., 2021, 337, spec. 341.

[16] M. Libertini, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Riv. Trim. dir. pubblico*, n. 4, 2022, 1069, spec. 1074-1075. Secondo l'A., ciò avrebbe portato ad apprezzare il dinamismo concorrenziale che ha caratterizzato i giganti del web come un successo dell'economica di mercato e meritevole di essere quindi assecondato.

[17] *Ivi*, 1076.

sulle modalità dettagliate di attuazione di determinate procedure che fanno capo alla Commissione stessa [18].

3. *Il ne bis in idem. La necessità di coordinare la disciplina antitrust tradizionale e il DMA*

Un primo problema della nuova disciplina europea è il suo coordinamento con la normativa in materia di concorrenza. Infatti, alcuni casi rischiano di ricadere nell'applicabilità di entrambe le normative con il rischio che uno stesso fatto venga sottoposto a una duplice sanzione [19].

La Commissione europea si trova in una posizione in cui l'applicazione del diritto della concorrenza avverrà, almeno in linea di principio, in parallelo alla supervisione e all'applicazione del DMA. Potrà accadere che una piattaforma digitale sia assoggettata a molteplici procedimenti a seguito di una medesima condotta sollevando l'interrogativo se ciò sia compatibile con il principio del *ne bis in idem* [20].

Si è fatto notare come l'interazione del DMA dovrà essere analizzata ed esplorata anche in relazione al c.d. Regolamento P2B, alla direttiva sulle pratiche commerciali sleali, al GDPR, alla direttiva

---

[18] Si tratta di profili specifici tra cui la forma, il contenuto ed altri elementi legati alle notifiche e alle comunicazioni connesse alla designazione dei *gatekeeper*; alle richieste motivate sugli obblighi imposti ai *gatekeeper*; alle relazioni regolamentari; alle notifiche e comunicazioni sugli obblighi di informazione in merito alle concentrazioni e all'obbligo di *audit*. Inoltre, regolamenta i procedimenti sull'inosservanza degli obblighi da parte dei *gatekeeper*; l'esercizio del diritto di essere ascoltati e la procedura di divulgazione previsti dall'art. 34 DMA.

[19] Sul tema si vedano M. LIBERTINI, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza,* cit., 1070-1078; N. M. FARAONE, *Della serie "a volte ritornano" (o non se ne sono mai veramente andati): il principio del ne bis in idem alla prova delle piattaforme digitali*, in *federalismi.it*, n. 6, 2023, 69; M. COLANGELO, *La regolazione ex ante delle piattaforme digitali: analisi e spunti di riflessione sul Regolamento sui mercati digitali,* in *Le nuove leggi civili commentate*, n. 2, 2023, 415, spec. 432.

[20] N.M. FARAONE, *Della serie "a volte ritornano"*, cit., 87.

AVMS sui servizi media audiovisivi e alla Direttiva Copyright. Un ulteriore conflitto potrebbe finanche aversi rispetto all'art. 30, L. 118/2022 che ha integrato l'abuso di dipendenza economica introducendo all'art. 9 della legge sulla subfornitura una presunzione non assoluta nel caso di impresa che utilizza servizi di intermediazione forniti da una piattaforma digitale che abbia un ruolo determinante per raggiungere utenti finali o fornitori, anche in termini di effetti di rete o di disponibilità dei dati; un elenco non vincolante di pratiche abusive realizzate dalle piattaforme digitali che possono integrare un abuso di dipendenza economica, modificando *ex novo* il secondo comma [21].

Tuttavia, parte della dottrina già rileva che DMA, abuso di dipendenza economica e abuso di posizione dominante hanno a che fare con tre moventi di interesse pubblico differenti e, dunque, che, a rigore, ne giustificano e ne legittimano una applicazione parallela e l'eventuale cumulo di sanzioni [22].

Anche altra dottrina sembra ammettere la possibilità di una applicazione cumulativa di norme antitrust e DMA rilevando però che, in caso di sanzioni, "l'eccesso" verrebbe scongiurato con l'applicazione del principio di proporzionalità [23]. Si può giungere a questa conclusione partendo dal considerando n. 11 e n. 78, oltre all'art. 1 DMA [24]. Il

---

[21] *Ivi*, 91.

[22] Sul punto V. Falce, *L'abuso di dipendenza economica nel digitale. Perché no?*, in *Filodiritto*, 5 maggio 2022, secondo cui DMA e abuso dipendenza economica perseguono fini diversi. La seconda completa il primo anziché sovrapporsi un po' come l'azione di classe rispetto all'illecito antitrust; N.M. Faraone, *Della serie "a volte ritornano"*, cit., 95.

[23] M. Libertini, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza,* cit.,1078; Sulla stessa linea si veda P. Bashenhof, *The digital Markets act (DMA): A Procompetitive Recalibration of Data Relations?*, in *Journal of Law, Technology and Policy*, n. 1, 2022, 101 ss., spec. 148.

[24] A mente del considerando n. 11 «gli articoli 101 e 102 TFUE e le corrispondenti norme nazionali in materia di concorrenza relative a comportamenti anticoncorrenziali unilaterali e multilaterali, come pure al controllo delle concentrazioni, si prefiggono quale obiettivo la protezione della concorrenza non falsata sul mercato.

secondo considerando riportato prevede il principio che fa salvo il potere della Commissione di aprire procedimenti ai sensi degli artt. 101 e 102 TFUE. Il testo può essere interpretato nel senso che l'Autorità europea sarebbe libera di avviare procedimenti antitrust nei mercati digitali solo in relazione a condotte non rientranti nell'ambito del DMA, facendo quindi pensare a un rapporto di specialità per cui la presenza di norme del DMA escluderebbe l'applicazione delle norme di concorrenza alla stessa fattispecie [25]. L'art. 1, par. 6, dal canto suo esclude testualmente che tra le norme del DMA e quelle antitrust ci sia un rapporto di specialità, ma lascia aperti i problemi relativi alla contemporanea vigenza dei due complessi normativi, inclusi quelli relativi allo scopo delle norme e agli interessi tutelati [26].

In sostanza, si tratta di un tema che dovrà necessariamente trovare una risposta univoca e definitiva ancorché, ad oggi, sembra prevalere una tesi che, sulla base di un'interpretazione teleologica, non esclude l'applicabilità simultanea di entrambi gli strumenti normativi.

4. *I gatekeeper secondo il Digital Markets Act*

Il DMA è essenzialmente dedicato a quegli operatori digitali che per il loro potere assumono un ruolo di regolatori privati dei mercati e controllori delle porte che ne delimitano l'accesso; da qui, il termine

---

Il presente regolamento persegue un obiettivo complementare, ma diverso, alla protezione della concorrenza non falsata su un dato mercato, quale definita in termini di diritto della concorrenza, e tale obiettivo consiste nel garantire che i mercati in cui sono presenti gatekeeper siano e rimangano equi e contendibili, indipendentemente dagli effetti reali, potenziali o presunti sulla concorrenza in un dato mercato derivanti dal comportamento di un dato gatekeeper contemplato dal presente regolamento. Il presente regolamento mira pertanto a proteggere un interesse giuridico diverso rispetto a quello protetto da tali norme e dovrebbe applicarsi senza pregiudicare l'applicazione di queste ultime».

[25] M. LIBERTINI, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza,* cit.*,* 1070.

[26] *Ibidem*.

inglese di *gatekeeper*, inteso come "custode" [27]. Quest'ultimo, secondo l'art. 2 DMA, è identificato in quell'impresa che fornisce servizi di piattaforma di base, vale a dire: intermediazione online; motori di ricerca; *social network*; condivisione video; comunicazione interpersonale indipendenti dal numero; sistemi operativi; *browser web*; assistenti virtuali; *cloud computing*; pubblicità online o qualunque servizio di intermediazione pubblicitaria erogati da un'impresa che fornisce uno dei precedenti servizi [28]. Questo è il requisito "qualitativo".

La designazione del *gatekeeper* (art. 3 DMA) avviene anche in forza di un altro requisito "quantitativo", vale a dire con il superamento di determinate soglie di mercato. Al verificarsi dei requisiti di legge, l'impresa interessata è tenuta a una notifica alla Commissione europea entro due mesi dalla loro verificazione [29].

Può tuttavia accadere che, pur raggiungendo tutte le soglie previste dal Regolamento, per alcune circostanze relative al funzionamento del servizio non siano soddisfatti i requisiti richiesti e che l'impresa possa essere esentata dall'applicazione del DMA. È facoltà della Commissione europea quella di procedere in ogni caso alla designazione dell'impresa quale *gatekeeper* in base alle informazioni in suo possesso.

I requisiti affinchè una impresa sia designata come *gatekeeper* riguardano l'impatto significativo sul mercato interno. Questo è presunto se viene raggiunto un fatturato annuo nell'Unione europea pari o superiore a 7,5 miliardi di euro in ciascuno degli ultimi tre esercizi finanziari o se la sua capitalizzazione di mercato media o il suo valore equo di mercato era quanto meno pari a 75 miliardi di euro nell'ultimo eser-

---

[27] M. W. Monterossi, *La tutela dell'utente commerciale nei mercati digitali*, cit., 928.

[28] Per una ricostruzione storica della figura del *gatekeeper*, si veda J. Zittrain, *History of Online Gatekeeping,* in *Harvard J. Of Law & Tech.*, vol. 19, n. 2, 2006, 253.

[29] Sulla designazione dei *Gatekeeper* si veda M. Scialdone, *Digital Services Act e Digital Markets Act,* cit., 301 ss.; P. Manzini, *Equità e contendibilità nei mercati digitali,* cit., 37, rileva come il DMA individui i *gatekeeper* sulla base di criteri diversi rispetto all'art. 102 TFUE per stabilire il dominio sul mercato. Il primo criterio è relativo al tipo di servizi offerti dalla piattaforma (parametro qualitativo); il secondo, riguarda elementi dimensionali della stessa (parametro quantitativo).

cizio finanziario. Affinché vi sia la presunzione in questione, l'impresa deve fornire il servizio almeno in tre stati membri UE. Un secondo requisito si riferisce al fatto che il servizio deve costituire un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano quelli finali. Anche in questo caso è prevista una presunzione legale, ossia se nell'ultimo esercizio finanziario l'impresa ha avuto almeno 45 milioni di utenti finali attivi su base mensile e almeno 10.000 utenti commerciali attivi su base annua stabiliti nell'UE identificati e calcolati conformemente alla metodologia e agli indicatori presenti nell'allegato del DMA. Un ulteriore requisito risiede nel fatto che l'impresa detiene una posizione consolidata e duratura o qualora sia prevedibile che acquisisca siffatta posizione nel prossimo futuro.

Sul tema della designazione dei *gatekeeper* si è già assistito a un contenzioso europeo instaurato da Bytedance (TikTok), il quale ha impugnato la decisione della Commissione europea che lo designava come tale. Il giudizio si è concluso con la decisione del Tribunale UE che il 17 luglio 2024 ha rigettato la domanda di Bytedance [30].

La maggior parte degli obblighi e divieti prescritti dal DMA, che si vedrà qui di seguito, si ispirano a quei precedenti giurisprudenziali già conclusi in tema di diritto della concorrenza e a quei casi ancora aperti [31].

---

[30] Nel caso Bytedance, T-1077/23, 17 luglio 2024, curia.europa.eu, il Tribunale UE ha accertato la correttezza dell'operato della Commissione europea, la quale ha accertato adeguatamente le soglie quantitative considerando, tra le varie, anche la portata internazionale della società, il numero di utenti nell'UE e il numero di anni durante i quali la soglia degli utenti è stata raggiunta. È stata d'altra parte ritenuta infondata la tesi del ricorrente che sosteneva come la portata principale della società fosse da ascrivere al mercato cinese e che l'impatto nel mercato interno europeo non fosse significativo. Una seconda tesi difensiva, anch'essa rigettata, riguardava il fatto che TikTok non si avvalesse dei sistemi che producevano effetti di rete o lock-in al pari di concorrenti come Instagram e Facebook.

[31] M.V. LA ROSA, *Digital Services Act e Digital Markets Act,* cit., 260; per l'associazione delle varie prescrizioni legislative ai rispettivi casi giurisprudenziali si farà riferimento al contributo di M. COLANGELO, *La regolazione ex ante delle piattaforme digitali,* cit., 415.

5. *Le pratiche sleali o limitative della contendibilità (artt. 5 - 7 DMA): gli obblighi e i divieti*

Il DMA prescrive alcuni divieti in capo ai *gatekeeper*, alcuni dei quali applicabili salvo che l'utente finale presti il proprio consenso a una scelta specifica [32].

Da una lettura complessiva del regolamento - e quindi come regola/parametro generale - c'è chi sostiene che va ritenuta "sleale" qualsivoglia pratica con la quale il *gatekeeper*, basandosi sullo squilibrio dei rapporti di forza, riesce a comprimere eccessivamente l'utilità degli utenti commerciali. La pratica, secondo tale tesi, potrebbe essere concettualmente ricondotta nella categoria degli abusi di sfruttamento [33].

I vari obblighi del DMA possono essere suddivisi in due categorie:

la prima, inerente a quegli obblighi che mirano a evitare alcune pratiche di sfruttamento degli utenti dei sevizi, sia finali che commerciali e, la seconda che mira a prevenire alcune pratiche di esclusione dei concorrenti riconducibili alla tipologia delle vendite abbinate.

Quindi, anche in questo caso si riproduce la dicotomia tra abusi di sfruttamento e abusi escludenti.

Nell'ambito dell'art. 6, invece, verrebbero a configurarsi tre classi di obblighi, tutti relativi a condotte escludenti e «aventi ad oggetto le pratiche discriminatorie dei concorrenti, alcune vendite aggregate e, infine, alcune restrizioni all'accesso ai dati» [34].

L'intersezione naturale della disciplina con la materia dei dati personali emerge immediatamente dalla lettura dell'art. 5 del DMA, il

---

[32] In relazione alla prestazione del consenso si esprime in senso critico E. Cremona, *L'erompere dei poteri privati nei mercati,* cit., 904, che sul divieto di combinazione dati rileva che «una operazione di sostituzione di un consenso globale delle condizioni generali (o dei termini d'uso) con tanti specifici consensi rischia di risolversi in una consapevolezza ancor minore delle scelte effettuate».

[33] P. Manzini*, Equità e contendibilità nei mercati digitali*, cit., 40.

[34] *Ibidem*. Secondo altri in dottrina, invece, la distinzione tra i due elenchi degli artt. 5 e 6 non è chiara. In quest'ultimo senso, M. Colangelo, *La regolazione ex ante delle piattaforme digitali,* cit., 431.

quale prevede che il *gatekeeper* non può - per finalità pubblicitarie - trattare i dati personali degli utenti che utilizzano servizi di terzi i quali si avvalgono della piattaforma di base; non può combinare dati personali provenienti dal servizio della piattaforma con altri dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi del *gatekeeper* o con dati provenienti da altri servizi di terzi; non può utilizzare "in modo incrociato" dati personali provenienti dalla piattaforma in altri servizi forniti parallelamente dallo stesso soggetto; non può far accedere con registrazione gli utenti finali ad altri servizi del *gatekeeper* al fine di combinare i dati personali [35]. Questi divieti sono applicabili a meno che l'utente non presti il consenso a procedere con le combinazioni dei dati come previsto. Nel caso in cui l'utente finale neghi il consenso, il *gatekeeper* è tenuto a offrire un servizio alternativo, meno personalizzato ma equivalente [36].

Un ulteriore divieto, che invece prescinde dal consenso prestato dall'utente, riguarda il fatto che non è possibile imporre agli utenti finali o commerciali l'abbonamento o l'iscrizione ad altro servizio come condizione per l'utilizzo e l'accesso ad altro servizio della stessa piattaforma.

Lo stesso art. 5 prevede una serie di obblighi a carico del *gatekeeper*. A tutela dell'utente commerciale è previsto che si deve consentire a questi di offrire gli stessi prodotti o servizi agli utenti finali attraverso servizi di intermediazione di terzi o con il proprio canale di vendita online a prezzi o condizioni diversi da quelli offerti attraverso la piattaforma del *gatekeeper* [37].

In merito a tale ultimo divieto riguardante il *multi-homing*, si può pe-

---

[35] Per questi divieti il legislatore si rifà al caso sottoposto all'Autorità tedesca sulla concorrenza del 2019 e giunto alla nota sentenza della CGUE del 4 luglio 2023, cit., cfr. M. COLANGELO, *La regolazione ex ante delle piattaforme digitali,* cit*.,* 424.

[36] G. AFFERNI, *Digital Services Act e Digital Markets Act,* cit., 318.

[37] Ad ispirare questa prescrizione sarebbero stati i numerosi procedimenti in tema di *most favoured nation clauses* (MFN) nei contratti tra hotel e le agenzie di viaggi online come booking ed Expedia (AGCM, proc. N. 1779, decisione 21 aprile 2015; Commissione europea, caso COMP/AT. 40153, sugli e-books nei confronti di

rò notare un contrasto con la differente disciplina prevista all'art. 10, par. 1, P2B, secondo il quale «qualora, nell'ambito della fornitura dei loro servizi, i fornitori di servizi di intermediazione online limitino la capacità degli utenti commerciali di offrire gli stessi beni e servizi ai consumatori a condizioni diverse tramite mezzi che non siano i suddetti servizi, essi includono nei loro termini e nelle loro condizioni le ragioni di tale limitazione e le rendono facilmente accessibili al pubblico. Tra tali ragioni figurano le principali considerazioni di ordine economico, commerciale o giuridico». Quindi, il P2B ammette, se adeguatamente motivato, un divieto contrattuale di avvalersi di piattaforme concorrenti.

L'art. 5 DMA prosegue prescrivendo che il *gatekeeper* deve consentire agli utenti commerciali di comunicare e promuovere offerte agli utenti finali acquisiti attraverso il proprio servizio di piattaforma di base o attraverso altri canali e di stipulare contratti con tali utenti, a prescindere dal fatto che essi si avvalgano della piattaforma del *gatekeeper*; deve consentire agli utenti finali di accedere a contenuti, abbonamenti, componenti o altri elementi e di utilizzarli attraverso i suoi servizi della piattaforma avvalendosi dell'applicazione *software* di un utente commerciale, anche se gli utenti finali hanno acquistato tali elementi dall'utente commerciale senza utilizzare i servizi della piattaforma del *gatekeeper*[38]. In quest'ultimo caso si tratta del *multi-homing* da parte degli utenti finali che consente loro di utilizzare su qualsiasi piattaforma un prodotto o servizio acquistato attraverso qualunque altro canale; quindi, anche per il tramite di altra piattaforma di base o direttamente da un utente commerciale della piattaforma[39].

Amazon). In tal senso, M. Colangelo, *La regolazione ex ante delle piattaforme digitali,* cit., 424.

[38] Per quest'ultima prescrizione la fattispecie ispiratrice potrebbe essere il caso Apple Store / Comm. Eu., AT.40437.

[39] G. Afferni, *Gli obblighi dei gatekeeper,* cit., 324. Secondo il considerando n. 41 DMA, «non dovrebbe risultare pregiudicata o limitata la capacità degli utenti finali di acquistare contenuti, abbonamenti, componenti o altri elementi al di fuori dei servizi di piattaforma di base del gatekeeper. È in particolare opportuno evitare una situazione in cui i gatekeeper limitino l'accesso a tali servizi e il loro uso da parte degli

Il *gatekeeper* è poi tenuto a fornire, a ogni inserzionista cui eroga servizi pubblicitari, se richiesto, informazioni, su base giornaliera e a titolo gratuito, relative a ogni annuncio pubblicato dall'inserzionista e in particolare:

a) il prezzo e le commissioni pagati dall'inserzionista; b) la remunerazione percepita dall'editore; c) i parametri di calcolo di ogni prezzo, commissione e remunerazione.

Il *gatekeeper* deve fornire, a ogni editore cui eroga servizi pubblicitari, se richiesto, informazioni, su base giornaliera e a titolo gratuito, relative a ogni annuncio pubblicitario che appare pubblicato nello spazio dell'editore e in particolare:

a) la remunerazione e commissioni percepite dall'editore; b) prezzo pagato dall'inserzionista; c) il parametro di calcolo di ogni prezzo e remunerazione.

Anche all'art. 6 DMA sono previsti una serie di divieti gravanti sul *gatekeeper*. In sintesi, quest'ultimo non può utilizzare, in concorrenza con altri utenti commerciali, dati non accessibili al pubblico generati o forniti da tali utenti commerciali (inclusi quelli generati o forniti dai clienti di questi ultimi) nell'ambito dell'utilizzo dei servizi della piattaforma [40]; non può garantire un trattamento più favorevole - in termini di posizionamento e indicizzazione - ai servizi e prodotti offerti dallo stesso *gatekeeper* rispetto a servizi o prodotti analoghi di terzi (prescrizione chiaramente ispirata al caso *Google Shopping*, T-612/2017) [41]; non può limitare a livello tecnico, o in altro modo, la possi-

---

utenti finali tramite un'applicazione software in esecuzione sul loro servizio di piattaforma di base». Per esempio, «agli abbonati a un contenuto online acquistato al di fuori di un'applicazione software, un negozio di applicazioni software o un assistente virtuale, non dovrebbe essere impedito di accedere a tale contenuto online utilizzando un'applicazione software sul servizio di piattaforma di base del gatekeeper solo perché è stato acquistato al di fuori di tale applicazione software, negozio di applicazioni software o assistente virtuale».

[40] Questo divieto può essere ricondotto al caso *Amazon Marketplace* (Commissione europea Caso AT.40670, 22 giugno 2021).

[41] *Ibidem*.

bilità per gli utenti finali di abbonarsi a servizi diversi, cui hanno accesso avvalendosi dei servizi di piattaforma di base del *gatekeeper*.

Lo stesso art. 6 DMA prevede che si deve consentire agli utenti finali di disinstallare qualsiasi applicazione presente nel sistema operativo del *gatekeeper*, al di là di quelle applicazioni essenziali per il funzionamento del servizio o dispositivo [42]; deve consentire agli utenti finali di modificare facilmente le impostazioni predefinite del sistema operativo che indirizzano od orientano gli utenti finali verso prodotti o servizi forniti dal *gatekeeper*. È inclusa in questa fattispecie la richiesta agli utenti finali, al momento del primo utilizzo, del motore di ricerca o di un *browser web* di scegliere, da un elenco di principali fornitori, il motore di ricerca online, l'assistente virtuale o il *browser web* verso cui il sistema indirizza oppure orienta in maniera predefinita gli utenti; deve consentire l'installazione e l'uso effettivo di applicazioni *software* con mezzi diversi dai servizi del *gatekeeper*; deve consentire ai fornitori di servizi di *hardware* l'effettiva interoperabilità con le stesse componenti *hardware* e *software* che sono disponibili per i servizi forniti dal *gatekeeper;* deve fornire a inserzionisti ed editori l'accesso ai propri strumenti di misurazione delle prestazioni e i dati a loro necessari affinché possano effettuare una verifica indipendente dell'offerta di spazio pubblicitario [43].

---

[42] Prescrizione ispirata al caso Microsoft Explorer (AT.39530, 6 marzo 2013).

[43] In tema di interoperabilità di una piattaforma digitale rispetto all'infrastruttura sviluppata da una impresa in posizione dominante, una recente pronuncia della Corte di Giustizia ha stabilito che: «l'art. 102 TFUE deve essere interpretato nel senso che il rifiuto, da parte di un'impresa in posizione dominante che ha sviluppato una piattaforma digitale, di garantire, a un'impresa terza che ne ha fatto richiesta, l'interoperabilità di tale piattaforma con un'applicazione sviluppata da detta impresa terza può costituire un abuso di posizione dominante anche qualora detta piattaforma non sia indispensabile per lo sfruttamento commerciale di detta applicazione su un mercato a valle, ma sia idonea a rendere la stessa applicazione più attraente per i consumatori, quando la medesima piattaforma non è stata sviluppata dall'impresa in posizione dominante unicamente ai fini della propria attività». In tal senso, CGUE, C-233/23, 25 febbraio 2025, *Google / Enel X,* eur-lex.europa.eu

Come accennato nei capitoli precedenti, nel DMA è previsto che il *gatekeeper* deve consentire a utenti finali e terzi autorizzati l'effettiva portabilità dei dati. È previsto che l'obbligato deve fornire gli strumenti per favorire l'effettiva portabilità dei dati a titolo gratuito ed è tenuto a fornire un accesso continuo e in tempo reale ai dati in questione [44].

L'art. 6 DMA prosegue prevedendo che il *gatekeeper* deve fornire agli utenti commerciali e terzi autorizzati un accesso efficace, continuo e di qualità ai dati aggregati e non aggregati, inclusi quelli perso-

---

[44] Il considerando n. 59 DMA prevede, inoltre, che i *gatekeeper* «usufruiscono dell'accesso a grandi quantità di dati che raccolgono nel fornire i servizi di piattaforma di base, nonché altri servizi digitali. Al fine di garantire che i gatekeeper non compromettano la contendibilità dei servizi di piattaforma di base, o il potenziale di innovazione del dinamico settore digitale, limitando il passaggio ad altri fornitori o il multihoming, è opportuno assicurare agli utenti finali, nonché a terzi autorizzati da un utente finale, l'accesso effettivo e immediato ai dati da essi forniti o che sono stati generati tramite le loro attività sui pertinenti servizi di piattaforma di base del gatekeeper. I dati dovrebbero essere ricevuti in un formato immediatamente ed effettivamente accessibile e utilizzabile da parte dell'utente finale o dei pertinenti terzi autorizzati dall'utente finale a cui i dati sono trasferiti. È altresì opportuno che i gatekeeper provvedano, per mezzo di misure tecniche adeguate e di elevata qualità, quali per esempio le interfacce di programmazione delle applicazioni (API), a che gli utenti finali o i terzi autorizzati dagli utenti finali possano trasferire liberamente i dati in maniera continua e in tempo reale. Ciò dovrebbe applicarsi del pari a tutti gli altri dati a diversi livelli di aggregazione necessari affinché tale portabilità sia effettivamente consentita. Al fine di evitare dubbi, l'obbligo per il gatekeeper di garantire l'effettiva portabilità dei dati a norma del presente regolamento integra il diritto alla portabilità dei dati a norma del regolamento (UE) 2016/679. Agevolare il passaggio ad altri fornitori o il multihoming dovrebbe a sua volta comportare una maggiore scelta per gli utenti finali e costituire un incentivo all'innovazione per i gatekeeper e gli utenti commerciali». Al considerando n. 96 DMA si legge che l'attuazione di alcuni degli obblighi a carico dei gatekeeper, come per esempio quelli relativi all'accesso ai dati, alla portabilità dei dati o all'interoperabilità, potrebbe essere favorita dalla previsione di norme tecniche. Perciò, viene sollecitata la Commissione europea, ove opportuno e necessario, nel chiedere alle organizzazioni europee di normazione l'elaborazione di tali norme.

nali [45]; deve garantire «alle imprese terze che forniscono motori di ricerca online, su loro richiesta, l'accesso a condizioni eque, ragionevoli e non discriminatorie a dati relativi a posizionamento, ricerca, *clic* e visualizzazione per quanto concerne le ricerche gratuite e a pagamento generate dagli utenti finali sui suoi motori di ricerca online. I dati relativi a ricerca, *clic* e visualizzazione che costituiscono dati personali sono resi anonimi».

Nel caso di fornitura di servizi di comunicazione interpersonale, indipendente dal numero, deve garantire l'interoperabilità con i servizi di comunicazione di un altro fornitore che offre o intende offrire i medesimi servizi nella UE (art. 7 DMA).

6. *I poteri della Commissione europea*

Con il DMA il legislatore ha abbracciato un modello di *enforcement* caratterizzato da un approccio fortemente centralizzato a livello UE, con l'attribuzione di ampi poteri di natura investigativa ed esecutiva in capo alla Commissione europea assimilabili a quelli disponibili in materia di concorrenza [46]. Di contro, il potere in capo alle autorità nazionali risulta essere alquanto marginale [47]. Tali poteri verranno qui descritti per sommi capi.

---

[45] Anche per quanto riguarda l'accesso ai dati generati dagli utenti commerciali il regolamento P2B, all'art. 9, prevede una disciplina differente. Sul punto si veda G. Afferni, *Gli obblighi dei gatekeeper*, 322-323.

[46] M. Colangelo, *La regolazione ex ante delle piattaforme digitali,* cit.,429. L'A. rileva, p. 435, come la Commissione sia l'unica autorità a cui viene conferito il potere di applicare il DMA, stando al considerando n. 91. Una autorità nazionale di concorrenza può svolgere una indagine su un caso previa informativa scritta alla Commissione che, nel caso in cui apra un procedimento ex art. 20, preclude l'azione dell'autorità nazionale.

[47] Sul tema si veda G. Giordano, *Il Digital Markets Act e la centralizzazione dei poteri in capo alla Commissione europea: quale ruolo per le Autorità antitrust nazionali?*, in *Comparazione e diritto civile*, n. 3, 2022, 979.

La Commissione ha il potere di adottare atti di esecuzione diretti a sospendere un obbligo per uno specifico fornitore qualora venga dimostrato che la sua osservanza metterebbe a rischio, per circostanze eccezionali fuori dal suo controllo, la redditività economica della sua attività nell'UE (art. 9 DMA). L'istituzione europea ha anche il potere di adottare atti di esecuzione per esonerare uno specifico fornitore da un obbligo per motivi di salute pubblica o sicurezza pubblica (art. 10 DMA).

Entro sei mesi dalla sua designazione il *gatekeeper* è tenuto a trasmette alla Commissione una relazione, oltre a un documento di sintesi, contenente la descrizione delle misure attuate per garantire l'osservanza degli obblighi previsti dal regolamento (art. 11 DMA).

Entro la stessa data è tenuto a presentare una descrizione, sottoposta ad *audit* indipendente, riguardante le tecniche di profilazione dei consumatori applicate dal *gatekeeper* ai suoi servizi di piattaforma di base (art. 15 DMA) [48]. L'impresa non può adottare misure antielusive, ossia, misure volte a impedire la designazione come *gatekeeper* schivando le soglie quantitative. Non può adottare alcun comportamento che pregiudichi l'effettiva osservanza degli obblighi di cui al DMA (art. 13 DMA). Infine, i *gatekeeper* sono tenuti a istituire una funzione di controllo della conformità indipendente dalle sue funzioni operative e composta da uno o più responsabili della conformità (art. 28 DMA).

Da un punto di vista sanzionatorio, l'art. 18 DMA prevede il potere della Commissione di attivare un'indagine di mercato su un'inosservanza sistematica. Si tratta di una disposizione criticata per l'indeterminatezza e il carattere potenzialmente illimitato della sanzione la

[48] In merito a tale adempimento, la Commissione europea, il 31 luglio 2023, ha adottato un modello per la segnalazione delle tecniche di profilazione dei consumatori utilizzate dalle piattaforme ai sensi dell'art. 15 DMA. Il modello, titolato "*Template relating to the audited description of consumer profiling techniques pursuant to article 15 of Regulation (EU) 2022/1925 (Digital Markets Act)*", specifica le informazioni minime che la Commissione si attende che i *gatekeeper* forniscano per favorire la trasparenza e la responsabilità delle loro tecniche di profilazione. Il documento è consultabile al sito digital-markets-act.ec.europa.eu

cui incertezza rischia di sfavorire l'innovazione danneggiando il mercato [49].

7. *I primi casi applicativi del DMA*

Si possono già segnalare e riportare i primi casi pratici di applicazione del *Digital Markets Act*.

Un primo caso meritevole di essere annoverato ha riguardato Meta, la quale nel luglio 2024 è stata informata dalla Commissione UE circa le risultanze preliminari riguardanti il modello *pay or consent* recentemente adottato che, secondo la Commissione UE, non sarebbe conforme al *Digital Markets Act* [50]. Infatti, secondo la Commissione si tratta di una scelta che costringe gli utenti a prestare il consenso alla combinazione dei loro dati personali e non riesce a fornire loro una versione meno personalizzata ma equivalente del *social network*. Dunque, non consentirebbe all'utente una vera e propria libera scelta come richiesto nel nuovo regolamento sui mercati digitali.

Riportando il contenuto dell'art. 5, par. 2, DMA, la Commissione rileva che, se un utente rifiuta di prestare il consenso, dovrebbe avere accesso a un'alternativa meno personalizzata ma equivalente. Viene sottolineato che il modello adottato da Meta non consente agli utenti di optare per un servizio che non utilizza i loro dati personali ed è equivalente al servizio basato su "annunci personalizzati".

Un'altra indagine riguarda invece Apple [51]. Infatti, La Commissione europea ha informato Apple del suo parere preliminare secondo cui la politica aziendale seguita nell'App Store violerebbe la normativa del

---

[49] A. Iannotti della Valle, *Il Digital Markets Act e il ruolo dell'unione europea verso un costituzionalismo digitale*, cit., 1877.

[50] *Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act*, consultabile al sito www.ec.europa.eu

[51] *Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple under the Digital Markets Act*, consultabile al sito ec.europa.eu

DMA poiché impedisce agli sviluppatori di app di indirizzare liberamente i consumatori verso canali alternativi per offerte e contenuti. Inoltre, sostiene la non conformità dei suoi nuovi requisiti contrattuali per gli sviluppatori di app e gli *app-store* di terze parti, tra cui la nuova *Core Technology Fee*, in quanto non sufficiente a garantire un effettivo rispetto degli obblighi prescritti nel DMA. Viene sottolineato che, ai sensi del DMA, gli sviluppatori che distribuiscono le loro app tramite lo *store* di Apple dovrebbero, gratuitamente, poter informare i clienti di altre possibilità di acquisto più economiche e indirizzarli verso tali offerte consentendo loro di effettuare acquisti [52]. La Commissione ha avviato un procedimento volto ad accertare la presunta violazione dell'art. 6, par. 4, DMA in merito agli obblighi che vengono imposti agli sviluppatori di app. In particolare, il nucleo dell'indagine si incentra su: la *Core Technology Fee* di Apple [53]; il percorso in più passaggi degli utenti di Apple per scaricare e installare app o app store alternativi su iPhone [54]; i requisiti di ammissibilità per gli sviluppatori nell'offerta

[52] La Commissione rileva, tra le criticità, ad esempio, che gli sviluppatori non possono fornire informazioni sui prezzi all'interno dell'app o comunicare in altro modo con i propri clienti per promuovere offerte disponibili su canali di distribuzione alternativi. Un'altra criticità attiene al sistema del *link-out;* vale a dire, in base alla maggior parte delle condizioni a cui sono sottoposti gli sviluppatori di app, Apple consente di indirizzare i clienti solo attraverso i "link-out", ossia gli sviluppatori possono includere nella loro app un apposito *link* che serve per reindirizzare i clienti verso una pagina web in cui possono stipulare un contratto. Questo sistema sarebbe soggetto a diverse restrizioni imposte da Apple che impedirebbero agli sviluppatori di app di comunicare, promuovere offerte e stipulare contratti attraverso il canale di distribuzione di loro scelta.

[53] Si tratta di una commissione di 0,50 € che gli sviluppatori terzi di app e di app store devono pagare per ogni app installata. La Commissione valuterà se Apple abbia dimostrato che la struttura tariffaria imposta, nell'ambito delle nuove condizioni commerciali e in particolare della *Core Technology Fee*, e sia effettivamente conforme al regolamento sui mercati digitali.

[54] La Commissione valuterà se i passaggi che un utente deve intraprendere per completare con successo il download e l'installazione di app o app store alternativi,

di *app store* alternative o nella diretta distribuzione di app dal web su iPhone [55].

Un altro caso significativo, riguardante però la designazione di *gatekeeper,* riguarda il social network X (già Twitter), il quale, nonostante raggiunga le soglie prescritte dal *Digital Markets Act*, non è stato designato dalla Commissione UE. La decisione fa seguito a un'indagine approfondita di mercato avviata nel mese di maggio 2024 a seguito della notifica da parte di X del suo *status* di potenziale *gatekeeper*. La società ha altresì presentato argomentazioni volte a escludere la sua qualifica di punto di accesso importante tra imprese e consumatori.

Previa consultazione del comitato consultivo per i mercati digitali, la Commissione ha concluso, quindi, che la piattaforma non si qualifica effettivamente come *gatekeeper* per il servizio di *social network*, considerato che l'indagine ha rivelato che non costituisce un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali.

8. *Il Digital Services Act (DSA - Reg. UE 2022/2065)*

Il 16 novembre 2022 ha segnato l'entrata in vigore del Regolamento europeo sui servizi digitali (Reg. UE 2022/2065), meglio conosciuto come *Digital Services Act* (DSA). La sua piena applicazione si è avuta a partire dal 17 febbraio 2024 e si va ad inserire nell'articolato piano regolatorio europeo del settore digitale [56].

Con questo intervento normativo è stato in parte modificato l'ap-

---

nonché le varie schermate di informazioni che Apple mostra all'utente, siano conformi al regolamento sui mercati digitali.

[55] La Commissione valuterà se i requisiti che gli sviluppatori di app devono soddisfare per poter beneficiare della distribuzione alternativa prevista dal regolamento sui mercati digitali, come l'essere in regola in qualità di membri dell'*Apple Developer Program*, siano conformi al regolamento.

[56] Sul puzzle di normative nel settore digitale che si vanno a intersecare con il DSA si veda A. Michinelli, *L'interazione del DSA con altre regole sui servizi digitali*, in *Digital Services Act e Digital Markets Act,* cit., 29 e ss.

proccio seguito con la direttiva 2000/31/CE dedicata al commercio elettronico e recepita in Italia con il d.lgs. n. 70 del 2003 [57].

Il DSA nasce da alcune esigenze del web, il quale ha prodotto una disintermediazione digitale provocando la marginalità di operatori professionali nel settore dell'informazione con un'amplificazione di informazioni su piattaforme digitali, *social network* e blog [58]. Questo scenario, secondo alcuni, favorirebbe la propagazione delle cc.dd. *fake news* e renderebbe arduo orientarsi a causa della difficoltà di individuare fonti affidabili [59].

Lo scopo del legislatore europeo, quindi, è quello di stabilire un primo gruppo di regole che definiscono il perimetro delle esenzioni da responsabilità dei prestatori di servizi intermediari e, un secondo gruppo, volto a stabilire obblighi in capo a questi ultimi. L'ultima parte, invece, è dedicata alle norme sull'attuazione, cooperazione, sanzioni ed esecuzione del regolamento. Le norme volte a individuare gli obblighi a carico dei fornitori mutano l'impianto normativo di riferimento della direttiva sul commercio elettronico [60]. Infatti, il modello di responsabilità dei fornitori di servizi digitali muta rispetto alla direttiva 2000/31/CE poiché in quest'ultima venivano collocati in una posizione privilegiata, con una responsabilità limitata (regime del *safe harbour*), mentre con il DSA è l'utente a costituire il fulcro della tutela [61].

---

[57] Su questo tema si veda G. FINOCCHIARO, *Responsabilità delle piattaforme e tutela dei consumatori*, in *Giornale di diritto amministrativo*, n. 6, 2023, 730; G. MONGA, *Responsabilità degli intermediari. Il Digital Services Act*, in M. MAGGIORE (a cura di), *Il commercio elettronico*, Torino, Giappichelli, 2024, 194-201.

[58] B. GRAZZINI, *Piattaforme e content moderation - Fake news e disinformazione*, in *Giurisprudenza italiana*, n. 2, 2024, 491, spec. 493.

[59] *Ibid*. Sul tema della disinformazione e sulla diffusione di notizie tra utenti si veda anche M. DEL VICARIO, A. BESSI, F. ZOLLO, W. QUATTROCIOCCHI, *The spreading of misinformation online*, in PNAS, vol. 13, 3, 2016, 554-559.

[60] G. FINOCCHIARO, *Responsabilità delle piattaforme e tutela dei consumatori,* cit., 733.

[61] *Ivi*, 733-734, secondo L'A. «il consumatore, sul web, non è solo un fruitore dei servizi digitali, ma è un *prosumer*, ossia un consumatore e un produttore che, fruendo dei servizi digitali, contribuisce alla produzione di tali servizi. I motori di ricerca, il commercio elettronico, i blog e i social network basano il proprio funzionamento

I protagonisti del regolamento, pertanto, sono i prestatori di determinati servizi della società dell'informazione così come definiti dalla direttiva (UE) 2015/1535; si tratta di coloro i quali prestano qualsiasi servizio, normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario [62]. Il riferimento normativo all'elemento del «normalmente dietro retribuzione» può essere considerato uno degli elementi che pone l'esigenza di comporre, in modo univoco e definitivo, la questione sulla fallace gratuità di alcuni servizi di operatori digitali. Se tali servizi venissero considerati come servizi "gratuiti", si potrebbero avere problematiche di applicazione soggettiva anche del DSA là dove richiede - tramite un rinvio alla direttiva (UE) 2015/1535 - un servizio reso «normalmente dietro retribuzione».

Ciò premesso, il regolamento riguarda gli operatori del mercato di-

---

anche sulla collaborazione dell'utente-consumatore, che, mentre naviga e vive la sua onlife, contribuisce a determinare il prezzo delle inserzioni pubblicitarie o a costruire la reputazione di un venditore o di un prodotto». Un ulteriore elemento di complessità sarebbe costituito dal fatto che esiste un noto «livello di asimmetria tecnologica e informativa tra gli utenti e gli operatori del web. Non si tratta soltanto di un disequilibrio di natura economica, ma soprattutto di un disequilibrio causato da una disparità di conoscenze tecniche e di informazione. Tale asimmetria può influire sulla corretta formazione della volontà, anche contrattuale, dell'utente. Considerato che, al momento della conclusione di un contratto on line, generalmente esiste una notevole differenza fra le conoscenze delle parti contraenti, tale *information gap* può generare erronee aspettative o un illegittimo affidamento nei confronti del fornitore del servizio fino al limite a giungere a viziare il momento di formazione della volontà». Peraltro, il 22 giugno 2023, la Commissione europea ha adottato il regolamento di esecuzione (UE) 2023/1201 sulle modalità di dettaglio di attuazione di determinate procedure del DSA.

[62] Il riferimento normativo all'elemento del «normalmente dietro retribuzione» può essere considerato uno degli elementi che pone l'esigenza di comporre in modo univoco e definitivo la questione attinente alla fallace gratuità di alcuni servizi di operatori digitali. Se tali servizi venissero considerati come servizi "gratuiti", si potrebbero avere problematiche di applicazione soggettiva anche del DSA là dove richiede – tramite un rinvio alla direttiva (UE) 2015/1535 – un servizio reso «normalmente dietro retribuzione».

gitale che vanno dai *social network* alle piattaforme *e-commerce* sino ai motori di ricerca. Anche in questo caso, gran parte della disciplina consiste in un recepimento della giurisprudenza della Corte di Giustizia europea formatasi negli anni. Tra le novità, si può notare l'introduzione di regole riguardanti i discussi «sistemi di raccomandazione», strumenti tecnologici di cui si avvalgono molti operatori [63].

9. *Scopo e applicazione del Digital Services Act*

Lo scopo principale del DSA riposa sulla creazione di un ambiente online sicuro, prevedibile e affidabile. L'intento è anche quello di rendere più trasparenti alcuni strumenti già oggi ampiamente utilizzati come i già citati sistemi di raccomandazione e altri sistemi algoritmici automatizzati. L'idea è quella di rendere più efficace il sistema di rimozione di contenuti illegali o contrari alle condizioni generali di contratto del fornitore, benché il tema possa aprire la spinosa questione della censura e la discutibile creazione della figura dei c.d. segnalatori attendibili [64].

---

[63] Il sistema di raccomandazione viene definito come un sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per: (i) suggerire informazioni specifiche ai destinatari del servizio; oppure (ii) per mettere in ordine di priorità dette informazioni anche quale risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine o l'importanza delle informazioni visualizzate. Non viene fatto alcun riferimento ad una personalizzazione delle raccomandazioni o delle priorità delle informazioni. A differenza di quanto avviene nell'AI act in cui si delinea una disciplina riguardante i sistemi IA sotto un profilo oggettivo, nel DSA la disciplina sembra concentrarsi sull'uso dei sistemi di raccomandazione che, talvolta, possono coincidere con i sistemi IA. Per questo profilo sia consentito il rinvio a G. PROIETTI, *Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un quadro sistematico*, in *Contratto e Impresa*, n. 3, 2024, 880.

[64] Sulle condizioni generali di contratto anche alla luce del DSA, nonché della direttiva UE 770/2019 e della direttiva UE 2161/2019, cfr. E. PODDIGHE, V. ZENO-ZENCOVICH, *La «correttezza» nelle condizioni generali di contratto delle grandi piattaforme online*, cit., 1 ss.

Un elemento centrale riguarda, perciò, il concetto di «contenuto illegale» che, stando al DSA, deve rispecchiare quello corrispondente all'applicazione delle norme nell'ambiente offline. Questo concetto è definito in senso lato, in modo da coprire anche le informazioni riguardanti i contenuti, i prodotti, i servizi e le attività illegali. Con «contenuto illegale» ci si riferisce alle informazioni, indipendentemente dalla loro forma, che sono da considerarsi tali ai sensi del diritto applicabile, come l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori, o che «le norme applicabili rendono illegali in considerazione del fatto che riguardano attività illegali»[65]. Tra queste figurano, a titolo esemplificativo, «la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il *cyberstalking* (pedinamento informatico), la vendita di prodotti non conformi o contraffatti, la vendita di prodotti o la prestazione di servizi in violazione della normativa sulla tutela dei consumatori, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore, l'offerta illegale di servizi ricettivi o la vendita illegale di animali vivi. Per contro, un video di un testimone oculare di un potenziale reato non dovrebbe essere considerato un contenuto illegale per il solo motivo di mostrare un atto illecito quando la registrazione o la diffusione di tale video al pubblico non è illegale ai sensi del diritto nazionale o dell'Unione»[66].

---

[65] In tal senso il considerando n. 12 del DSA. Sul tema riguardante i «contenuti illegali» ci si chiede «quando le *fake news* costituiscono espressione di libertà di manifestazione del pensiero esercitata in modo non conforme all'ordinamento (ma, ancor prima, cosa debba intendersi per fake news) ed in quali (non sempre sovrapponibili) casi esse possono venire inibite senza che si entri in frizione con le regole ed i principi fondamentali, di livello costituzionale». In questo senso, B. Grazzini, *Piattaforme e content moderation,* cit., 496. Sulla definizione di contenuto illegale ai sensi del DSA si veda anche G. Monga, *Responsabilità degli intermediari. Il Digital Services Act,* cit., 194, il quale sottolinea il carattere generale e onnicomprensivo della nozione che include ogni violazione di legge o del diritto europeo, «a prescindere da quale sia il diritto o la norma di legge concretamente violata».

[66] In tal senso sempre il considerando n. 12 del DSA.

I prestatori di servizi intermediari, secondo il DSA, hanno la facoltà di svolgere indagini proprie per scovare i contenuti illegali, ma non sono tenuti a sorvegliare le informazioni e i contenuti che trasmettono o memorizzano, né sono tenuti ad accertare i fatti o le circostanze che inducono a ritenere sussistente la presenza di attività illegali.

L'ulteriore profilo riguarderebbe il delicato bilanciamento degli interessi in gioco che il fornitore sarebbe chiamato ad effettuare. Dall'analisi del regolamento emerge che il fornitore può procedere con l'adozione diretta di una misura restrittiva senza che vi sia un provvedimento di un'autorità alla base [67]. Su questo aspetto, quindi, la soluzione sembrerebbe ispirata a quanto già offerto dalla giurisprudenza della Corte di Giustizia europea [68]. Il DSA non prevede una disciplina fo-

[67] In questo senso interpretativo sembra implicitamente deporre anche il considerando n. 54 DSA in cui viene specificato che se un prestatore di servizi di memorizzazione di informazioni decide di rimuovere le informazioni fornite da un destinatario del servizio o di disabilitare l'accesso alle stesse o di limitarne in altro modo la visibilità o la monetizzazione perché costituiscono contenuti illegali o sono incompatibili con le condizioni generali (ad esempio a seguito del ricevimento di una segnalazione o agendo di propria iniziativa), dovrebbe informare in modo chiaro e facilmente comprensibile il destinatario della sua decisione dei motivi della stessa e dei mezzi di ricorso disponibili per contestare la decisione, tenuto conto delle conseguenze negative che tali decisioni possono comportare per il destinatario, anche per quanto concerne l'esercizio del suo diritto fondamentale alla libertà di espressione. Se la decisione venisse adottata a seguito del ricevimento di una segnalazione, il prestatore di servizi di memorizzazione di informazioni dovrebbe rivelare l'identità della persona o dell'entità che ha presentato la segnalazione al destinatario del servizio solo se tale informazione è necessaria per identificare l'illegalità del contenuto, ad esempio in caso di violazione dei diritti di proprietà intellettuale.

[68] Da ultimo, sempre in questo senso, anche la più recente CGUE, Grande Sezione, C-460/208, dicembre 2022, *Google*, curia.europa.eu, secondo la quale il motore di ricerca può dar seguito alla richiesta di deindicizzazione se il richiedente riesce a fornire un *fumus* di prova della manifesta inesattezza delle notizie indicizzate senza necessità di una precedente pronunzia del giudice. Sul tema della responsabilità del gestore del motore di ricerca bisogna ovviamente far riferimento anche alla nota sentenza *Google Spain* della Corte di giustizia europea del 13 maggio 2014, C-131/12, eur-lex.europa.eu. In particolare, sul diritto alla deindicizzazione nell'ordinamen-

calizzata sulla individuazione di ciò che online costituirebbe un contenuto illegale, benché tenti di delinearlo indirettamente; il fulcro del sistema si concentra sulle politiche aziendali dei prestatori e sulle condizioni contrattuali da loro predisposte.

Per rendere più efficace l'applicazione del DSA, tra l'altro, è stato istituito il Centro europeo per la trasparenza algoritmica (ECAT) chiamato a vigilare sull'utilizzo dei sistemi algoritmici. L'ECAT è tenuto a coadiuvare la Commissione europea per garantire che i sistemi algoritmici utilizzati dalle piattaforme e dai motori di ricerca di grandi dimensioni rispettino i requisiti in tema di gestione e di attenuazione dei rischi. L'attuazione del DSA e il suo collegamento con le copiose e articolate normative ad esso complementari giocherà un ruolo cruciale che determinerà il risultato finale della sfida che il legislatore europeo intende affrontare.

10. *Il quadro di esenzione da responsabilità dei prestatori di servizi intermediari*

Il primo gruppo di norme del DSA riguarda le esenzioni. Si tratta di quelle regole che determinano le condizioni affinché un prestatore possa essere esentato da responsabilità a fronte di contenuti online illegali. Tali regole vengono suddivise sulla base del servizio prestato e non del soggetto che lo presta [69].

I servizi, infatti, vengono suddivisi nel:

---

to nazionale secondo la più recente giurisprudenza di legittimità si veda S. M. Lener, *Diritto alla deindicizzazione - La domanda di deindicizzazione e le interferenze tra la Dir. 2000/31 e il Reg. 2016/679*, in *Giurisprudenza italiana*, n. 3, 2022, 587 ss.

[69] Sul quadro di esenzione in dottrina si veda M. A. Astone, *Digital services act e nuovo quadro di esenzione dalla responsabilità dei prestatori di servizi intermediari: quali prospettive?,* in *Contratto e impresa*, vol. 33, n. 4, 2022, 1050, spec. 1060. L'A. segnala come l'obiettivo del DSA sarebbe quello di «intervenire più che sulle fattispecie o sui criteri di imputazione della responsabilità e sulla presunzione di colpa – quasi invariati rispetto alla disciplina contenuta nella direttiva 2000/31/CE – sulle modalità di esenzione dalla stessa, in un'ottica che resta sempre quella della composizione degli interessi in gioco per evitare sbilanciamenti di tutela».

(i) *semplice trasporto*, ove si ricomprendono i punti di interscambio internet, i punti di accesso senza fili, le reti private virtuali, i risolutori e i servizi di DNS, i registri dei nomi di dominio di primo livello, i *registrar*, le autorità di certificazione che rilasciano certificati digitali, il *Voice over IP* e altri servizi di comunicazione interpersonale;

(ii) *memorizzazione temporanea*, che includono la sola fornitura di reti per la diffusione di contenuti, *proxy* inversi o *proxy* di adattamento dei contenuti [70].

(iii) *memorizzazione di informazioni*, che includono categorie come la c.d. nuvola informatica, la memorizzazione di informazioni di siti web, i servizi di referenziazione a pagamento o i servizi che consentono la condivisione di informazioni e contenuti online, compresa la condivisione e la memorizzazione di *file*.

I servizi intermediari possono essere prestati isolatamente, nel quadro di un altro tipo di servizio intermediario o simultaneamente ad altri servizi intermediari. Il discernimento tra un servizio e l'altro dipende esclusivamente dalle funzionalità tecniche del servizio; esse devono essere valutate caso per caso perché suscettibili di mutare nel tempo.

Nel caso di prestazione di un servizio di semplice trasporto è previsto che il prestatore non sia responsabile delle informazioni trasmesse o a cui si è avuto accesso se (i) non ha dato origine alla trasmissione; (ii) non seleziona il destinatario della trasmissione; (iii) non seleziona né modifica le informazioni trasmesse. Quest'ultima condizione non include quelle manipolazioni di carattere tecnico effettuate nel corso della trasmissione o dell'accesso, purché non alterino l'integrità delle informazioni trasmesse o alle quali è fornito l'accesso.

Nel caso di prestazione di un servizio di memorizzazione temporanea il prestatore non è responsabile (se questa viene effettuata per facilitare l'inoltro delle informazioni ad altri destinatari del servizio

[70] Sono quei servizi fondamentali che garantiscono una trasmissione fluida ed efficiente delle informazioni fornite su internet.

su loro richiesta) se (i) non modifica le informazioni; (ii) si conforma alle condizioni di accesso alle informazioni; (iii) si conforma alle norme sull'aggiornamento delle informazioni riconosciute dalle imprese del settore; (iv) non interferisce con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; (v) agisce prontamente per rimuovere le informazioni memorizzate o per disabilitare l'accesso a queste quando viene a conoscenza della loro rimozione dalla rete o che l'accesso è stato disabilitato o che un'autorità ne abbia ordinato la disabilitazione o rimozione.

Nel caso di prestazione di un servizio di memorizzazione di informazioni il prestatore non è responsabile delle informazioni memorizzate su richiesta del destinatario se (i) non è effettivamente a conoscenza delle attività e dei contenuti illegali; (ii) quando ne viene a conoscenza agisca immediatamente per la rimozione degli stessi o per disabilitare l'accesso. Questa regola non trova però applicazione se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

L'esenzione non si applica neppure per quelle piattaforme che consentono ai consumatori di concludere contratti a distanza con operatori commerciali se pubblicano informazioni che fanno ritenere che le informazioni o il prodotto siano forniti dalla stessa piattaforma [71].

In generale, i prestatori hanno la facoltà di svolgere indagini volontarie ma non sono tenuti a sorvegliare le informazioni e i contenuti che trasmettono o memorizzano, né sono tenuti ad accertare fatti o circostanze che indichino la presenza di attività illegali (art. 8 DSA). Inoltre, con una formulazione piuttosto contorta, è previsto che non vengono meno le esenzioni ivi stabilite se i prestatori realizzano indagini volontarie finalizzate a individuare e rimuovere contenuti illegali (art. 7 DSA). Si tratta con tutta evidenza di una regola volta a

[71] Il caso è quello della piattaforma online che non mostra chiaramente l'identità dell'operatore commerciale.

favorire e incentivare le "indagini volontarie" e l'adozione di "misure necessarie" [72].

Queste due disposizioni aprono un tema già conosciuto nelle Corti europee, ossia quello riguardante la responsabilità dell'*Internet Service Provider* [73].

La giurisprudenza europea si è espressa sul tema proponendo la nota distinzione tra fornitore *neutro*, il quale pone in essere una attività puramente di carattere passivo e tecnico [74] e il fornitore *attivo* che, viceversa, può ritenersi responsabile [75].

Sull'argomento si è espressa anche la giurisprudenza nazionale di merito con un approccio in parte differente in quanto si è arrivati a recenti pronunce in cui, nonostante il fornitore fosse considerato come un *host provider* passivo, è stato ritenuto responsabile per i contenuti pubblicati da terzi [76]. Tuttavia, rispetto ai primi anni duemila, ossia

---

[72] La disposizione dell'art. 7, lessicalmente formulata in modo quasi incomprensibile, prescrive testualmente che: «i prestatori di servizi intermediari non sono considerati inammissibili all'esenzione dalla responsabilità prevista agli articoli 4, 5 e 6 per il solo fatto di svolgere, in buona fede e in modo diligente, indagini volontarie di propria iniziativa o di adottare altre misure volte a individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione e del diritto nazionale conforme al diritto dell'Unione, comprese le prescrizioni stabilite nel presente regolamento».

[73] M. BASSINI, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità "complessa"?*, in *federalismi.it*, n. 3, 2015, 1, spec. 11.

[74] Sul tema può essere menzionata la pronuncia della CGUE, C-236/08, C-238/08, *Google France SARL*, in *Foro Italiano*, n. 4, 2010, 458.

[75] Con la sentenza CGUE, C-324/09, 12 luglio 2011, *eBay c. L'Oréal*, in *Diritto e giustizia*, 2011, il fornitore è stato ritenuto attivo poiché gestiva un mercato online in quanto aveva consentito ai propri utenti di vendere i prodotti contraffatti oppure privi dei requisiti di legge necessari per la vendita.

[76] A titolo esemplificativo, il Tribunale di Roma ha condannato Facebook (oggi, Meta) statuendo che: «Sebbene l'hosting provider c.d. "passivo" non possa essere soggetto ad un obbligo generale di sorveglianza, va affermata la responsabilità della società che gestisce un social network ove venga messa a conoscenza, da parte del

a seguito dell'emanazione della normativa sul commercio elettronico, si è andata via via sfocando quella figura dell'*hosting provider* neutro (o passivo), che faceva leva sull'art. 14 della direttiva *e-commerce*[77].

11. *Gli obblighi per i prestatori di servizi intermediari nel DSA*

Il capo dedicato agli obblighi per i prestatori suddivide le norme a seconda degli operatori coinvolti. Quindi, vengono prescritti:

(i) obblighi applicabili a tutti i prestatori (artt. 11-15 DSA);

(ii) obblighi applicabili ai prestatori di servizi di memorizzazione di informazioni (artt. 16-18 DSA);

---

titolare dei diritti lesi, del contenuto illecito dei contenuti pubblicati dagli utenti su un profilo telematico ove non si sia attivata per rimuoverli o impedire l'accesso agli stessi». In tal senso, Trib. Roma, Sez. spec. in materia di imprese, 15 febbraio 2019, n. 3512, nota di B. Tassone, in *Rivista di diritto industriale*, n. 4, 2019, 372. Lo stesso Trib. Roma si era pronunciato nel senso che «ai fini dell'affermazione della responsabilità dell'*hosting provider* "attivo" occorre in ogni caso dimostrare che questi fosse a conoscenza o potesse essere a conoscenza dell'illecito commesso dall'utente mediante l'immissione sul portale del materiale audiovisivo in violazione dei diritti di sfruttamento economico detenuti dal titolare dei diritti lesi. Ciò in quanto anche all'*hosting provider* "attivo" si applica il divieto, previsto dall'art. 15 della direttiva 31/2000 (e dall'art. 17 del decreto attuativo n. 70/2003), di un obbligo generalizzato di sorveglianza preventiva sul materiale trasmesso o memorizzato e di ricerca attiva di fatti o circostanze che indichino la presenza di attività illecite da parte degli utenti del servizio. Correlativamente, neppure può escludersi una responsabilità dell'*hosting provider* "passivo" ogniqualvolta sia stato messo a conoscenza, da parte del titolare dei diritti lesi, del contenuto illecito delle trasmissioni e ciononostante non si sia attivato prontamente per rimuovere le stesse e abbia proseguito, invece, nel fornire agli utenti gli strumenti per la prosecuzione della condotta illecita». In quest'ultimo senso, Trib. Roma, Sez. spec. in materia di imprese, 10 gennaio 2019, n. 693, nota di M. Iaselli, *Rivista di diritto industriale*, n. 4, 2019, 387. Per la giurisprudenza di legittimità si veda invece Cass. civ., sez. I, 19 marzo 2019, n. 7708, in *Quotidiano giuridico*, 2019; Cass. civ., sez. I, 19 marzo 2019, n. 7709, in *Foro Italiano*, n. 1, 2019, 2045.

[77] Sul tema, O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* in *Percorsi Costituzionali*, n. 1, 2014, 46 ss.

(iii) obblighi (e poteri) per i fornitori di piattaforme online (artt. 19-28 DSA);

(iv) obblighi aggiuntivi per i fornitori di piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali (artt. 29-32 DSA);

(v) obblighi supplementari per i fornitori di piattaforme online e di motori di ricerca online di dimensioni molto grandi (artt. 33-43 DSA).

Nei successivi paragrafi verrà sintetizzato il dettato normativo di ciascuna categoria di obblighi.

11.1 *Obblighi applicabili a tutti i prestatori*

Le prime disposizioni previste nella sez. I del capo III, sono applicabili indistintamente a tutti i prestatori. Questi consistono nel dovere di istituire punti di contatto per le Autorità degli Stati membri, Commissione e Comitato (art. 11 DSA) e un punto di contatto per i destinatari del servizio (art. 12 DSA).

Nelle condizioni generali di contratto sono tenuti a specificare (in modo conciso, intellegibile e accessibile) le informazioni riguardanti le restrizioni che impongono sull'uso dei loro servizi, tra cui le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, incluso il processo decisionale algoritmico e la verifica umana, oltre alle regole procedurali del loro sistema interno per la gestione dei reclami. I prestatori devono agire in modo diligente, obiettivo e proporzionato tenendo conto dei diritti e degli interessi di tutte le parti coinvolte, tra cui la libertà di espressione, il pluralismo dei media e altri diritti e libertà sanciti dalla Carta.

I prestatori sono tenuti a pubblicare - con cadenza annuale - relazioni chiare e intellegibili sulle attività di moderazione dei contenuti. Queste relazioni devono incentrarsi su elementi tra cui il numero di ordini ricevuti; numero di segnalazioni presentate; utilizzo di strumenti automatizzati e il numero di reclami ricevuti (art. 15 DSA).

11.2 *Obblighi applicabili ai prestatori di servizi di memorizzazione di informazioni*

Per i prestatori di servizi di memorizzazione viene imposta l'istituzione di un meccanismo per le segnalazioni di contenuti illegali per via elettronica. Le decisioni che devono far seguito alle segnalazioni dovranno essere tempestive, adottate diligentemente e in modo non arbitrario e obiettivo. Se ci si avvale dell'utilizzo di strumenti automatizzati, deve essere inclusa un'adeguata informazione sull'uso (art. 16 DSA).

In caso di adozione di misure restrittive, queste devono essere accompagnate da una adeguata motivazione. Ciò trova una eccezione, però, nel caso in cui le informazioni fossero riferite a contenuti commerciali ingannevoli ad ampia diffusione. Casi concreti potrebbero essere quelli di un utilizzo non autentico del servizio, come l'utilizzo di *bot* o *account* falsi o altri usi ingannevoli.

La motivazione che accompagna la misura restrittiva deve contenere una serie di informazioni, tra cui l'indicazione dell'oggetto, ossia se la decisione comporta la rimozione delle informazioni, la disabilitazione dell'accesso, la limitazione della visibilità o altre misure; deve esporre i fatti e le circostanze su cui si basa, le informazioni sugli strumenti automatizzati utilizzati per la decisione; il riferimento alla base giuridica invocata; i mezzi di ricorso disponibili. Questa disposizione sull'esposizione dei motivi e delle circostanze, tuttavia, non trova applicazione nel caso di adozione di un ordine di rimozione da parte di una Autorità (art. 17 DSA). Nell'ipotesi di sospetto sulla commissione di un reato, il prestatore è tenuto informare, senza indugio, le autorità giudiziarie dello stato membro (art. 18 DSA).

Le tipologie di restrizioni che il prestatore può adottare non sono tipiche e, quindi, non vengono menzionate dal DSA, ma tra queste si possono ipotizzare:

(i) la restrizione della visibilità, che può consistere nella retrocessione nel posizionamento o nei sistemi di raccomandazione, come pure la restrizione dell'accessibilità da parte di uno o più destinatari del servizio o nell'esclusione dell'utente da una comunità online senza che quest'ultimo ne sia consapevole («*shadow banning*»).

(ii) un'altra restrizione ipotizzata riguarda la monetizzazione - grazie agli introiti pubblicitari - delle informazioni fornite dal destinatario del servizio, la quale può essere limitata mediante la sospensione o la soppressione del pagamento in denaro o degli introiti connessi a tali informazioni.

Si tratta, in ogni caso, di misure molto discrezionali. Il potere che viene conferito a tali soggetti privati, i prestatori di servizi, è molto ampio e suscettibile di sfociare in una forma di vera e propria censura. Un analogo potere è previsto per alcuni tipi di piattaforme online.

11.3 *I poteri dei fornitori di piattaforme online e i relativi obblighi*

Le piattaforme online sono una sottocategoria rispetto ai prestatori di servizi di memorizzazione. Con «piattaforme *on-line*» il legislatore intende i *social network* o quelle piattaforme che consentono ai consumatori di concludere contratti a distanza con operatori commerciali (quindi, tutte quelle piattaforme che operano nel *e-commerce*). Esse sono definite come prestatori di servizi di memorizzazione di informazioni che non solo memorizzano informazioni fornite dai destinatari del servizio su richiesta di questi ultimi, ma le diffondono al pubblico su richiesta dei destinatari.

A queste piattaforme si applicano un nutrito numero di obblighi. Questi, però, non si applicano a quei fornitori che si qualificano come microimprese o piccole imprese come definite dalla raccomandazione 2003/361/CE.

Tra gli obblighi in questione è prevista:

a) la predisposizione di un sistema interno per la gestione dei reclami contro una decisione presa dal fornitore all'atto del ricevimento di una segnalazione o contro una serie di decisioni adottate dallo stesso e indicate nel par. 1 dell'art. 20 DSA. Per le decisioni sui reclami non ci si può avvalere esclusivamente di strumenti automatizzati;

b) la previsione della possibilità di risolvere stragiudizialmente le controversie (art. 21 DSA). Di tale possibilità i destinatari del servizio devono essere informati e deve essere accessibile sulla interfaccia on-

line. L'organismo incaricato per la risoluzione delle controversie non può adottare decisioni vincolanti per le parti;

c) la priorità da concedere alla figura del "segnalatore attendibile" [78]. Si tratta di una qualifica riconosciuta, su richiesta di qualunque ente, dal Coordinatore in cui è stabilito il richiedente. Si può trattare di enti pubblici, privati o no profit. È necessario che siano dimostrate: capacità e competenze particolari per l'individuazione, identificazione e notifica di contenuti illegali; indipendenza rispetto a qualsiasi fornitore di piattaforme online; capacità di svolgimento dell'attività in modo diligente, accurato e obiettivo [79]. I segnalatori pubblicano (e trasmettono al coordinatore), almeno una volta ogni anno, una relazione sulle segnalazioni presentate. Alle segnalazioni che pervengono da questi soggetti deve essere data priorità (art. 22 DSA);

d) l'indicazione del numero di controversie sottoposte agli organismi di risoluzione delle controversie, i risultati delle stesse, il tempo medio per il loro espletamento, il numero di sospensioni applicate ai sensi dell'art. 23 DSA [80]. Ogni sei mesi i fornitori pubblicano per ciascuna piattaforma e per ciascun motore di ricerca, informazioni sul numero medio mensile di destinatari attivi del servizio nell'UE (art. 24 DSA);

---

[78] Si tratta di una figura non del tutto sconosciuta, considerato che erano già ammesse nel "Codice di condotta UE" per contrastare l'incitamento all'odio online di giugno 2016 e nella raccomandazione della Commissione 2018/334 sulle misure di contrasto ai contenuti illeciti. Si veda a tal proposito, A. Michinelli, *La gestione dei contenuti: illegali e non, la loro moderazione*, in *Digital Services Act e Digital Markets Act,* cit., 131, spec. 160.

[79] In Italia, il Coordinatore dei servizi digitali è stato designato con il d.l. 123/2023 convertito con modificazioni dalla L. 159/2023, che lo ha affidato all'Autorità per le garanzie nelle comunicazioni (AGCOM). Con la delibera n. 40/2024, l'AGCOM ha avviato una consultazione pubblica per acquisire osservazioni ed elementi d'informazione, da parte dei soggetti interessati, sullo schema di regolamento di procedura per il riconoscimento della qualifica di segnalatore attendibile, nonché sulle modalità operative e le aree di competenza.

[80] Ciò in aggiunta alle informazioni relative alle relazioni sulle attività di moderazione dei contenuti prescritte dall'art. 15 DSA per tutti i prestatori.

e) la progettazione, l'organizzazione e la gestione delle interfacce, in modo che i destinatari dei servizi offerti non vengano ingannati o manipolati o in modo che le loro capacità nell'assumere decisioni libere e informate siano materialmente falsati o compromesse. Il suddetto divieto non trova applicazione per le pratiche contemplate dalla direttiva in materia di pratiche commerciali scorrette (dir. 2005/29/CE) o dal GDPR (art. 25 DSA);

f) nel caso in cui presentino pubblicità sulle proprie interfacce, i fornitori sono tenuti a far sì che i destinatari siano in grado di identificare in modo chiaro, conciso, inequivocabile e in tempo reale: (i) che l'informazione è una pubblicità; (ii) la persona per conto della quale viene presentata; (iii) la persona che finanzia la pubblicità se diversa dalla lettera precedente; (iv) indicazioni su parametri utilizzati per determinare il destinatario a cui viene presentata e alla modalità di modifica di tali parametri.

I fornitori devono mettere a disposizione dei destinatari una funzione che consente di dichiarare se i contenuti che forniscono (gli stessi destinatari) siano o contengano comunicazioni commerciali.

I fornitori non possono presentare pubblicità sulla base della profilazione di cui al GDPR avvalendosi di categorie speciali di dati personali di cui all'art. 9 GDPR (art. 26 DSA);

g) se si avvalgono di sistemi di raccomandazione, sono tenuti a specificare nelle proprie condizioni contrattuali i principali parametri utilizzati nei sistemi, qualunque opzione a disposizione dei destinatari che consente di modificare o influenzare siffatti parametri. Qualora esistano diverse opzioni di parametri, deve essere consentito al destinatario di scegliere l'opzione preferita (art. 27 DSA);

h) nel caso di piattaforme accessibili ai minori, devono essere adottate misure adeguate e proporzionate per garantire l'elevato livello di tutela della vita privata, sicurezza e protezione dei minori. Se si è consapevoli che il destinatario è minore di età, non è consentita la pubblicità basata su profilazione (art. 28 DSA).

Il regolamento, all'art. 23, sebbene li inserisca nell'ambito degli obblighi, prevede alcuni poteri in capo ai fornitori. È sancito che questi, dopo un avviso, possono sospendere i loro servizi - limitato ad un ra-

gionevole periodo di tempo - per alcuni destinatari che forniscono contenuti illegali in modo reiterato. Possono, inoltre, sospendere il servizio dei reclami interni a quei segnalatori che presentano a più riprese reclami o segnalazioni manifestamente infondati. I fornitori devono determinare la loro politica in ordine a tali abusi, anche tramite esempi, nelle loro condizioni generali per l'utilizzo del servizio.

Per le piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali e i loro relativi obblighi, il DSA prevede che i fornitori possono consentire agli operatori commerciali di utilizzare le loro piattaforme solo se questi ultimi trasmettono determinate informazioni come i dati identificativi, l'iscrizione al registro delle imprese o altro registro. Spetta sempre al fornitore verificare con diligenza la veridicità di tali informazioni (art. 30 DSA).

Se il fornitore viene a conoscenza dell'offerta di un prodotto o di un servizio illegale da un operatore, è tenuto a darne immediata informazione (per gli acquisti avvenuti entro i sei mesi antecedenti) ai consumatori che hanno acquistato il prodotto o servizio.

11.4 *Obblighi supplementari per i fornitori di piattaforme online (VLOP) e di motori di ricerca online di dimensioni molto grandi (VLOSE)*

Il DSA prevede precisi obblighi dedicati ai *gatekeeper*, per utilizzare la terminologia fatta propria nel DMA, benché in questo caso i criteri per la loro individuazione sono differenti e si parli di VLOP e VLOSE.

È stato fatto notare come il DSA preveda degli obblighi in modo asimmetrico con l'intento di stimolare la concorrenza dei diversi operatori, prescrivendo adempimenti più rigidi per quelli di grande dimensione [81].

[81] A. Landi, *I fornitori di servizi di intermediazione molto grandi*, in *Digital Services Act e Digital Markets Act,* cit., 63.

La Commissione europea, anche nel DSA, ha il compito di stabilire quelle che sono le piattaforme online o i motori di ricerca di grandi dimensioni. Ciò avviene secondo un parametro quantitativo, ossia quando hanno un numero medio mensile di destinatari attivi del servizio nell'UE pari o superiore a 45 milioni. Tale qualità cessa e la decisione revocata se per un periodo ininterrotto di almeno un anno non si è prodotto il numero medio mensile predetto. L'elenco delle piattaforme e dei motori di ricerca in questione vengono pubblicati nella G.U. UE (art. 33 DSA).

La prima designazione è avvenuta il 25 aprile 2023. Le piattaforme designate sono state diciassette [82], mentre i motori di ricerca solamente due, ossia Google Search e Bing. Il 20 dicembre 2023, la Commissione ha designato altri tre VLOP [83].

Gli obblighi che seguono, quindi, sono aggiuntivi e trovano applicazione solo nei confronti di questi soggetti di grandi dimensioni designati dalla Commissione europea.

In particolare, essi:

a) sono tenuti a redigere ogni anno una relazione per individuare, analizzare e valutare eventuali rischi sistemici derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi sistemi, compresi quelli algoritmici o dall'uso dei loro servizi. I rischi sistemici di cui tenere conto riguardano: la diffusione contenuti illegali; gli eventuali effetti negativi prevedibili per l'esercizio dei diritti fondamentali; gli eventuali effetti negativi prevedibili sul dibattito civico, sui processi elettorali e sulla sicurezza pubblica; qualsiasi effetto negativo prevedibile relativo alla violenza di genere, alla protezione della salute pubblica e dei minori.

Nella valutazione in questione si dovrà tenere conto de: (i) la progettazione dei sistemi di raccomandazione e di qualsiasi altro sistema

---

[82] Si tratta di Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando.

[83] Si tratta di Pornhub, Xvideos e Stripchat.

algoritmico pertinente; (ii) i loro sistemi di moderazione dei contenuti; (iii) le condizioni generali applicabili; (iv) i sistemi di selezione e presentazione di pubblicità; (v) le pratiche del fornitore relative ai dati (art. 34 DSA).

Questi elementi consentono di analizzare in quale modo i rischi vengono influenzati dalla manipolazione intenzionale del servizio prestato, anche mediante l'uso non autentico o lo sfruttamento automatizzato del servizio, nonché l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e delle informazioni incompatibili con le condizioni generali.

Questi rischi possono sorgere, quindi, da un uso non autentico del servizio come la creazione di *account* falsi, l'uso di *bot* o altri usi ingannevoli di un servizio, e da altri comportamenti automatizzati o parzialmente automatizzati che possono condurre alla rapida e ampia diffusione al pubblico di informazioni che costituiscono contenuti illegali o incompatibili con le condizioni generali della piattaforma online o del motore di ricerca.

b) sono tenuti all'adozione di misure di attenuazione dei rischi sistemici (art. 35 DSA). Le misure possono includere l'adeguamento: (i) della progettazione, delle caratteristiche o del funzionamento dei servizi; (ii) delle condizioni generali; (iii) delle procedure di moderazione dei contenuti; (iv) dei sistemi algoritmici, inclusi i sistemi di raccomandazione; (v) dei sistemi di pubblicità e adozione di misure per limitare o adeguare la presentazione della pubblicità associata al servizio prestato; oppure, il rafforzamento dei processi interni, in particolare per il rilevamento dei rischi sistemici; (vi) l'avvio o l'adeguamento della cooperazione con i segnalatori attendibili e l'attuazione delle decisioni degli organismi di risoluzione delle controversie; (vii) l'avvio o l'adeguamento della cooperazione con altri fornitori in merito a codici di condotta e protocolli di crisi; (viii) l'adozione di misure di sensibilizzazione e l'adattamento dell'interfaccia online per fornire maggiori informazioni ai destinatari; (ix) l'adozione di misure mirate per salvaguardare i diritti dei minori; (x) il ricorso a un contrassegno visibile per far sì che un elemento di una informazione (immagine, audio, video generati o manipolati) che assomigli a persone, oggetti, luoghi o altro, e

che a una persona appaia falsamente autentico, sia distinguibile quando è presentato sulle loro interfacce online. Deve essere fornita una funzionalità che consenta ai destinatari del servizio di indicare tale informazione (sono le ipotesi del c.d. *deep fake*).

c) in caso di circostanze eccezionali che possono comportare una grave minaccia per la sicurezza pubblica o la salute pubblica nell'UE o in parti significative della stessa che determinano una "crisi" (art. 36 DSA), la Commissione UE, su raccomandazione del Comitato, può adottare una decisione che impone a uno o più fornitori di intraprendere una o più azioni (proporzionate, necessarie, giustificate e per un periodo non superiore a tre mesi prorogabile una sola volta) tra cui: una valutazione sulla eventuale portata e sul modo in cui il funzionamento e l'uso dei loro servizi contribuiscono alla crisi; l'individuazione e l'applicazione di misure specifiche, efficaci e proporzionate per prevenire, eliminare o limitare il suddetto contributo; una relazione alla Commissione sulle predette valutazioni e sulle misure adottate.

d) sono tenuti, almeno una volta ogni anno, ad essere sottoposti a revisioni indipendenti di propria iniziativa affinché sia valutata la conformità rispetto agli obblighi di cui al capo III, agli obblighi assunti con i codici di condotta e ai protocolli di crisi (art. 37 DSA) [84].

e) in caso di sistemi di raccomandazione, i fornitori devono assicurare almeno una opzione che non preveda la profilazione di cui all'art. 4, par. 4, GDPR.

f) per la pubblicità online, i fornitori sono tenuti a rendere accessibile al pubblico, in una specifica sezione, un registro contenente alcune informazioni tra cui: (i) il contenuto della pubblicità, incluso il nome del prodotto o servizio; (ii) la persona per conto della quale vie-

[84] La Commissione europea ha di recente posto in pubblica consultazione una bozza di regolamento sulle modalità di esecuzione delle revisioni indipendenti previste dall'art. 37 del DSA. Il Regolamento, che verrà adottato entro la fine dell'anno corrente, definisce i principi che i revisori dovrebbero applicare nella scelta delle metodologie e delle procedure di revisione fornendo ulteriori dettagli per la revisione della conformità delle VLOP e VLOSE agli obblighi di gestione del rischio e di risposta alle crisi.

ne presentata e che ha provveduto al pagamento, se diversa; (iii) il periodo durante il quale è stata presentata; (iv) indicazioni se l'annuncio era destinato a un gruppo specifico di destinatari e, in caso positivo, i parametri utilizzati a questo scopo; (v) le comunicazioni commerciali pubblicate sulle piattaforme e individuate ai sensi dell'art. 26, par. 2, DSA; (vi) il numero dei destinatari raggiunti e (se opportuno) i dati aggregati suddivisi per ciascun Stato membro relativi al gruppo o ai gruppi di destinatari ai quali la pubblicità era destinata (art. 39 DSA).

i) sono tenuti a garantire l'accesso ai dati per valutare la conformità al DSA al coordinatore dei servizi digitali (art. 40 DSA).

j) sono tenuti a istituire una funzione di controllo della conformità indipendente dalle loro funzioni operative e composta da uno o più responsabili della conformità (art. 41 DSA).

k) sono tenuti, per le relazioni di cui all'art. 15 DSA, a specificare ulteriori informazioni tra cui: le risorse umane dedicate al servizio offerto nell'UE, le qualifiche e le competenze linguistiche delle persone che svolgono le attività predette e gli indicatori di accuratezza.

12. *I primi casi applicativi del DSA*

Si possono segnalare e riportare anche i primi casi pratici di applicazione del *Digital Services Act*.

Un primo caso meritevole menzione ha riguardato ancora una volta Meta, nei confronti della quale è stata aperta una procedura formale per violazione del DSA in riferimento alle politiche e pratiche relative alla pubblicità ingannevole e ai contenuti di natura politica presente nei servizi offerti dalla piattaforma [85]. Le presunte violazioni riguarderebbero anche la indisponibilità di uno strumento di "monitoraggio delle elezioni"; in particolare, l'assenza di uno strumento efficace vol-

[85] *Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act*, comunicato stampa del 30 Aprile 2024, consultabile al sito www.digital-strategy.ec.europa.eu

to a monitorare in tempo reale le discussioni civiche. La Commissione si riferisce alla scelta di Meta di dismettere uno strumento chiamato *CrowdTangle*, il quale consentiva di raccogliere dati pubblici sui contenuti online e analizzare le conversazioni in tempo reale, senza fornire un'adeguata alternativa.

La Commissione UE ha poi informato la piattaforma X della valutazione preliminare sulle violazioni del DSA nell'ambito dell'uso dei *dark patterns*, della trasparenza nella pubblicità e nell'accesso ai dati per i ricercatori [86]. Quindi, il riferimento normativo individuato dalla Commissione riguarda gli artt. 25, 39 e 40, par. 12, del DSA.

Un altro caso ha riguardato Amazon [87]. In particolare, la Commissione ha chiesto di fornire maggiori informazioni sulle misure adotta-

---

[86] *Commission sends preliminary findings to X for breach of the Digital Services Act*, comunicato stampa del 12 luglio 2024, consultabile al sito www.digital-strategy.ec.europa.eu

[87] Amazon, già designato nel 2023 come VLOP, è stato già protagonista di un giudizio nell'ambito del quale il vicepresidente della Corte di giustizia ha emesso un'ordinanza, la quale ha rigettato la richiesta di sospensione dell'obbligo di rendere pubblico il suo *repository* pubblicitario. Amazon, quindi, è tenuta a rispettare l'intero set di obblighi DSA. In tal senso, Commissione UE c Amazon Services Europe Sàrl, 27 marzo 2024, C-639/23 P(R), eur-lex.europa.eu; il 27 settembre 2023 il Tribunale UE aveva, in sede di primo grado, ordinato la sospensione dell'efficacia della decisione della Commissione che prevedeva per Amazon Store l'obbligo di rendere pubblico il *repository* della pubblicità. Dunque, la Commissione ha presentato appello alla Corte di Giustizia contro l'ordinanza e il Vicepresidente della Corte di Giustizia ha annullato la parte della decisione del Presidente del Tribunale Generale ritenendo che alla Commissione fosse stato impedito di replicare alle deduzioni di Amazon durante il procedimento innanzi al Tribunale. Il Vicepresidente della Corte ha ritenuto che la tesi di Amazon secondo cui l'obbligo di rendere pubblico il *repository* della pubblicità limita illegittimamente i suoi diritti fondamentali al rispetto della vita privata e alla libertà di intraprendere un'attività economica non possa essere considerato irrilevante. È stata rilevata la necessità di valutare se l'equilibrio di tutti gli interessi in gioco possa giustificare il rifiuto della sospensione. È stato sottolineato che gli interessi tutelati dal legislatore europeo prevalgono, nel caso specifico, sugli interessi materiali di Amazon, con il risultato che l'equilibrio degli interessi pende a favore del rigetto della richiesta di sospensione.

te dalla piattaforma per conformarsi agli obblighi del DSA relativi alla trasparenza dei sistemi di raccomandazione e dei relativi parametri, nonché alle disposizioni sulla tenuta di un archivio pubblicitario e del relativo rapporto di valutazione dei rischi. Le informazioni richieste riguardano la trasparenza dei sistemi di raccomandazione, i fattori di *input*, le caratteristiche, i segnali, le informazioni e i metadati applicati per tali sistemi e le opzioni offerte agli utenti per rinunciare a essere profilati dai sistemi di raccomandazione [88]. La società è inoltre tenuta a fornire maggiori informazioni sulla progettazione, lo sviluppo, l'implementazione, i test e la manutenzione dell'interfaccia online della *Ad Library* di Amazon Store e i documenti di supporto relativi al suo rapporto di valutazione del rischio.

Un altro caso ha riguardato Microsoft, ossia il modello di IA generativa Copilot di Bing [89]. La Commissione ha richiesto a Bing di fornire ulteriori documenti e dati interni rispetto a una precedente risposta. La presunzione è che Bing abbia violato il DSA per i rischi legati all'IA generativa, come le cosiddette "allucinazioni", la diffusione virale di *deepfake*, nonché la manipolazione automatizzata di servizi che possono trarre in inganno gli elettori. Infatti, come previsto dal DSA, già visto in precedenza, i soggetti designati devono effettuare un'adeguata valutazione dei rischi e adottare le rispettive misure di mitigazione dei rischi (in tal senso i già analizzati artt. 34 e 35 del DSA).

Una ulteriore richiesta di informazioni ha visto come protagonisti le società Temu e Shein affinché offrano chiarimenti sulle misure adottate nel rispetto del DSA per le *Notice and Action mechanism*, ossia quella impostazione che permette agli utenti di segnalare i prodotti illegali, sulle interfacce online che devono essere progettate in modo da non ingannare o manipolare gli utenti tramite i cosiddetti *dark pattern*,

---

[88] *Commission requests information to Amazon under the Digital Services Act*, comunicato stampa del 5 luglio 2024, consultabile al sito www.digital-strategy.ec.europa.eu

[89] *Commission compels Microsoft to provide information under the Digital Services Act on generative AI risks on Bing*, comunicato stampa del 17 maggio 2024, consultabile al sito www.digital-strategy.ec.europa.eu

oltre alle misure adottate per la protezione dei minori, la trasparenza dei sistemi di raccomandazione, alla tracciabilità dei commercianti e alla conformità fin dalla progettazione [90].

Un ultimo caso meritevole di essere annoverato, incentrato particolarmente sul meccanismo di moderazione dei contenuti, vede come protagonisti i *provider* di Pornhub, Stripchat e XVideos ai quali sono state chieste informazioni sugli obblighi di segnalazione, poiché sembrerebbero difettare informazioni chiare e facilmente comprensibili sulle pratiche di moderazione dei contenuti. La carenza comprende le informazioni inerenti alle ordinanze del tribunale, avvisi, processi di moderazione dei contenuti, sistema interno di gestione dei reclami, nonché i mezzi automatizzati utilizzati ai fini della moderazione dei contenuti [91]. Viene inoltre chiesto di fornire informazioni sulle risorse umane dedicate alla moderazione dei contenuti, comprese quelle informazioni sulle loro qualifiche e competenze linguistiche, nonché gli indicatori di accuratezza e le informazioni correlate sui mezzi automatizzati utilizzati per scopi di moderazione dei contenuti. Anche in questo caso la Commissione chiede informazioni dettagliate sui *repository* degli annunci pubblicitari delle piattaforme, poiché sospetta che questi non siano facilmente consultabili e non permettano agli utenti (o alle autorità competenti) di eseguire ricerche avanzate su più criteri contemporaneamente (ad esempio, cercare pubblicità specifiche in base a vari fattori come data, tipo di prodotto, target di pubblico, ecc.).

Inoltre, non sarebbero offerti strumenti di interfaccia di programmazione delle applicazioni (API), consistenti in *software* che permettono ad altre applicazioni o sistemi di interagire facilmente con la loro piattaforma per ottenere o inviare dati. Il *Digital Services Act* impone,

---

[90] *Commission requests information from online marketplaces Temu and Shein on compliance with the Digital Services Act*, comunicato stampa del 28 giugno 2024, consultabile al sito www.digital-strategy.ec.europa.eu

[91] *Commission requests information under the Digital Services Act to Pornhub, Stripchat and XVideos on their transparency reports and advertisement repositories,* comunicato stampa del 18 ottobre 2024, consultabile al sito www.digital-strategy.ec.europa.eu

infatti, alle piattaforme online di rendere questi dati facilmente accessibili e utilizzabili per garantire maggiore trasparenza e controllo da parte delle autorità e degli utenti. Se una piattaforma non rispetta questi requisiti, potrebbe non essere conforme alle normative stabilite dal DSA.

13. *La nuova figura di «utente commerciale» e di «operatore commerciale» nei mercati digitali*

I recenti regolamenti europei del DMA e DSA lasciano trasparire una politica legislativa peculiare che, *inter alia*, considera la centralità di una "nuova" figura riguardante l'utente commerciale, il quale, nelle dinamiche di mercato, è apparso come soggetto meritevole di una tutela *ad hoc*.

Questa figura compare anzitutto nel regolamento P2B e viene definito come «un privato che agisce nell'ambito delle proprie attività commerciali o professionali o una persona giuridica che offre beni o servizi ai consumatori tramite servizi di intermediazione online per fini legati alla sua attività commerciale, imprenditoriale, artigianale o professionale» (art. 2 P2B). Il regolamento offre una serie di tutele all'utente commerciale nell'ambito del suo rapporto con il fornitore di servizi di intermediazione online e, a differenza del DMA, il fornitore in questione può essere di qualsiasi dimensione, non necessariamente un *gatekeeper*.

Nel DMA emerge una definizione quasi del tutto identica di «utente commerciale» e dalla sua analisi se ne ricava, a chiare lettere, che innanzi alla dominanza e al potere di alcuni grandi operatori digitali, il legislatore ha ritenuto che gli interessi economici e giuridici dell'utente commerciale debbano essere salvaguardati, soprattutto perché, spesso, questo svolge un'attività economica concorrente alla grande impresa che gestisce la piattaforma.

Quindi, con il DMA è stato preso atto che situazioni di questo genere sono frequenti e che il *gatekeeper* può trarre vantaggio utilizzando i dati generati o forniti dai suoi utenti commerciali dalle loro attività al

momento dell'utilizzo dei servizi di piattaforma di base. Questi casi si possono verificare allorché una piattaforma metta a disposizione degli utenti commerciali un mercato online o un negozio online di applicazioni *software* offrendo allo stesso tempo servizi in qualità di impresa fornitrice di servizi di vendita al dettaglio o applicazioni *software*. Ciò ha portato, come si è visto, a vietare l'utilizzo dei dati aggregati o non aggregati, che potrebbero includere dati anonimizzati e personali non accessibili al pubblico, per fornire servizi analoghi a quelli dei loro utenti commerciali [92]. Tale divieto, riguardante un *gatekeeper* collocato in una duplice posizione, deve esse esteso anche a quei dati che un servizio di piattaforma di base ha ricevuto dalle imprese allo scopo di fornire servizi pubblicitari online relativi a tale servizio di piattaforma di base. Si è visto, peraltro, come il DMA tutela l'utente commerciale da quei conflitti di interesse della piattaforma digitale evitando pratiche di "auto-preferenza" nell'indicizzazione dei propri motori di ricerca. Una tutela che si affianca a quella prevista all'art. 5 P2B dove è previsto, per i fornitori di servizi di intermediazione online e i motori di ricerca, che siano stabiliti i principali parametri che determinano il posizionamento degli utenti commerciali e i motivi dell'importanza di questi parametri [93]. Sul punto, la Commissione europea ha adottato una comunicazione relativa agli "orientamenti sulla trasparenza del posizionamento a norma del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio" con l'obiettivo dichiarato di agevolare - anche con l'illustrazione di esempi concreti - il rispetto e l'applicazione da parte dei fornitori dei requisiti di cui all'art. 5 del P2B.

Inoltre, prendendo spunto da altre pratiche effettivamente realizzate da *gatekeeper*, nel DMA è previsto che, al fine di evitare il rafforza-

---

[92] Si veda a tal proposito il considerando n. 46 del DMA.

[93] Con «posizionamento», secondo l'art. 2 P2B, deve intendersi «la rilevanza relativa attribuita ai beni o ai servizi offerti mediante i servizi di intermediazione online, o l'importanza attribuita ai risultati della ricerca da motori di ricerca online, come illustrato, organizzato o comunicato, rispettivamente, dai fornitori di servizi di intermediazione online o dai fornitori di motori di ricerca online a prescindere dai mezzi tecnologici usati per tale presentazione, organizzazione o comunicazione».

mento ulteriore della loro dipendenza dai servizi di piattaforma di base, e con lo scopo di promuovere il c.d. *multihoming*, gli utenti commerciali devono essere liberi di promuovere e di scegliere il canale di distribuzione che ritengono più adeguato a interagire con qualsiasi utente finale già acquisito per mezzo della piattaforma di base.

Con il DSA, il legislatore utilizza un lessico differente che non aiuta l'analisi sistematica degli atti legislativi. Rimanendo focalizzati sulla figura dell'utente commerciale, il DMA lo definisce come «qualsiasi persona fisica o giuridica che, nell'ambito delle proprie attività commerciali o professionali, utilizza i servizi di piattaforma di base ai fini della fornitura di beni o servizi agli utenti finali o nello svolgimento di tale attività» (art. 2 DMA).

Nel DSA, invece, si parla di «operatore commerciale», intendendo «qualsiasi persona fisica o giuridica, pubblica o privata, che agisce, anche tramite persone che operano a suo nome o per suo conto, per fini relativi alla propria attività commerciale, imprenditoriale, artigianale o professionale» (art. 3 DSA).

Le differenze che si colgono si incentrano sul fatto che la nozione di operatore commerciale è più estesa di quella di utente commerciale del DMA. Il primo, infatti, da un punto di vista soggettivo, sembra raccogliere più soggetti, poiché l'intento sembra quello di ricomprendere qualunque attività economica che l'operatore possa compiere rispetto all'utente commerciale del DMA che riguarda le attività commerciali o professionali. Inoltre, quest'ultimo fa riferimento solo a quel soggetto che nell'esercizio della propria attività utilizza la piattaforma di base per erogare i suoi servizi.

Dunque, l'operatore commerciale rappresenta una figura più ampia rispetto all'utente commerciale. Perciò, vi sono situazioni in cui l'utente commerciale può rientrare anche nell'ambito della nozione di operatore commerciale e, quindi, essere sottoposto ad una serie di obblighi previsti nel DSA. Ad esempio, gli operatori sarebbero tenuti a fornire determinate informazioni essenziali ai fornitori di piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori stessi, anche ai fini della promozione di messaggi o dell'offerta di prodotti. L'operatore deve essere sempre tracciabile quando offre

un prodotto o un servizio attraverso una piattaforma online (art. 30 DSA).

14. *La creazione dei servizi di intermediazione nella strategia europea per i dati con il Data Governance Act (DGA – Reg. UE 2022/868)*

Nell'ambito digitale non può affatto trascurarsi un'altra recente normativa come il regolamento sulla *governance* europea dei dati, entrato in vigore il 23 giugno 2022 e applicabile dal 24 settembre 2023.

Si tratta di un regolamento che si inserisce nel complesso quadro della «strategia europea per i dati» con cui ci si pone l'obiettivo di creare uno spazio comune europeo di dati nel quale questi possono essere utilizzati indipendentemente dal luogo di conservazione nell'UE [94]. Si realizza così il passaggio da una disciplina puramente incentrata sulla salvaguardia di determinati beni incorporali dovuta al potenziale di conoscenza che possono rivelare in merito ad una persona, a una disciplina riguardante la circolazione e l'uso di dati «in relazione alla loro strutturazione formale (...), indipendentemente dal tipo di significati che questi siano atti a veicolare» [95].

---

[94] A. MORACE PINELLI, *La circolazione dei dati personali tra tutela della persona,* cit., 1322. In senso anche critico si veda F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, vol. 26, n. 1, 2021, 199, spec. 256. «Con il Data Governance Act l'UE intraprende una strada interessante, che cela però il rischio di svilimento dei diritti fondamentali della persona qualora la direzione intrapresa, registrata sin dai significativi mutamenti del lessico, porti ad un irreversibile processo di reificazione dei dati prima e del soggetto poi, sul quale occorre far rimanere sempre desta l'attenzione, facendo sì che in Europa rimanga viva, anche nella prassi applicativa oltre che nell'impianto di sistema, la «convinzione che l'essere umano sia e debba rimanere l'elemento centrale».

[95] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista Trimestrale di diritto pubblico*, n. 4, 2022, 971, spec. 976. Secondo l'A. è intervenuto il passaggio da una normativa essenzialmente limitativa ad una di stampo promozionale sull'uso dei dati e sottolinea come in Europa circa l'85% dei dati raccolti non viene riutilizzato.

Si intende, quindi, creare un'economia dei dati per consentire alle imprese di prosperare e garantire la neutralità dell'accesso, portabilità e interoperabilità dei dati evitando effetti di dipendenza (*lock-in*). In questo quadro, si intende stimolare una circolazione dei dati libera e sicura, non solo all'interno dei confini europei ma finanche con paesi terzi; per questo, la visione del legislatore è quella di creare spazi comuni europei di dati specifici per settore (come sanità, manifattura, clima, energia e altri). La *ratio* della normativa è di garantire il ruolo neutrale degli intermediari rispetto ai dati scambiati tra gli utenti, realizzando una separazione anche strutturale del modello organizzativo dell'attività d'impresa [96].

Il contenuto normativo che rileva ai fini di quanto in discussione può essere compendiato nel capo II dedicato al riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici, dal capo III dedicato ai servizi di intermediazione dei dati e dal capo IV dedicato all'altruismo dei dati. Nel capitolo II si è già dato conto del capo VII dedicato invece all'accesso internazionale e al trasferimento dei dati.

Il DGA precisa che (art. 1, par. 2, co. 2, DGA) non sono pregiudicate ulteriori e concorrenti normative europee o nazionali settoriali che impongano a enti pubblici, fornitori di servizi di intermediazione o organizzazioni per l'altruismo, un ulteriore regime di certificazione o autorizzazione. Queste norme troverebbero comunque applicazione. In caso di conflitto tra le norme del DGA e le norme del GDPR, o le norme nazionali adottate in conformità di quest'ultimo, prevale la normativa prevista nel DGA (art. 1, par. 3, DGA) [97]. Il paragrafo successivo specifica che il regolamento «lascia impregiudicata l'applicazione del diritto della concorrenza».

Il capo II prevede la facoltà, per alcuni enti pubblici, di consentire il

---

[96] D. Poletti, *Gli intermediari dei dati, in European Journal of Privacy Law & Technologies*, n. 1, 2022, 45, spec. 51.

[97] Per un commento sul rapporto tra GDPR e DGA, nonché sullo scopo del *data governance act*, si veda V. Bellomia, G. Fonsi, *comm. Articolo 1*, in *Dalla* Data Protection *alla* Data Governance*: il Regolamento (UE) 2022/868*, in A. Morace Pinelli (a cura di), *Commentario al* Data Governance Act, Pisa, Pacini, 2024, 133-144.

riutilizzo di una o più categorie di dati previste all'art. 3 DGA [98]. Con «riutilizzo» si intende un diverso e secondario utilizzo dei dati per scopi diversi rispetto a quello originario. Affinché possa essere concesso il riutilizzo dei dati, è necessario che questi siano stati anonimizzati (se si tratta di dati personali) e modificati, aggregati o trattati con qualsiasi altro metodo di controllo della divulgazione in caso di informazioni commerciali riservate. È necessario garantire poi un ambiente di trattamento sicuro. I "riutilizzatori" sono tenuti ad attuare tutte le tecniche volte a impedire la re-identificazione degli interessati a cui quei dati personali fanno riferimento e sono tenuti a osservare un obbligo di riservatezza che impedisce loro di divulgare quei dati per i quali sono stati autorizzati.

Qualora le predette condizioni, come l'anonimizzazione, previste dal DGA, non possono essere rispettate e non vi sia una valida base giuridica per il trasferimento dei dati ai sensi del GDPR, l'ente pubblico si adopera per fornire assistenza ai riutilizzatori e ottenere il consenso da parte degli interessati.

Gli enti pubblici possono imporre delle tariffe per la concessione del riutilizzo dei dati, le quali debbono essere proporzionate, non discriminatorie e non devono limitare la concorrenza (art. 6 DGA).

Il capo III è invece dedicato all'intermediazione dei dati, ossia a un servizio che mira a instaurare rapporti commerciali per finalità di condivisione dei dati tra un numero indeterminato di interessati e di titolari di dati, da un lato, e gli utenti dall'altro. Per condivisione dei dati si intende la fornitura di dati da un interessato o un titolare dei dati a un utente ai fini del loro utilizzo.

Con «titolare dei dati» il legislatore fa riferimento a quel soggetto che ha il diritto di concedere l'accesso a determinati dati personali o non personali, o di condividerli. Per «utente dei dati» ci si riferisce

[98] La normativa del DGA va a completare la disciplina dettata dalla direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione nel settore pubblico, recepita con il D.lgs. n. 200/2021. In tal senso, D. POLETTI, *Gli intermediari dei dati,* cit., 49.

invece a quella persona che ha legittimo accesso a determinati dati e che ha diritto a utilizzarli per finalità commerciali o non commerciali.

È stato annotati che attraverso il DGA il legislatore ha operato un vero e proprio cambio di paradigma anche lessicale facendo riferimento per la prima volta ad una «titolarità» dei dati, circostanza che non si era mai verificata. È un cambio di paradigma che rischia di tradursi in un preludio all'introduzione, per via normativa, di «una reificazione dei dati personali, quali entità giuridicamente rilevanti ex sé più che quali attribuiti della persona» [99].

Il DGA, all'art. 12, prescrive una serie di condizioni affinché si possa fornire il servizio di intermediazione dei dati che è un servizio il cui esercizio è subordinato a una prodromica procedura di notificazione prevista all'art. 11 DGA. L'intermediazione dei dati può avvenire tra titolari dei dati e potenziali utenti dei dati e può includere servizi come scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati (art. 10, lett. a, DGA); può consistere in servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati e potenziali utenti dei dati consentendo così l'esercizio dei diritti degli interessati di cui al GDPR (art. 10, lett. b, DGA); oppure, si può trattare di cooperative di dati (art. 10, lett. c, DGA) [100] salutate positivamente da più parti [101].

---

[99] F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act,* cit., 203; sulla definizione di "titolare dei dati" presente nel DGA, la quale denota una titolarità legata direttamente al dato in sé e al potere del titolare, non di prendere decisioni sulle finalità e mezzi del trattamento, ma di concedere l'accesso a determinati dati, si veda V. Bellomia, *comm. Articolo 2*, in *Dalla* Data Protection *alla* Data Governance, cit., 145, spec. 168.

[100] Per queste ultime si veda F. Bravo, *Le cooperative di dati*, in *Contratto e impresa*, vol. 36, n. 3, 2023, 757; L. Petrone, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, vol. 36, n. 3, 2023, 800; per una analisi più estesa, si veda il volume *EU Data Cooperatives, l'ingresso delle cooperative di dati nell'ordinamento europeo*, F. Bravo (a cura di), Torino, Giappichelli, 2024.

[101] G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 986.

Il capo IV del regolamento è invece dedicato all'altruismo dei dati. Si tratta di un meccanismo, già avallato dall'EDPB, con il quale un soggetto interessato può spontaneamente offrirsi di mettere a disposizione determinati dati per finalità di riutilizzo. Perciò, il DGA prevede una serie di condizioni e prescrizioni affinché questo meccanismo possa essere attuato per il tramite di apposite organizzazioni per l'altruismo dei dati riconosciute le quali sono sottoposte ad una serie obblighi.

Il DGA ha poi portato all'adozione di norme nazionali di adeguamento (D.lgs. del 07 ottobre 2024, n. 144) attraverso il quale è stata nominata la Agenzia per l'Italia digitale quale autorità competente per lo svolgimento dei compiti relativi alla procedura di notifica per i servizi di intermediazione e per la registrazione di organizzazione per l'altruismo dei dati. Questa autorità è incaricata anche in relazione alle attività di controllo e monitoraggio previste all'art. 14 e 24 DGA. Viene designata anche come organismo competente per l'assistenza agli enti pubblici che concedono o rifiutano l'accesso al riutilizzo delle categorie di dati di cui all'art. 3 DGA. L'art. 4 del decreto in commento è dedicato, invece, alla disciplina sanzionatoria ai sensi dell'art. 34 del DGA.

15. *La circolazione dei dati nel sistema dell'Internet of Things con il Data Act (Reg. UE 2023/2854)*

In un altro percorso del dedalo normativo digitale ci si imbatte inevitabilmente nel *Data Act*. Tale regolamento rappresenta una normativa essenziale che completa la strategia europea in materia di dati. Esso, in una prospettiva complementare al DGA, intende favorire la circolazione dei dati e ampliare la platea dei soggetti che possono avere accesso alle informazioni, consentendo, ad esempio, ai proprietari di dispositivi connessi di accedere ai dati da essi generati, autorizzandone poi la condivisione con terze parti nella fornitura di servizi post-vendita.

Il regolamento è stato pubblicato nella G.U. europea il 22 dicembre

2023, ed è vigente dal 11 gennaio 2024. La sua applicazione è prevista a cadenze differenti a seconda dei relativi capi [102]. In caso di contrasto tra GDPR e *Data Act*, prevale il primo.

Il regolamento in questione stabilisce una serie di regole con cui si intende, *inter alia*, individuare i soggetti legittimati ad accedere e a utilizzare i dati generati dai prodotti connessi e dai servizi correlati [103].

---

[102] L'art. 50 del *Data Act* prevede la sua applicazione dal 12 settembre 2025. L'obbligo derivante dall'articolo 3, paragrafo 1, si applica ai prodotti connessi e ai servizi correlati immessi sul mercato dopo il 12 settembre 2026. Il capo III si applica solo in relazione agli obblighi di messa a disposizione dei dati a norma del diritto dell'Unione o della legislazione nazionale adottata in conformità del diritto dell'Unione, che entrano in vigore dopo il 12 settembre 2025. Il capo IV si applica ai contratti conclusi dopo il 12 settembre 2025. Il capo IV si applica a decorrere dal 12 settembre 2027 ai contratti conclusi il o anteriormente al 12 settembre 2025, a condizione che: a) siano a tempo indeterminato; o b) scadano almeno 10 anni dopo l'11 gennaio 2024.

[103] D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, n. 2, 2023, 367, spec. 373. Il considerando n. 15 del *Data Act* precisa a quali dati si fa riferimento nel regolamento legittimando l'accesso e la loro circolazione. Si specifica che i dati generati dall'uso di un prodotto connesso o di un servizio correlato devono essere intesi come dati registrati intenzionalmente o dati che derivano indirettamente da un'azione dell'utente, ad esempio i dati relativi all'ambiente o alle interazioni del prodotto connesso. «Ciò dovrebbe comprendere i dati sull'uso di un prodotto connesso generati da un'interfaccia utente o tramite un servizio correlato e non dovrebbe limitarsi all'informazione relativa al fatto che tale uso è avvenuto, ma dovrebbe comprendere tutti i dati generati dal prodotto connesso a seguito di tale uso, ad esempio i dati generati automaticamente da sensori e i dati registrati da applicazioni incorporate, incluse le applicazioni indicanti lo stato dell'hardware e i malfunzionamenti. Dovrebbe altresì comprendere i dati generati dal prodotto connesso o dal servizio correlato durante i periodi di inattività dell'utente, ad esempio quando quest'ultimo sceglie di non utilizzare un prodotto connesso per un determinato periodo di tempo ma di tenerlo in modalità stand-by o addirittura spento, in quanto lo stato di un prodotto connesso o dei suoi componenti, ad esempio le batterie, può variare quando il prodotto connesso è in modalità stand-by o spento. I dati che non sono modificati in modo sostanziale, ossia i dati in forma grezza, noti anche come dati fonte o dati primari che si riferiscono a punti di dati generati automaticamente senza alcuna ulteriore forma di trattamento, e i dati che sono stati pretrattati al fine

Con «servizio correlato» deve intendersi quel servizio digitale (diverso rispetto a un servizio di comunicazione elettronica), connesso con il prodotto al momento dell'acquisto o noleggio.

Anche nel *Data Act*, al pari di quanto avviene nel DGA, è presente un cambio di paradigma con i riferimenti alla titolarità dei dati [104]. Infatti, con «utente» si intende quella persona che possiede un prodotto connesso o una persona a cui, temporaneamente, sono stati concessi i diritti di utilizzo in relazione a tale prodotto. Con «titolare dei dati» si intende quella persona che ha il diritto o l'obbligo di utilizzare e mettere a disposizione dati, inclusi quei dati del prodotto o di un servizio correlato, se previsto contrattualmente. Con «destinatario dei dati» si intende quella persona alla quale vengono messi a disposizione i dati da parte del titolare.

Il *Data Act,* tra le varie aree di regolazione, prevede nuove prerogative di accesso ai dati da parte degli enti pubblici in presenza di «necessità eccezionali» [105].

Nel suo insieme, si tratta di un regolamento complesso che regola differenti sfaccettature e ambiti inerenti all'accesso ai dati. A partire dall'art. 3 del *Data Act* vengono stabilite una serie di regole volte a determinare le modalità di esercizio del diritto dell'utente di accedere ai dati generati dal prodotto connesso o dal servizio correlato. L'art. 5,

---

di renderli comprensibili e utilizzabili prima di ulteriori operazioni di trattamento e analisi rientrano nell'ambito di applicazione del presente regolamento».

[104] Per una analisi, anche di questo aspetto, si veda A. RICCI, *Introduzione al regolamento europeo sull'accesso equo e sul loro utilizzo*, in *Le nuove leggi civili commentate*, n. 4, 2024, 799, spec. 805-812. L'A. riporta esempi di prodotti connessi, tra i quali «le smart cars, i dispositivi medici che consentono di monitorare a distanza lo stato di salute della persona, i dispositivi fitness, quali cardio-sensori e contapassi, e i dispositivi per la casa intelligente»; riporta poi esempi di servizi correlati, tra i quali «nell'ambito dei dispositivi per la casa intelligente, le applicazioni che regolano le luci e la temperatura delle stanze, e le applicazioni che consentono, in base ai dati dei diversi sensori all'interno degli elettrodomestici, di valutare l'impatto ambientale dei diversi cicli di utilizzo e conseguentemente di regolarli».

[105] G. BUTTARELLI, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale di diritto amministrativo*, n. 1, 2023, 116, spec. 120.

peraltro, prevede un diritto dell'utente di condividere i dati con terzi, prontamente messi a loro disposizione dal titolare dei dati, oltre ai relativi metadati necessari a interpretare e utilizzare i dati in questione. Però, dalla nozione di «terzo» a cui possono essere messi a disposizione i dati, il par. 3 dell'art. 5 esclude espressamente quei soggetti che sono *gatekeeper* ai sensi del *Digital Markets Act* (DMA).

Se l'utente intende condividere - per i tramite del titolare - dati con terzi, qualora essi riguardino dati personali anche di altri soggetti, diversi dall'utente, possono essere messi a disposizione del terzo solo al cospetto di un'idonea base giuridica prevista dall'art. 6 GDPR e, se necessario, nel rispetto dell'art. 9 GDPR, inerente ai dati personali particolari e all'art. 5, par. 3, dir. (UE) 2022/58.

Il capo III del regolamento prescrive gli obblighi gravanti sul titolare di mettere a disposizione i dati ai destinatari sulla base delle condizioni concordate con questi ultimi (art. 8). Gli accordi tra questi due soggetti non devono contenere quelle clausole abusive disciplinate nel successivo art. 13 *Data Act*. L'attività prevista a carico del titolare dei dati può prevedere un congruo compenso.

L'utente dovrebbe essere libero di utilizzare i dati per qualsiasi finalità legittima, inclusa la fornitura dei dati che l'utente ha ricevuto nell'esercizio dei suoi diritti a un terzo che offre un servizio post-vendita e che può essere in concorrenza con un servizio fornito da un titolare dei dati.

I titolari dei dati devono perciò garantire che i dati messi a disposizione del terzo siano tanto accurati, completi, affidabili, pertinenti e aggiornati quanto i dati ai quali il titolare stesso può essere in grado o avere il diritto di accedere in virtù dell'uso del prodotto connesso o del servizio correlato [106].

Secondo il considerando n. 33, nella messa a disposizione dei dati a un terzo, un titolare dei dati non deve abusare della sua posizione per ottenere un vantaggio competitivo in mercati in cui il titolare dei dati e il terzo possono trovarsi in concorrenza diretta. Quindi, il titolare dei

[106] In questo senso il considerando n. 30 *Data Act*.

dati non deve utilizzare dati prontamente disponibili al fine di ottenere informazioni sulla situazione economica, sulle risorse o sui metodi di produzione del terzo o sul loro utilizzo da parte di quest'ultimo in un modo che possa compromettere la posizione commerciale del terzo sui mercati in cui quest'ultimo è attivo.

La normativa codifica anche un modello che viene denominato *Reverse PSI* e delinea una fattispecie generale di trasferimento dei dati (personali e non) dal settore privato a quello pubblico [107]. Infatti, il capo V del *Data Act* è rubricato «mettere i dati a disposizione di enti pubblici, della commissione, della banca centrale europea e di organismi dell'unione europea sulla base di necessità eccezionali» il quale dall'art. 14 prevede le ipotesi in cui gli enti pubblici possono utilizzare alcuni dati, inclusi i metadati, per le proprie funzioni nel perseguimento di un interesse pubblico messi a disposizione dai loro titolari su richiesta motivata. Ciò pone le premesse per una sorta di trasferimento coattivo dei dati per pubblico interesse rischiando di divenire l'equivalente strumento dell'espropriazione nel mondo digitale [108].

Nel capo VI del *Data Act* è disciplinato il «passaggio tra servizi di trattamento dei dati», ovvero una specificazione, o l'equivalente del diritto alla portabilità. Con «passaggio» il legislatore intende quel processo che coinvolge un fornitore di servizi di trattamento dei dati di origine [109], un cliente di un servizio di trattamento dei dati e, eventualmente, un fornitore di servizi di trattamento dei dati di destinazione. In questo processo di «passaggio» il cliente transita dall'utilizzo di un servizio di trattamento dei dati a un altro offerto da un diverso fornitore anche attraverso l'estrazione, trasformazione e caricamento dei dati. Agli artt. 25 - 30 del *Data Act* vengono sanciti una serie di obbli-

---

[107] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati,* cit., 980.

[108] *Ivi*, 981.

[109] Con «servizio di trattamento dei dati» si intende «un servizio digitale fornito a un cliente e che consente l'accesso di rete universale e su richiesta a un *pool* condiviso di risorse informatiche o altamente distribuita e che può essere rapidamente erogato e rilasciato con un minimo sforzo di gestione o interazione con il fornitore di servizi configurabili, scalabili ed elastiche di natura centralizzata, distribuita».

ghi e di condizioni per consentire l'esercizio del diritto di passaggio da un fornitore a un altro.

Infine, il capo VIII è dedicato alla disciplina della «interoperabilità», considerata dal legislatore come «la capacità di due o più spazi di dati o reti di comunicazione, sistemi, prodotti connessi, applicazioni, servizi di trattamento di dati o componenti di scambiare e utilizzare dati per svolgere le loro funzioni». Anche il *Data Act*, quindi, introduce importanti novità in termini di utilizzo, accesso e circolazione di dati personali (e non personali), rappresentando un ulteriore importante tassello nella normativa dei mercati digitali.

Capitolo V

LE NUOVE SFIDE NEL CONTESTO NORMATIVO DEI MERCATI DIGITALI

Sommario: 1. Il dedalo normativo nel settore dei mercati digitali. La (già) impellente necessità di delineare un quadro sistematico – 2. La ricostruzione del dibattito sull'incidenza della normativa privacy nelle dinamiche antitrust– 3. Il consenso al trattamento dei dati per l'erogazione del servizio o prodotto digitale «gratuito» in sostituzione del «corrispettivo» – 4. Gli elementi di una (complessa) indagine antitrust per i servizi o prodotti digitali: la valutazione del mercato rilevante nel «mercato a due versanti» richiede un approccio differente rispetto ai mercati tradizionali – 5. La perdurante centralità del consenso che non produce un trasferimento di un diritto dominicale in favore del titolare del trattamento – 6. Il dibattito sul *pay or consent* – 7. Gli standard del trattamento dei dati personali come parametro per la qualità del prodotto digitale a tutela di una libera scelta dell'utente consapevole – 8. Il nuovo quadro normativo europeo dei dati e dei mercati digitali introduce novità e consolida fattispecie previgenti – 9. L'utilizzo dell'algoritmo nel trattamento dei dati personali. Il caso *Mevaluate* – 9.1 Il caso "Schufa" (CGUE C-634/21). Ancora sullo *scoring* algoritmico, anche alla luce del regolamento europeo sull'intelligenza artificiale – 9.2 Il diritto di accesso ai dati personali e la nozione di informazioni significative sulla "logica utilizzata" nell'ambito di un processo decisionale automatizzato. Il caso "Dun & Bradstreet" (CGUE C-203/2022)

1. *Il dedalo normativo nel settore dei mercati digitali. La (già) impellente necessità di delineare un quadro sistematico*

Si è visto che nel settore digitale, dei dati personali e, in generale, nell'ambito delle nuove tecnologie, il legislatore si è dimostrato particolarmente produttivo.

Gli interventi normativi sono copiosi e necessitano di una proficua e complessa attività di attuazione e di coordinamento, fondamentale per evitare un "effetto sabbie mobili" nei vari ambiti. Un'attività impervia già solo per il differente lessico utilizzato nell'una e nell'altra normativa, in grado di disorientare l'interprete.

In particolare, è necessario ordinare le diverse normative che negli ultimi anni sono state adottate e altre che sono ancora in una fase di discussione. Tra le normative già entrate in vigore (sebbene con una applicazione differita), sono stati analizzati il *Data governance Act* (Reg. UE 2022/868) e il *Data Act* (Reg. UE 2023/2854), ai quali va aggiunto il regolamento europeo sullo spazio europeo dei dati sanitari (EHDS – Reg. UE 2025/327) e l'*AI Act* (Reg. UE 2024/1689), oltre alle già esaminate normative come il DSA, il DMA. L'intero quadro dovrebbe poi essere integrato con un'ulteriore normativa, ossia la legislazione in materia di cybersicurezza, come la nuova direttiva NIS 2 (Dir. UE 2022/2555), recentemente recepita con il d.lgs. n. 138 del 1 ottobre 2024, e il nuovo *Cyber Resilience Act*.

Infine, nel contesto normativo in formazione deve segnalarsi che la proposta di direttiva sulla responsabilità extracontrattuale derivante dai sistemi di IA è stata stralciata perché le istituzioni europee non sono riuscite a raggiungere un'intesa, mentre la nuova direttiva sulla responsabilità da prodotti difettosi è stata definitivamente emanata (Direttiva UE 2024/2853).

La molteplicità di iniziative legislative europee e nazionali va a comporre un vero e proprio dedalo normativo che rischia di minare la certezza del diritto, dissuadendo gli attori che investono in questi settori in via di sviluppo e disorientando l'utente-consumatore, incapace di rendersi consapevole di ciò in cui si imbatte e di quelli che sono i propri interessi tutelati.

Si è al cospetto di un contesto normativo che abbraccia sempre più l'opera di decodificazione del sistema giuridico già avviata nel secolo scorso [1], abbandonando un quadro sistematico composto da codici

[1] N. IRTI, *L'età della decodificazione*, Milano, Giuffrè, 1989, 26-27. L'A. già varie de-

classici e, ormai, anche da codici di settore. Tutto ciò rende necessaria un'opera di composizione di un quadro giuridico sistematico che consenta a tutti i soggetti coinvolti di orientarsi senza incertezze che andrebbero a minare gli interessi del soggetto più debole e pregiudicherebbero gli interessi economici dell'impresa.

Dunque, di seguito ci si focalizzerà su alcune delle più recenti sfide che il nuovo contesto normativo tenta di regolamentare nel settore dei mercati digitali sulla base di quanto già delineato nei precedenti capitoli. Tra queste, alcune riflessioni sulla incidenza, già vista nel capitolo III, della normativa *privacy* sulle dinamiche antitrust, oltre ad alcuni rilievi sulle dinamiche contrattuali che coinvolgono la fallace gratuità dei servizi digitali, nonché gli aspetti che riguardano il DSA, il DMA e il trattamento dei dati personali per l'ottenimento di un "punteggio" sul merito dell'interessato e nel settore della pubblicità online.

---

cadi fa metteva in evidenza come il «codice civile ci appare ormai aggredito dalle leggi speciali, che strappano istituti e categorie di rapporti, o provvedono alla disciplina di fenomeni appena emersi dalla realtà economica. Il periodo storico, che si apre con il secondo dopoguerra, sarà forse ricordato come l'età della decodificazione: di una quotidiana e penetrante conquista di territori da parte delle leggi speciali. (...) Nate come eccezioni o come mero svolgimento di principi codificati, le leggi speciali si impadroniscono di intere classi di rapporti, li sottopongono a nuove e diverse logiche di disciplina, esprimono criteri generali ed autonomi». Una caratteristica fondante del fenomeno, secondo l'A., 27-28, «risiede sempre più spesso nell'appartenenza dei destinatari a determinate cerchie o categorie di soggetti, sicché le leggi speciali si configurano come veri e propri *statuti di gruppi*. Quando una cerchia di soggetti (...) consegue nella forma della legge gli scopi, che avrebbe potuto raggiungere, o aspirare a raggiungere, mediante gli antichi strumenti negoziali, allora la legge diviene regola di un gruppo specifico e cessa di essere regola del cittadino neutro e indifferenziato».

2. *La ricostruzione del dibattito sull'incidenza della normativa privacy nelle dinamiche antitrust*

Per ripercorrere la storia del diritto della concorrenza è necessario riavvolgere il nastro della giurisprudenza e della legislazione per varie decadi.

Nel precedente capitolo III sono stati messi in luce alcuni caratteri essenziali di un ambito complesso e si è visto che, prendendo in esame il solo abuso di posizione dominante, le chiavi di lettura che sono state fornite in merito ai vari elementi costitutivi dell'istituto possono essere rintracciate già a partire dagli anni 60' e 70' del secolo scorso. La scienza giuridica ha dibattuto ampiamente su questi temi che, però, hanno incontrato alcune difficoltà applicative e uno scarso tasso di indagine nel campo dei mercati digitali.

Tuttavia, benché vi siano state precedenti avvisaglie, l'anno 2016 può essere considerato il periodo di svolta in questo settore, una specie di spartiacque. Questo perché si è assistito, da un lato, all'emanazione di un importante parere dell'EDPS [2] e, dall'altro, a un'indagine della Commissione europea che ha segnato un cambio di passo come quella che ha riguardato la fusione della piattaforma LinkedIn in Microsoft. In questa vicenda la Commissione ha ritenuto che la tutela dei dati personali, benché non faccia parte in modo diretto del diritto della concorrenza, sia in grado di avere un'incidenza antitrust qualora i consumatori la percepiscano come un fattore di *qualità* del servizio e qualora le imprese concorrano tra loro anche sulla base di tale componente.

I cambi di tendenza a cui si è assistito non si esauriscono a quanto poc'anzi accennato. Infatti, con i più recenti interventi legislativi si è potuto osservare un ulteriore cambio di paradigma. I poteri privati

[2] Ci si riferisce al parere n. 8/2016 con cui l'EDPS sostiene che le pratiche di acquisizione e l'utilizzo dei dati personali, nell'ottica di tutela della *privacy*, possano produrre un danno ai consumatori e quindi, di riflesso, comportare ipotesi di condotte anticoncorrenziali.

che i grandi operatori del mercato digitale hanno conquistato negli anni ha definito la impossibilità di soffermarsi esclusivamente sul classico rapporto dicotomico imprenditore/professionista e consumatore; sicché, si è venuto ad aggiungere, soprattutto con il regolamento P2B, il DMA e il DSA, la figura dell'*utente commerciale* [3].

Quest'ultimo è rappresentato, il più delle volte, da quelle piccole e medie imprese che competono nei mercati digitali e che necessitano di una tutela *ad hoc* per operare senza subire le asimmetrie informative e gli squilibri economici e contrattuali che le posizioni dominanti delle *big tech* producono. Questo rappresenta il punto di incontro tra le dinamiche contrattuali, le dinamiche concorrenziali e le questioni di tutela in senso stretto di nuovi soggetti "deboli" che si affiancano ai consumatori.

Il legislatore, si è visto, è intervenuto anche con lo scopo di rendere contendibile il mercato delle piattaforme digitali. Ciò ha condotto a un approccio normativo che prevede una regolamentazione di portata differente fra le grandi imprese e le altre imprese. Un obiettivo perseguito soprattutto con il DMA.

I profili illustrati costituiscono due facce della stessa medaglia. In altri termini, in riferimento all'incidenza della normativa *privacy* sulle dinamiche concorrenziali, esiste un profilo che riguarda la tutela *ex post* delle imprese e del mercato che si è visto nel III capitolo e un altro profilo, invece, che riguarda una tutela *ex ante*, riproduttivo di un elemento di novità sorto dalle difficoltà applicative della normativa tradizionale nel settore tecnologico. L'attuazione futura di questa nuova disciplina, affrontata nel capitolo IV, determinerà le sorti dei mercati digitali; in particolare, della loro equità e contendibilità [4].

---

[3] Come si è visto, nel DSA si parla di «operatore commerciale».

[4] In merito ai due regolamenti europei del DSA e DMA in dottrina ci si chiede se siano destinati a svolgere una funzione complementare che va ad incentivare un uso corretto delle nuove tecnologie, o se questi rischiano di rimanere inapplicati. Una riflessione è stata espressa in merito al rapporto tra diritto della concorrenza e Reg. UE 2018/3012 recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione, in V. Falce, *Appunti sul regolamento europeo sul*

3. *Il consenso al trattamento dei dati per l'erogazione del servizio o prodotto digitale «gratuito» in sostituzione del «corrispettivo»*

Soffermandoci sul primo profilo illustrato nel paragrafo precedente e, in modo particolare, sull'abuso di posizione dominante, le conclusioni che si possono trarre differiscono a seconda del ruolo che viene assegnato al trattamento dei dati personali. La valutazione dev'essere svolta nel quadro di una società in cui la circolazione dei dati personali ha conquistato un significato dirompente, portando anche al vivace dibattito (cfr. cap. I, § 16) che ha creato una visione personalistica e una patrimonialistica a cui si fa rinvio.

Con le ultime novità normative del DGA, del *Data Act* e della direttiva UE 2019/770, è evidente che l'intento sia quello di favorire una circolazione dei dati personali al livello europeo, regolando anche quello extra-europeo, senza sacrificare la sua integrità di diritto fondamentale.

Nella sinergia tra protezione dei dati personali e disciplina antitrust, la principale difficoltà che - si può dire fino al 2016 - accompagnava l'atteggiamento esitante delle Autorità nell'applicazione degli illeciti antitrust nel quadro dei mercati digitali spesso risiedeva nel fatto che la fornitura del servizio è priva di un corrispettivo pecuniario e, quindi, è apparentemente *gratuita*.

Il prezzo, in vero, funge da asse portante delle indagini anticoncorrenziali; perciò, in suo difetto, verrebbe a mancare l'elemento che consentirebbe di sviluppare ragionamenti giuridici in linea con quanto tradizionalmente effettuato. I consumatori, infatti, hanno di principio piena consapevolezza del prezzo dei beni e dei servizi, il quale funge da parametro oggettivo.

Basti quindi pensare al ruolo che ricopre il prezzo nell'indagine del mercato rilevante in sede di abuso di posizione dominante. Secondo la Commissione europea, il mercato rilevante si compone di una valutazione dicotomica. Essa è frutto della combinazione del mercato del prodotto e del mercato geografico [5]. Il primo, comprende tutti i pro-

---

geo-blocking e la neutralità geografica. In cammino verso il mercato unico digitale, in *Contratto e impresa*, vol. 33, n. 4, 2019, 1287, spec. 1291.

dotti e i servizi che vengono considerati intercambiabili o sostituibili dal consumatore in ordine alle loro caratteristiche, ma anche in base al loro prezzo e all'uso a cui sono destinati. Nell'indagine riguardante il mercato del prodotto rilevante, quindi, il prezzo ha sempre costituito un elemento basilare.

Dunque, un primo passo in avanti è stato compiuto allorché da più parti è emerso il risultato univoco, e pressocché inconfutabile, che i dati personali, *rectius*, il trattamento dei dati personali per finalità che esulano dall'esecuzione del contratto, rappresenta la condizione necessaria per ricevere la fornitura del servizio richiesto. In sostanza, nonostante le legittime perplessità, il consenso al trattamento dei dati personali (o il trattamento in sé) ha, per molti casi, sostituito il prezzo inteso in termini monetari. Sebbene non si intenda parlare di «corrispettivo» o di «controprestazione», la realtà dei fatti descritta dimostra sicuramente un cambio di paradigma che ha portato a uno scenario peculiare che merita di essere chiarito [6].

Ebbene, sulle caratteristiche di questo scenario si dibatte ampiamente da qualche anno. Da un lato, si tenta di fornire una qualificazione a tali modelli contrattuali, [7] e dall'altro, si discetta anche sulla natura del consenso al trattamento dei dati personali, inquadrandolo come una prestazione condizionale [8]. Se, però, si inquadra il rapporto negoziale tra utente e piattaforma come negozio gratuito, la prestazione del consenso potrebbe essere ritenuta l'elemento che genera un contratto modale [9].

---

[5] Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto comunitario in materia di concorrenza (97/C – 372/03).

[6] Sul ruolo e sulla funzione del consenso in questi rapporti si veda quanto indicato da C. Irti, *Consenso "negoziato",* cit., 102 ss., oltre a V. Ricciuto, *L'equivoco della privacy,* cit., 142.

[7] Si veda a tal proposito V. Ricciuto, *La patrimonializzazione dei dati personali,* cit., 711 ss.

[8] C. Irti, *Consenso "negoziato",* cit., 77.

[9] La giurisprudenza di legittimità si è espressa nel senso che le specifiche disposizioni che disciplinano il modus «non esauriscono la possibile gamma negoziale in cui può estrinsecarsi l'autonomia privata (...), attesa l'attitudine del modus a modi-

In questo senso, il consenso potrebbe costituire l'elemento contrattuale accidentale del «modo» che realizza l'interesse patrimoniale del contraente. Ciò sta a significare che, da un punto di vista privatistico, in caso di illiceità nel trattamento dei dati dovuto a un consenso estorto o non libero, il *modus* dovrebbe ritenersi illecito e, quindi, come "non apposto" o, nel caso in cui costituisse l'unico motivo determinante, provocare la nullità del contratto in questione. Il *modus* elide il carattere della gratuità del contratto solo se è tale da acquisire natura di controprestazione [10]. Per questa valutazione occorre raffrontare e bilanciare i sacrifici e i vantaggi che dal contratto derivano rispettivamente alle parti [11].

Se, invece, si esclude il rapporto negoziale tra utente e piattaforma come negozio gratuito, ritenendo che la prestazione del consenso equivalga a un «corrispettivo», per le ipotesi di «doppio binario» (*pay or consent*) si potrebbe ricadere nella disciplina di cui all'art. 1285 c.c. relativa all'obbligazione alternativa [12] oppure, a seconda della struttura del rapporto, nell'ambito della obbligazione facoltativa [13].

In casi del genere, l'alternativa al corrispettivo in denaro consisterebbe in una cessione di determinati diritti, ossia il diritto a un deter-

---

ficare, ampliandolo, il singolo schema negoziale, consentendo la realizzazione di singole e specifiche finalità estranee alla causa». Di questo tenore Cass. civ., Sez. I, Sent. 11 giugno 2004, n. 11096, *Foro Italiano*, n. 1, 2005, 466.

[10] Cass. civ., Sez. II, 25 settembre 1990, n. 9718, *Giurisprudenza italiana*, 1992.

[11] Cass. civ., Sez. III, 02 marzo 2001, n. 3021, *Giurisprudenza italiana*, 2001, che in tema di comodato ha statuito che «In presenza di un "modus" a carico del comodatario, il carattere di essenziale gratuità del comodato viene meno solo se il vantaggio conseguito dal comodante si pone come corrispettivo del godimento della cosa con natura di controprestazione e non quando il comodatario si limiti al pagamento della somma periodica a titolo di rimborso spese».

[12] Ciò ad eccezione dell'art. 1286, co. 2, c.c. che prescrive l'irrevocabilità della scelta, visto il diritto di revoca del consenso sancito nel GDPR, il quale va considerato prevalente.

[13] L'obbligazione facoltativa è strutturalmente differente da quella alternativa poiché prevede una prestazione dedotta nel rapporto obbligatorio e la facoltà per il debitore di liberarsi adempiendo, a sua scelta, a una diversa obbligazione. In tal senso si veda C.M. BIANCA, *Diritto civile*, Milano, Giuffrè, 1993, 125.

minato trattamento di dati personali. Ciò sarebbe una configurazione ammissibile se entrambe le prestazioni alternative (corrispettivo in denaro e trattamento dei dati personali) vengono dedotte in obbligazione e al debitore viene lasciata la scelta tra l'una o l'altra [14]. Sul meccanismo del *pay or consent* si tornerà anche successivamente.

4. *Gli elementi di una (complessa) indagine antitrust per i servizi o prodotti digitali: la valutazione del mercato rilevante nel «mercato a due versanti» richiede un approccio differente rispetto ai mercati tradizionali*

La riflessione sul rapporto tra protezione dei dati personali e diritto della concorrenza deve prendere spunto da presupposti di fondo consolidati per poi analizzare le peculiarità applicative.

Si è visto come nel corso degli anni si sono susseguite una serie di teorie sull'abuso di posizione dominante. Le principali, però, tra loro complementari, riguardano la *speciale responsabilità* che fa capo all'impresa in posizione dominante e la *concorrenza basata sui meriti* [15].

---

[14] La scienza giuridica ammette la configurazione di un'obbligazione come alternativa se v'è parità delle prestazioni, facoltà di scelta attribuita al debitore e deduzione nell'obbligazione (Trib. Biella, 06 maggio 2021, n. 201). Sul presupposto della parità delle prestazioni, Cass. civ., 27 ottobre 2020 n. 23556, CED Cassazione, 2020, sulla base di precedenti giurisprudenziali ha chiarito che nell'obbligazione alternativa «le prestazioni vengono poste in una posizione di parità reciproca, restando rimessa alla volontà del debitore o del creditore la scelta dell'una o dell'altra». La cassazione sottolinea anche la differenza con la "falsa alternativa" che si configura allorché la seconda delle due prestazioni sia dovuta solo in caso di inadempienza della prima rispetto alla quale la seconda si pone in un rapporto di subordinazione. Secondo la dottrina prevalente, le norme in materia di obbligazioni alternative potrebbero essere applicate in via analogica al caso in cui le differenti modalità di adempimento siano state oggetto di particolare apprezzamento delle parti, corrispondente ad un loro specifico interesse; cfr. A. Di Majo, B. Inzitari, *Obbligazioni alternative*, in *Enciclopedia del diritto*, XXIX, Milano, Giuffrè, 1979, 216.

[15] Si veda sul tema M. Libertini, *Abuso del diritto e abuso di posizione dominante,* cit., 9.

Si è visto che, perché si verifichi una condotta anticoncorrenziale, non è necessario che venga violata una norma, ma ciò che rileva è l'effetto restrittivo della concorrenza. Su questo piano, poi, si inserisce l'elemento soggettivo, per il quale è stata recentemente adita la Corte di giustizia europea. Nondimeno, ad oggi, secondo la giurisprudenza italiana dominante, è sufficiente che vi sia una consapevolezza dell'effetto restrittivo della concorrenza derivante dalla condotta, ma non sarebbe necessaria la consapevolezza di aver violato un divieto previsto da una norma.

Si è visto, peraltro, che la concorrenza basata sui meriti sorge dalla difficoltà di individuare una fattispecie antitrust là dove l'effetto escludente dei concorrenti dipenda da meriti di una impresa dovuti solitamente a fattori innovativi. Sicché, la meritevolezza viene valutata sulla base della qualità delle offerte vagliate dalla *libera scelta* dei consumatori. Oggi, probabilmente, per alcuni mercati, oltre alla libera scelta dei consumatori, dovrebbe essere considerata, in aggiunta o in alternativa, anche la libera scelta degli utenti commerciali.

In virtù di quanto sopra ripercorso e sintetizzato, si possono classificare alcuni elementi più concreti.

Prendendo le mosse dall'indagine sul mercato rilevante, la peculiarità storicamente riscontrata nell'ambito dei mercati digitali, è utile ripeterlo, è rappresentata dall'assenza del prezzo in termini pecuniari dal lato degli utenti.

Invero, la valutazione della sostituibilità sul versante della domanda si è sempre focalizzata su una indagine riguardante la possibilità per i consumatori di passare ad un prodotto simile a seguito di un esiguo e permanente aumento di prezzo [16].

L'apparente gratuità del servizio o del prodotto che caratterizza alcuni servizi non può tuttavia costituire un ostacolo all'applicazione della normativa antitrust dal momento che le piattaforme digitali agiscono nel rispetto della logica di mercato poiché perseguono finalità

[16] Sul tema si veda V. FALCE, *Piattaforme ed ecosistemi digitali. Scelte pro-concorrenziali*, in *Rivista di diritto industriale*, n. 4-5, 2022, 172, spec. 177-184.

commerciali,[17] sebbene in una logica di «mercato a due versanti»[18]. Come è stato rilevato in giurisprudenza, l'attività consistente nell'offrire un servizio digitale "gratuito" costituisce un'attività economica, poiché, pur utilizzandolo, gli utenti accettano che il gestore (come era, ad esempio, nel caso di specie, un motore di ricerca) raccolga dati che li riguardano, suscettibili di essere valorizzati, in particolare con gli inserzionisti che intendono visualizzare annunci pubblicitari nelle pagine dei risultati[19].

Nei mercati tradizionali a un versante i prezzi vengono fissati sulla base dell'elasticità della domanda e del costo marginale. Ma, nel caso di mercati a due o più versanti, l'operatore può concedersi l'applicazione di prezzi inferiori ai costi marginali grazie agli effetti di rete e ai ricavi provenienti da entrambi i lati[20].

Il parametro della sostituibilità della domanda, dunque, si è dovuta adattare in qualche modo alla nuova economia dei dati poiché non esistono "parametri di prezzo" tradizionalmente intesi in questi modelli

---

[17] Sul tema si veda M. Maggiolino, *I Big Data e il diritto antitrust*, cit., 198

[18] Con mercati a due versanti (o a due lati), o «*two-sided Markets*», si fa riferimento a quei mercati in cui una opera una piattaforma che unisce due gruppi di utenti e le relazioni che instaura con ciascuno di loro influenza anche il comportamento dell'altro gruppo, solitamente con una esternalità come l'effetto di rete. Si veda sul punto F. Thépot, *Market Power in Online Search and Social Networking: A Matter of Two-Sided Markets*, in *World Competition, Kluwer Law International*, vol. 36, n. 2, 2013, 195, spec. 198.

[19] Trib. UE, T-612/17, Sent. 10 novembre 2021, eur-lex.eu. Si legge poi nella sentenza, § 43, che «in generale, nelle piattaforme «bilaterali», un lato gratuito per un tipo di utente (nella fattispecie l'utente di Internet) consentirebbe, se funziona correttamente, di rafforzare la domanda dell'altro lato, a sua volta a pagamento per il suo tipo di utente (nella fattispecie l'inserzionista che intenda raggiungere il maggior numero possibile di utenti di Internet). In tal senso, i vari servizi di ricerca generale su Internet sarebbero in concorrenza per attirare sia gli utenti di Internet che gli inserzionisti attraverso la qualità del loro motore di ricerca».

[20] Nei mercati tradizionali ci si affida allo SSNIP test, non più applicabile per le dinamiche che caratterizzano i mercati digitali.

commerciali [21]; l'attribuzione di un corrispettivo equivalente al trattamento dei dati - inteso in termini di qualità - è ancora oggi un'operazione giuridica non immediata.

Su questa linea, con una decisione della Commissione europea del 2019 è stato sottolineato che la fornitura di pubblicità collegata alle ricerche online costituisce un mercato del prodotto rilevante distinto in quanto non sostituibile con la pubblicità offline, con la pubblicità online non collegata alle ricerche e con i risultati di ricerche specializzate a pagamento. Viene specificato nella decisione che il mercato dell'intermediazione pubblicitaria nei motori di ricerca costituisce un mercato del prodotto rilevante distinto in quanto vi è una limitata sostituibilità con: i) le vendite dirette online; e ii) i servizi di intermediazione pubblicitaria per la pubblicità online non collegata alle ricerche [22].

D'altro canto, nell'analisi della Commissione non si rinviene alcun riferimento al prezzo ed è stata effettuata una valutazione del mercato rilevante su due fronti, ossia individuando da un lato il mercato rilevante del prodotto (dal versante dell'utente) nel motore di ricerca e, dall'altro (dal versante dell'inserzionista) nella pubblicità online.

Nei mercati a due versanti, quindi, non si possono applicare gli stessi parametri abitualmente impiegati per quelli tradizionali [23]. La necessità di analizzare entrambi i mercati, come nel caso della pubblicità online, ossia il versante dell'utente da un lato e dell'inserzionista dall'altro, rende senz'altro più complessa l'indagine [24].

---

[21] Come affermato in dottrina, quindi, «il diritto antitrust deve affrancarsi da un'enfasi ristretta al prezzo dei beni finali intesa come misura del potere di mercato, arrivando a contemplare le dinamiche degli ecosistemi multi-prodotto e multi-attore», V. FALCE, *Piattaforme ed ecosistemi digitali,* cit., 181.

[22] Decisione Commissione europea del 20 marzo 2019, Caso AT.40411 - *Google Search (AdSense).*

[23] F. THÉPOT, *Market Power in Online Search,* cit., 199-200 e 214-215.

[24] Si è iniziato a prendere atto della necessità dei due mercati quando si tratta di piattaforme digitali già a partire dal 2010 con il caso della Commissione europea, M.2727, *Microsoft / Yahoo! Search Business*, consultabile al sito competition-cases.ec.eu-

La complessità di questo profilo si acuisce se si considera un altro aspetto delle grandi piattaforme sempre più evidente e costituito dal potere di *leveraging*, riguardante lo sfruttamento della posizione acquisita per ottenere vantaggi in altri mercati. Si assiste perciò alla tendenza dei grandi operatori di sfociare in differenti e separati mercati mettendo a nudo quella differenza tra concorrenza sul mercato e concorrenza per il mercato [25]. Basti pensare alla imponente espansione ancora in corso di Amazon, con un raggio di azione non più limitato al *marketplace*, ma esteso al mercato delle spedizioni, dei film e della musica, per citarne solo alcuni. Un elemento che ha reso, e rende tutt'oggi difficile utilizzare le tradizionali regole antitrust nelle dinamiche del mondo digitale [26].

In sostanza, l'economia digitale rende più che mai necessario il passaggio a un approccio differente che consenta di garantire la certezza del diritto. Questo in virtù degli standard tradizionali che vengono applicati in ordine all'art. 102 TFUE, considerati eccessivamente laschi [27].

Nella sopracitata decisione della Commissione europea del 2019 la condotta che ha portato a un abuso ha riguardato la previsione di una clausola di esclusiva, ma sono diversi i casi in cui si potrebbe giungere a una ipotesi anticoncorrenziale nei mercati digitali tramite un abuso di posizione dominante derivante da una politica aziendale in materia di dati personali. Individuare quest'ultimo elemento non è meno difficoltoso di ciò che riguarda il mercato rilevante.

Ma, prima di individuare le fattispecie di abuso che si potrebbero

---

ropa.eu, in cui l'Autorità ha riconosciuto la loro interdipendenza. L'analisi del mercato rilevante dell'uno non può prescindere dall'analisi dell'altro.

[25] B. Jullien, A. Pavan, M. Rysman, *Two-sided Markets, Pricing, and Network Effects*, in *Toulouse School of Economics,* vol. 1238, 2021, 1, spec. 30.

[26] N. Petit, *Technology Giants, The "Moligopoly" Hypothesis and Holistic Competition: A Primer*, 2016, consultabile al sito www.SSRN.com

[27] M. Rato, N. Petit, *Abuse of Dominance in Technologyenabled Markets*, cit., 64. Secondo gli AA. è necessario il passaggio ad un approccio basato sugli effetti.

inquadrare, sorge l'esigenza di rintracciare il valore da assegnare ai dati personali, o meglio, al diritto a trattare i dati personali.

5. *La perdurante centralità del consenso che non produce un trasferimento di un diritto dominicale in favore del titolare del trattamento*

Come si è già avuto modo di vedere nel capitolo I, non è il dato personale in sé che sostituisce il corrispettivo monetario generando un processo di reificazione dell'interessato, bensì si verifica la concessione di un diritto al trattamento per determinate finalità che deve avvenire secondo le prescrizioni e i modi previsti dalla normativa. Non si produce un trasferimento del diritto di proprietà sul dato personale in capo al titolare del trattamento, ma ciò che rileva è che il controllo finale sia conservato dall'interessato attraverso l'esercizio di quei diritti che gli consentono di preservare la protezione dei dati personali nella sua sfera di diritto fondamentale [28]. La cornice normativa che consente il mantenimento di un controllo su come i propri dati personali vengono trattati è il fulcro della discussione. Non si tratterebbe del trasferimento di un diritto dominicale, né di attributi della personalità. Quello che rileva nell'ambito della circolazione, sia europea che transfrontaliera, concerne la concessione di un diritto secondo specifiche finalità.

Nel quadro di un controllo sul trattamento dei propri dati, delegabile finanche a terzi mediante gli schemi sanciti nel *Data Governance Act*, spicca su tutti il diritto alla portabilità dei dati (art. 20 GDPR), il quale consente di evitare fenomeni di *lock-in* e favorisce la circolazione dei dati. Un diritto che, per questo, è stato riaffermato e consolidato anche nelle ultime novità legislative, rafforzando così la sua pregnanza e la sua centralità.

Molti operatori, peraltro, hanno tentato - per alcuni anni con suc-

[28] Il riferimento è alla tesi ascrivibile a V. RICCIUTO, *La patrimonializzazione dei dati personali,* cit., 715.

cesso - di procedere a un trattamento dei dati personali che esula dal perimetro di esecuzione del contratto senza ottenere il consenso dell'interessato, ossia avvalendosi della base giuridica dell'interesse legittimo e seguendo una sua applicazione *sui generis*, poi definitivamente arrestata dalla Corte di Giustizia europea con la sentenza del 4 luglio 2023 (C-252/21).

Infatti, si è spesso fatto ricorso a tale base giuridica in virtù di quanto descritto nel considerando n. 47 del GDPR secondo cui si può configurare un legittimo interesse nel trattamento di dati personali per finalità di *marketing* diretto.

Ma quanto prospettato dal legislatore non è un automatismo ed è pur sempre necessario procedere con un test di bilanciamento tra l'interesse del titolare del trattamento e i diritti e le libertà dell'interessato, il quale costituisce una verifica da effettuarsi sulla base del principio di proporzionalità e trasparenza. In questa valutazione, come affermato dalla più recente giurisprudenza, vanno tenute in debita considerazione le aspettative dell'interessato rispetto al trattamento che il titolare intende eseguire (CGUE C-252/21, 4 luglio 2023) [29].

Quindi, oggi, come si è visto, si va affermando una nuova prassi, quella del «doppio binario» (*pay or consent*): si offre all'utente la scelta di prestare il consenso al trattamento dei dati per finalità di *marketing* oppure di procedere con il pagamento di un corrispettivo.

Si tratta di una pratica differente rispetto alle operazioni di *tying* (ammessa in dottrina e giurisprudenza) in cui l'unica alternativa possibile sarebbe quella di rifiutare di prestare il consenso senza, però, la possibilità di ricevere l'erogazione del servizio.

Il consenso, come base giuridica del trattamento, quindi, sebbene

[29] Si è visto, inoltre, che l'EDPB, il 27 ottobre 2023, ha adottato una decisione urgente e vincolante sul trattamento dei dati personali per la pubblicità comportamentale di Meta. Con questa decisione, l'Organismo ha incaricato il DPA irlandese affinché vengano adottate misure atte ad imporre un divieto di trattamento dei dati personali per la pubblicità comportamentale sulle basi giuridiche del contratto e dell'interesse legittimo in tutto lo Spazio economico europeo (SEE).

secondo molti commentatori abbia perso la sua centralità e costituirebbe un elemento non più confacente ai tempi odierni, andrebbe invece ritenuto il presupposto che consente all'interessato, se non coartato o ingannato, di esprimere appieno la propria libertà di scelta [30], anche in virtù di un principio di autoresponsabilità.

La perdurante centralità del consenso quale presupposto di determinate azioni e conseguenze è dimostrata dal suo richiamo anche nei più recenti interventi normativi come il DGA e il *Data Act*, oltre al DMA.

Pertanto, ciò di cui bisogna curarsi è che non ci siano elementi che rendano apparente tale libertà attraverso una effettiva applicazione dei principi che elidono quelle asimmetrie informative e quegli squilibri di potere che favoriscono il contraente più forte. In questo senso, la corretta applicazione dei principi di *privacy by design* e *by default* figurano come elementi essenziali.

Su questa linea, la prassi del *pay or consent* può astrattamente contribuire nel senso annunciato e può favorire la percezione del livello di *privacy* come elemento della qualità del servizio, determinante ai fini antitrust, ma allo stesso tempo può rendere fallace l'idea di consenso "libero". Si tratta di una prassi che si sta diffondendo ma sta creando dibattiti. Infatti, se da un punto di vista squisitamente giuridico possa apparire lecita e, quindi, praticabile per un *vulnus* normativo, il rischio è pur sempre quello di rendere la "privacy" un lusso per i più facoltosi. Ciò è, infatti, quanto può ricavarsi dal recente parere dell'EDPB, il quale si è espresso in senso critico.

---

[30] Come osservato in dottrina, già la "condizionalità" del consenso sta a significare una assenza di libertà nella sua prestazione ogni volta che v'è una pressione o influenza inappropriata sull'interessato che gli possa impedire di esercitare il suo libero arbitrio. In questi termini, A. ADDANTE, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali,* cit., 903.

6. *Il dibattito sul pay or consent*

La prassi del *pay or consent* ha dato alla luce un vivo dibattito che è recentemente confluito innanzi all'autorità giudiziaria europea.

Infatti, a seguito di questa pratica, attuata da vari prestatori nei diversi mercati digitali, è intervenuto l'EDPB con il parere n. 8 del 2024 esprimendosi in senso piuttosto negativo. A tale parere è seguita l'impugnazione da parte di Meta.

Nel parere i modelli del *pay or consent* vengono descritti come quei casi in cui un titolare del trattamento offre agli interessati una scelta tra almeno due opzioni per ottenere l'accesso a un servizio online fornito dal titolare del trattamento: l'interessato può acconsentire al trattamento dei propri dati personali per una finalità specifica, oppure «decidere di pagare un contributo e accedere al servizio online senza che i propri dati personali vengano trattati per tale finalità. Il presente parere si concentrerà sui modelli in cui è possibile prestare il consenso al trattamento dei dati personali per finalità di pubblicità comportamentale». L'EDPB, tra l'altro, ha analizzato la questione anche alla luce di quanto previsto dal *Digital Services Act* e dal *Digital Markets Act*. Quest'ultima normativa, invero, è piuttosto chiara sul punto allorché si tratti di pratiche realizzate da grandi operatori.

L'organismo, nel suo parere, si concentra sulla base giuridica del consenso e sulla validità di quest'ultimo. Sostiene che per le grandi piattaforme online, nella maggior parte dei casi, non è possibile soddisfare i requisiti per un consenso valido se collocano gli utenti di fronte a una scelta binaria tra il consenso al trattamento dei dati personali per scopi di pubblicità comportamentale e il pagamento un corrispettivo poiché i dati personali non possono essere equiparati a una *commodity*.

Perciò, nel parere viene sottolineato che l'alternativa che le grandi piattaforme online devono considerare di fornire agli interessati dovrebbe essere *equivalente* e non deve portare al pagamento di un compenso. L'ipotesi formulata è quella di una diversa forma di pubblicità che non è la pubblicità comportamentale ma una pubblicità "tradizionale".

Quindi, il 27 giugno 2024 Meta ha impugnato il parere dell'EDPB innanzi al Tribunale europeo chiedendo il suo annullamento (C/2024/4865 – Case T-319/24). Tra i sette motivi di ricorso viene contestato il mancato rispetto della sentenza della CGUE emessa nella causa riguardante proprio Meta (C-252/21), un ingiusto bilanciamento dei diritti fondamentali contrapposti creando una sproporzione con l'art. 16 della Carta, la violazione del principio di parità di trattamento ai sensi dell'art. 20 della Carta e l'introduzione di un nuovo e incoerente obbligo non presente nel GDPR riguardante la nozione di consenso e la minimizzazione dei dati.

La decisione sulla validità del modello in questione – a dir poco dubbia per i grandi operatori in virtù del DMA - sarà decisiva per l'intero quadro regolatorio, anche in un'ottica inerente al livello di *privacy* quale standard qualitativo del servizio offerto.

7. *Gli standard del trattamento dei dati personali come parametro per la qualità del prodotto digitale a tutela di una libera scelta dell'utente consapevole*

Dai casi analizzati nei capitoli precedenti si è potuto constatare che dalla violazione di disposizioni in tema di protezione dei dati potrebbero derivare conseguenze anche in tema di concorrenza.

Si potrebbero verificare, *inter alia*, abusi di dipendenza economica, concentrazioni illecite o abusi di posizione dominante. Le disposizioni in materia di *privacy* che hanno una loro centralità per il profilo di cui si discute sono senza dubbio quelle riguardanti la portabilità dei dati, oltre a quelle riguardanti la profilazione dell'interessato e le decisioni automatizzate (art. 22 GDPR). Sono, va da sé, fondamentali anche le norme che sanciscono i principi generali in materia di *data protection* e i presupposti di liceità del trattamento (artt. 5 e 6 GDPR).

Per tentare di definire un quadro ordinato dell'analisi che ci si prefigge, è necessario soffermarsi sulla *privacy* come elemento della qualità del servizio o prodotto digitale e, per questo scopo, è la consapevolezza della concessione del diritto al trattamento dei propri dati personali e del loro intrinseco valore economico che rende possibile rite-

nerlo una qualità del servizio prestato. Si è visto che è la stessa Corte di Giustizia che nel succitato caso riguardante la piattaforma LinkedIn ha rilevato come una incidenza antitrust sia ammissibile là dove i consumatori la percepiscano come un fattore di qualità del servizio e se le imprese concorrono anche in virtù di tale elemento.

La carenza di consapevolezza in questi termini impedisce che il trattamento dei dati possa costituire una dimensione della interazione tra le imprese in grado di essere regolata dalla concorrenza nel mercato dei servizi primari.

Allo stato attuale, come si è avuto modo di vedere, soprattutto nell'esame della disciplina che tutela i dati personali, tale consapevolezza non può considerarsi piena, rendendo perciò difficoltoso il rapporto tra la fornitura dei dati e il benessere dei consumatori, i quali spesso non percepiscono il loro valore.

A minare tale consapevolezza, va da sé, hanno contribuito condotte ingannevoli e scorrette da parte di alcune grandi imprese che commercializzavano i loro prodotti ponendo enfasi sulla loro *gratuità*, attraverso informazioni distorte, o del tutto omesse, sulle modalità di utilizzo dei dati personali degli utenti inerenti alle loro preferenze e ai contenuti da loro generati [31].

Alla luce di quanto emerso, e in linea astratta, perciò, si può ritenere che un'impresa dominante in un determinato mercato abusi della propria posizione ove realizzi pratiche opache, scorrette, discriminatorie o ingannevoli nel trattamento dei dati o nella prodromica descrizione del trattamento in questione.

Un simile scenario si può verificare in diversi casi. Basti pensare a quell'operatore che riesce a ottenere una rilevante quantità di dati personali degli utenti (finali o commerciali) grazie a una applicazione distorta dei principi di *privacy by design*, avvalendosi di *dark patterns,* i quali inducono l'utente medio a una scelta forviata proprio da una proget-

[31] Su questo aspetto, si è visto, si sono pronunciate le Autorità come la CGUE, C-252/21, cit., e l'AGCM (caso Facebook, 29 novembre 2018, n. 27432).

tazione della piattaforma che lo porta ad accettare un determinato trattamento dei dati personali che altrimenti non avrebbe prestato.

In casi di questo genere, la scelta dell'utente non potrebbe ritenersi effettivamente libera, andando così a pregiudicare il benessere dei consumatori.

L'ipotesi può essere estesa anche a una applicazione scorretta dei principi di *privacy by default*. Si può facilmente prospettare il vantaggio competitivo di quell'impresa che applica, con una impostazione predefinita nella piattaforma digitale, una politica di raccolta dei dati più invasiva rispetto a quel concorrente che rimette la scelta all'interessato predisponendo di *default* una opzione meno invasiva.

Ma un ragionamento di questo genere può essere esteso a un ventaglio di altre ipotesi come il caso della violazione o elusione del principio di minimizzazione dei dati, della limitazione delle finalità del trattamento, della proporzionalità, della trasparenza e del principio di conservazione e sicurezza dei dati, così come nel caso di utilizzo di una base giuridica inappropriata come nel caso che ha portato alla sentenza CGUE del 4 luglio 2023.

In questi scenari si dovrebbe ricomprendere anche l'eventuale elusione o violazione della normativa in materia di trasferimento dei dati verso Stati terzi. L'impresa dominante che elude le norme sulla circolazione transfrontaliera potrebbe avere un illegittimo vantaggio competitivo – riuscendo pertanto a valorizzare i dati raccolti o i "dati secondari" - se il paese terzo non prevede, ad esempio, parametri equivalenti a quelli europei in tema di conservazione o di sicurezza dei dati.

Casi di tal specie potrebbero realizzarsi in tutte quelle circostanze in cui non vengono applicate misure supplementari richieste dall'art. 46 GDPR e potrebbero porre le basi per effetti di rete suscettibili di creare barriere all'ingresso grazie a una qualità dell'offerta distorta a causa di pratiche opache o scorrette.

Si possono nondimeno verificare situazioni pregiudizievoli anche per tutte quelle ipotesi in cui non sia previsto un effettivo controllo dell'interessato sul trattamento dei propri dati come, ad esempio, l'i-

potesi in cui il paese terzo non preveda un rimedio processuale adeguato.

In un'ottica generale, ciò che si prospetta necessario, quindi, si traduce nella *trasparenza* a cui deve attenersi l'impresa. L'elemento primario è che l'impresa sia trasparente nei confronti dell'utenza in modo che questa sia in grado di valutare la qualità dell'offerta senza subire manipolazioni o coartazioni nella scelta, la quale deve essere realmente libera, anche perché assunta da un soggetto consapevole e reso, allora, responsabile delle proprie decisioni [32].

La trasparenza deve essere attuata attraverso una comunicazione che sia effettivamente chiara e intellegibile per il consumatore o utente. Solo in questo modo si può avere un *utente consapevole* e un *operatore meritevole* della sua posizione nel mercato in cui accede.

Il perimetro della scelta rimessa all'utente non può essere frutto di scelte arbitrarie dell'operatore digitale, ma si deve comunque adattare al tipo di servizio o prodotto offerto, alla sua qualità e alle sue finalità. Si tratta di valutazioni rimesse a una analisi caso per caso il cui bilanciamento di interessi e diritti non è agevole.

I casi che sono stati qui prospettati condurrebbero ad abusi escludenti per mezzo di effetti di rete e, come dimostrato nel caso della già citata acquisizione di LinkedIn, devono essere valutati in base alle circostanze del caso concreto. L'esistenza di tali effetti non indica di per sé un problema in termini concorrenziali. In un'ottica generale, occorre tener conto che la condotta di un'impresa finalizzata ad assumere un ruolo di *leadership* nell'ambito di un determinato settore di mercato non costituisce di per sé un abuso di posizione dominante ove non leda la libertà di azione delle imprese concorrenti [33].

---

[32] Se, ad esempio, per l'erogazione del servizio o prodotto digitale, fosse necessario estrarre dati secondari a mezzo di una specifica profilazione dell'utente che si avvale di algoritmi e di decisioni automatizzate, è indispensabile che quest'ultimo venga informato e possa adottare una libera scelta sulla base di un principio di autoresponsabilità.

[33] Cass. civ., Sez. I, 13 ottobre 2016, n. 20688, *Quotidiano Giuridico*, 2016.

I problemi di concorrenza, però, possono subentrare se, in caso di effetti di rete, essi precludano l'accesso ai concorrenti o rendano più difficile l'espansione della loro base di utenza [34]. Questo può verificarsi in quei casi in cui vi sia una applicazione errata della normativa in materia di dati personali tale da incidere sulla libertà di scelta del consumatore o dell'utente, determinando così una ripercussione negativa in un fattore di qualità del servizio. Nel caso LinkedIn, si è constatato come tali effetti di rete svolgevano un ruolo rilevante dal momento che i professionisti (utenti del servizio) tendono a trarre vantaggio dal fatto che un maggior numero di utenti si unisca alla rete e la utilizzi attivamente; il motivo sta nel fatto che ciò si tradurrebbe in un maggior numero di contatti professionali, di visualizzazioni del profilo e di opportunità lavorative [35]. Questo, però, nel caso analizzato dalla Commissione, non ha impedito di accertarne il rischio di effetti escludenti [36].

---

[34] In tal senso il documento M.8124 - Microsoft / LinkedIn del 6 dicembre 2016, § 342, consultabile al sito www.ec.europa.eu. La Commissione ha infatti affermato che: «*the existence of network effects as such does not a priori indicate a competition problem in the market affected by a merger. Such effects may however raise competition concerns in particular if they allow the merged entity to foreclose competitors and make more difficult for competing providers to expand their customer base. Network effects have to be assessed on a case-by-case basis*».

[35] *Ivi.*, § 341, dove si legge che: «*network effects occur when the value of a product or service for a customer increases when the number of other customers also using it increases. In the present case, network effects are likely to play an important role in light of the nature of PSN services. Indeed, professionals tend to benefit as more professionals join the network and use it actively, as this is likely to translate into a higher number of professional contacts, of profile views and of recruitment opportunities. The majority of respondents to the market investigation confirmed the importance of network effects for PSN services and submitted that the size of the user base is a very important parameter of competition in PSN services*».

[36] Nel caso concreto, la Commissione ha rilevato, al § 343, che sussistesse la probabilità che gli effetti di rete potessero escludere concorrenti di servizi analoghi già esistenti in alcuni paesi del SEE o di potenziali nuovi operatori. Tale conseguenza derivava, secondo la Commissione, dal fatto che l'aumento del numero di membri di LinkedIn, avrebbe indotto altri utenti a iscriversi generando attività sulla sua piattaforma in questione. Di contro, un numero sempre minore di utenti sarebbe stato

In un'ottica generale, perciò, le implicazioni che l'ambito del trattamento dei dati personali, o delle attività prodromiche al trattamento, possono generare implicazioni in materia di diritto della concorrenza, sfociando in abusi di posizione dominante, possono ricondursi a quella condotta abusiva tipizzata all'art. 3 L. 287/1990, la quale si traduce nell'impedire o limitare lo sviluppo tecnico o il progresso tecnologico a danno dei consumatori.

8. *Il nuovo quadro normativo europeo dei dati e dei mercati digitali introduce novità e consolida fattispecie previgenti*

L'impianto normativo europeo delineato negli ultimi anni, da un lato restituisce conferme e dall'altro introduce novità che rafforzano principi e strutture normative già esistenti. Tali novità normative, esposte nel capitolo IV, sono state suddivise in due parti:

la prima, afferisce al quadro normativo sulla «strategia europea per i dati»; la seconda, attiene al quadro normativo sul mercato digitale europeo.

In relazione al primo gruppo di norme, si scorge un intento confermativo, ed anzi, rafforzativo della funzione circolatoria e dell'accesso ai dati, valorizzandoli in quanto *asset* economico ormai essenziale. Con questi atti legislativi l'UE sembra voler in qualche modo ridurre lo svantaggio competitivo con altri Stati, da una parte, tutelando gli interessi e le libertà dei cittadini europei a fronte di normative di Stati terzi senz'altro più lasche in materia e, dall'altra, regolamentando un utilizzo dei dati personali ordinato e competitivo che possa incentivare in termini di innovazione.

La nuova normativa europea, oltre a promuovere l'accesso e la circolazione dei dati in un ambiente sicuro, tiene ferma la centralità del GDPR e rafforza la funzione essenziale del principio di trasparenza e della base giuridica del consenso, il quale, se libero e pieno, rimane

---

indotto a iscriversi a fornitori di servizi concorrenti, per la loro minore attrazione in termini di dimensioni delle loro reti e per le relative opportunità di lavoro.

l'elemento più confacente anche per i nuovi rapporti giuridici diffusi nella prassi.

Il presupposto del consenso, per la sua centralità, lo si ritrova anche nel secondo gruppo normativo, ovvero nel *Digital Markets Act*.

In questo regolamento, come si è visto, viene individuato il consenso quale strumento per gli utenti finali nel trattamento dei dati personali in caso di pubblicità online e viene poi posto l'accento sulla necessità di predisporre l'opzione del doppio binario, lasciando la libera scelta agli utenti finali.

Nel considerando n. 36 del DMA si prende infatti in considerazione la prassi delle grandi piattaforme di acquisire dati personali degli utenti finali per fornire servizi pubblicitari online quando gli utenti finali utilizzano siti web e applicazioni *software* di terzi. Questi ultimi, forniscono anche i dati personali dei loro utenti finali per avvalersi di determinati servizi offerti dai *gatekeeper* nel contesto dei loro servizi di piattaforma di base, come per esempio un "pubblico" personalizzato. Questo trattamento dei dati personali provenienti da terzi che utilizzano i servizi di piattaforma di base offre la possibilità di accumulare un gran numero di dati, realizzando barriere all'ingresso.

I vantaggi derivano anche dalla combinazione dei dati personali degli utenti finali raccolti da un servizio di piattaforma di base con i dati raccolti da altri servizi, dall'uso incrociato dei dati personali provenienti da un servizio di piattaforma di base in altri servizi offerti separatamente dalla piattaforma, oppure dall'accesso con registrazione degli utenti finali a diversi servizi del *gatekeeper* finalizzato a combinare i dati personali.

Perciò, è previsto che il *gatekeeper* è tenuto a consentire agli utenti finali una libera scelta, consistente nel seguire queste pratiche di trattamento dei dati e l'accesso con registrazione, offrendo però un'alternativa meno personalizzata ma equivalente. Tutto ciò senza che l'utilizzo della piattaforma di base sia subordinata alla prestazione del consenso dell'utente finale, il quale può essere negato [37]. Quindi, come si è

[37] Nel considerando n. 37 si legge poi che «l'alternativa meno personalizzata non

detto in precedenza, nel rapporto con il *gatekeeper,* e alla luce della disciplina dettata dal DMA, il modello del *pay or consent* appare una pratica discutibile, in linea con quanto già espresso dall'EDPB.

Anche qui, dunque, risalta la libera scelta dell'utente, la quale può assurgere a requisito della qualità del servizio prestato e che sorge da un corretto trattamento dei dati personali.

Lo scenario raffigurato, in ogni caso, non esclude la possibilità per la piattaforma di trattare i dati personali, o di far accedere con registrazione gli utenti finali a un servizio, in virtù della base giuridica che fa leva sull'adempimento di un obbligo legale, sulla salvaguardia di interessi vitali dell'interessato o di altra persona, oppure, sull'esecuzione di un compito di interesse pubblico. Il trattamento, però, non potrebbe avvenire in forza della base giuridica focalizzata sulla esecuzione di un contratto o in virtù di un interesse legittimo del titolare del trattamento.

Da ultimo, non per importanza, può ritenersi che anche l'impianto normativo del *Digital Services Act*, se disatteso o aggirato da un operatore potrebbe condurre a conseguenze in tema di concorrenza. L'esito potrebbe dipendere dal fatto che l'intera struttura del regolamento si focalizza sulla elisione, o comunque, riduzione, di contenuti illegali dal web. La violazione di alcuni obblighi e divieti sanciti nel DSA, là dove comportino ripercussioni negative sulla "qualità dell'offerta" e qualora incida sul benessere dei consumatori, sarebbe in grado di riflettersi negativamente anche in termini di competitività.

---

dovrebbe essere differente o di qualità inferiore rispetto al servizio fornito agli utenti finali che prestano il proprio consenso, a meno che il deterioramento della qualità non sia una conseguenza diretta del fatto che il *gatekeeper* non possa procedere al trattamento dei dati personali o fare accedere con registrazione gli utenti finali a un servizio (...)». Quindi, anche in questo caso, è il legislatore stesso che pone in evidenza - come si è tentato di descrivere nei paragrafi precedenti per finalità antitrust - la differenza esistente tra le situazioni in cui un determinato trattamento dei dati sia necessario per la qualità del servizio o per l'erogazione *tout court* del servizio rispetto al caso in cui tale operazione non sia necessaria.

9. *L'utilizzo dell'algoritmo nel trattamento dei dati personali. Il caso Mevaluate*

A rendere ancor più articolato il tessuto normativo in tesi si inserisce l'uso delle nuove tecnologie. Per rendere tangibili le questioni a cui ci si riferisce si possono riportare alcuni recenti casi.

Un primo caso, riguardante il trattamento dei dati personali per mezzo di un algoritmo, è stato oggetto di un travagliato processo, giunto per due volte innanzi alla Suprema Corte di Cassazione e definito nel 2023 [38].

La vicenda in questione riguarda l'associazione Mevaluate che si prefigge lo scopo di creare la prima rete di reputazione democratica. In altri termini, l'associazione mira alla realizzazione di una comunità di associati in cui questi possano ricevere la definizione di un proprio *rating* reputazionale sulla base di elementi oggettivi. Il *rating* costituisce il risultato di una elaborazione algoritmica ad esito di una procedura di acquisizione di specifici dati personali dell'interessato.

In seno al processo che ha visto l'associazione impugnare il provvedimento sanzionatorio del Garante per la protezione dei dati personali è emerso il tema del principio di trasparenza che deve essere rispettato allorché il titolare del trattamento si avvalga di un algoritmo [39].

La Cassazione ha stabilito che, in casi di tal genere, il consenso dell'interessato può ritenersi valido allorché sia espresso in riferimento a specifiche informazioni sulle finalità e sulle modalità del trattamento, incluse le modalità del procedimento che coinvolgono l'algoritmo, non occorrendo, invece, una informativa con un linguaggio matematico e informatico.

---

[38] Cass. civ., sez. I, 10 ottobre 2023, n. 28358, *La nuova Giurisprudenza Civile Commentata*, n. 2, 2024, 402, nota di BRUTTI; per un commento della sentenza cfr. altresì F. CEREA, *Trattamento algoritmico dei dati a fini reputazionali tra consenso dell'interessato e controllo ex ante di conformità al GDPR e all'AI Act*, in *Responsabilità civile*, n. 6, 2023, 2005.

[39] In considerazione del periodo in cui si sono svolti i fatti, *ratione temporis*, quindi, si discettava in merito agli artt. 13 e 23 del D.lgs. n. 196/2003.

Nella sua ordinanza, la Cassazione ha precisato che un algoritmo «è un procedimento di risoluzione di un problema: da determinati dati di ingresso (input) derivano soluzioni (output). Lo "schema esecutivo" di un algoritmo specifica, pertanto, i passi da eseguire in sequenza, per giungere al risultato»[40]. Perciò, ha stabilito che ciò che rileva è che l'interessato possa conoscere l'algoritmo inteso come procedimento affidabile per ottenere un certo risultato o risolvere un certo problema e che sia descritto in modo univoco e dettagliato, capace di portare al risultato in un tempo finito. Nell'ordinanza, al par. 4.3 si aggiunge che «il procedimento, come spiegato con i termini della lingua comune, sia altresì idoneo ad essere tradotto in linguaggio matematico è tanto necessario e certo, quanto irrilevante: ed invero, non è richiesto nè che tale linguaggio matematico sia osteso agli utenti, nè, tanto meno, che essi lo comprendano».

A questo principio si è giunti a seguito della cassazione della sentenza del Tribunale di Roma n. 5715 del 4 aprile 2018, la quale non aveva analizzato il funzionamento dell'algoritmo per il calcolo del *rating*, concentrandosi sulla circostanza che sarebbe stato "il mercato" a stabilire l'efficacia del risultato e del servizio prestato. La Cassazione ha stabilito, infatti, che ciò che rileva non è la risposta del mercato, bensì la validità del consenso prestato dall'interessato e il requisito della consapevolezza da parte dell'interessato non è soddisfatto se lo schema esecutivo dell'algoritmo e gli elementi che lo compongono restano ignoti o non conoscibili[41]. Il caso è poi giunto nuovamente in-

[40] In questo senso, sempre Cass. civ., sez. I, 10 ottobre 2023, n. 28358, § 4.2. La definizione di algoritmo e, dall'altro, quella di sistema di intelligenza artificiale è un tema piuttosto spinoso che apre altresì all'applicabilità dell'*Artificial Intelligence Act* (Reg. UE 2024/1689). Sul punto, sia consentito il rinvio a G. Proietti, *Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico*, cit., 882.

[41] Cass. civ., sez. I, 25 maggio 2021, n. 14381, in *Diritto dei Servizi Pubblici.it*, 2021. L'ordinanza ha sancito il seguente principio: «in tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di

nanzi al Tribunale di Roma che si è pronunciata con la sentenza n. 9995 del 22 giugno 2022, nuovamente cassata nel 2023 con la sentenza sopra riportata [42].

A conferma di quanto sostenuto nei precedenti paragrafi, come si può notare, il principio di trasparenza e la base giuridica del consenso hanno ricoperto un ruolo centrale anche in questa vicenda.

Nel processo che ha interessato il caso non è stato affrontato il tema delle decisioni basate unicamente su un trattamento automatizzato (art. 22 GDPR), anche perché ha riguardato la disciplina previgente al GDPR. Il tema, però, ha interessato la vicenda che ha portato alla già citata sentenza Schufa della CGUE.

9.1 *Il caso "Schufa" (CGUE C-634/21). Ancora sullo scoring algoritmico, anche alla luce del regolamento europeo sull'intelligenza artificiale*

Con la sentenza "Schufa", la Corte di Giustizia europea ha stabilito altri principi sul tema riguardante il trattamento dei dati personali mediante algoritmi finalizzato all'elaborazione di un punteggio (*score*). La vicenda origina dall'attività resa dalla omonima società tedesca che offre ai propri partner contrattuali le informazioni sul merito creditizio di terzi [43]. In particolare, come si legge nella sentenza, si tratta di un

---

una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati».

[42] Il Tribunale di Roma ha ritenuto non sufficiente, in termini di trasparenza, la descrizione dell'algoritmo di Mevaluate poiché non sarebbe fornita alcuna spiegazione sulla incidenza specifica e sulle modalità con cui interagiscono i fattori presi in considerazione nell'ottenimento del risultato (il rating reputazionale). Tale ragionamento è stato censurato dalla Cassazione la quale ha sottolineato come la descrizione del sistema non deve essere così ampia e precisa da riguardare l'intero processo seguito dall'algoritmo.

[43] Sentenza CGUE, C-634/21, 7 dicembre 2023, *Schufa*, curia.europa.eu.

servizio attraverso il quale viene stabilito «un pronostico sulla probabilità di un comportamento futuro di una persona («score»), come il rimborso di un prestito, a partire da alcune caratteristiche di tale persona, sulla base di procedure matematiche e statistiche. Il calcolo dei punteggi («scoring») si basa sul presupposto che assegnando una persona a un gruppo di altre persone con caratteristiche comparabili che si sono comportate in un certo modo, si può prevedere un comportamento analogo» [44].

Il fulcro della decisione ha portato essenzialmente all'enunciazione dei seguenti tre principi:

(i) il significato di «decisione» (automatizzata) di cui all'art. 22 GDPR è sufficientemente ampia da ricomprendere al suo interno anche il risultato inerente al calcolo della solvibilità dell'interessato quale tasso di probabilità in relazione alla capacità di tale soggetto di adempiere ai futuri pagamenti;

(ii) il calcolo automatizzato di un tasso di probabilità fondato sull'elaborazione di dati personali che riguardano la capacità di una persona di onorare futuri prestiti rientra nella definizione di «profilazione» di cui all'art. 4, n. 4, GDPR;

(iii) l'elaborazione algoritmica di uno *score* sulla futura solvibilità dell'interessato incide in modo significativo sulla decisione del terzo (ad esempio, concedere o meno un finanziamento) e, quindi, è in grado di incidere in modo significativo sulla persona dell'interessato ai fini di quanto previsto all'art. 22 GDPR.

La Corte di giustizia rileva, inoltre, che in uno schema che coinvolge tre soggetti come è il caso analizzato, non si potrebbe sostenere una interpretazione restrittiva dell'art. 22 GDPR secondo il quale il calcolo del tasso di probabilità deve essere considerato solo un atto preparatorio rispetto alla decisione che compete al terzo. Infatti, se così fosse, in assenza di una decisione da parte di chi fornisce il "tasso di probabilità", l'interessato non sarebbe legittimato a esercitare il proprio diritto di accesso (art. 15, par. 1, lett. h, GDPR) nei suoi confron-

[44] *Ivi*, § 14.

ti. Inoltre, anche considerando l'atto adottato dal terzo nell'ambito di applicazione dell'art. 22, par.1, GDPR, egli «non sarebbe in grado di fornire tali informazioni specifiche in quanto generalmente non ne dispone» [45].

La sentenza, infine, fornisce indicazioni anche in merito alle misure appropriate che è necessario attuare ai sensi del par. 3 dell'art. 22 GDPR. Viene, perciò, operato un rinvio anche al considerando n. 71 a mente del quale tali misure devono ricomprendere l'obbligo di utilizzare «procedure matematiche o statistiche appropriate per la profilazione, di metter in atto misure tecniche e organizzative adeguate al fine di garantire 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 impedire, tra l'altro, effetti discriminatori nei suoi confronti». Queste misure includono «quantomeno il diritto dell'interessato di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione adottata nei suoi confronti» [46].

In Germania, su questo tema, una recente sentenza ha stabilito che un punteggio elaborato da una società rientra nell'ambito di applicazione dell'art. 22 GDPR solo nel caso in cui sia stato l'unico criterio utilizzato nel processo decisionale [47].

Nel dedalo normativo europeo il tema dello *scoring* algoritmico deve essere coniugato anche con quanto previsto nel regolamento sull'intelligenza artificiale (*AI Act* - Reg. UE 2024/1689). Alla lett. c) del suo art. 5 è vietata la pratica di immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o

---

[45] *Ivi*, § 63.

[46] *Ivi*, § 66.

[47] *LG Traunstein, Endurteil*, 22.05.2024 – 6 O 2465/23, consultabile al sito www.gesetze-bayern.de

della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità. Nel considerando n. 31 dell'*AI act* viene precisato che i sistemi di IA che permettono ad attori pubblici o privati di attribuire un punteggio sociale alle persone fisiche possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano le persone fisiche o i gruppi di persone fisiche sulla base di vari punti di dati riguardanti il loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note, inferite o previste nell'arco di determinati periodi di tempo. Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. I sistemi di IA che comportano tali pratiche inaccettabili di punteggio aventi risultati pregiudizievoli o sfavorevoli dovrebbero pertanto essere vietati. Tale divieto non dovrebbe pregiudicare le pratiche lecite di valutazione delle persone fisiche effettuate per uno scopo specifico in conformità del diritto UE e nazionale.

Sebbene sia discutibile, tra i primi commenti alla normativa non manca chi ritiene che alcune pratiche e sistemi di *credit scoring* in ambito finanziario e assicurativo possano rientrare nel divieto in questione, così come i *reputation system* nel settore della *sharing economy*, in particolare per l'ambito dei trasporti e delle telecomunicazioni [48].

[48] F. P. Levantino, I. Neroni Rezende, *Rischio inaccettabile: usi proibiti*, in O. Pol-

Nelle linee guida elaborate dalla Commissione europea sulle pratiche vietate ai sensi dell'*AI Act*, in riferimento all'art. 5, lett. c), viene menzionato proprio il caso "Schufa" come ipotesi di "valutazione" (intesa come "profilazione") suscettibile di rientrare nel divieto in questione se ricorrono anche le altre condizioni previste [49]. Tale valutazione deve essere, ovviamente, effettuata caso per caso. Va da sé che l'ipotesi citata dalla Commissione potrebbe rientrare nel divieto poiché è stata accertata una violazione, *rectius*, una falsa applicazione dell'art. 22 GDPR.

Infatti, qualora la pratica fosse conforme al GDPR, il divieto non impedirebbe la messa a punto di pratiche lecite e volte a valutare le persone per scopi specifici, legittimi e conformi al diritto dell'Unione e nazionale; in particolare, quando queste normative specificano i dati rilevanti per tali scopi della valutazione e garantiscono che qualsiasi trattamento pregiudizievole o sfavorevole risultante per le persone sia giustificato e proporzionato.

Questo dato è confermato dalle stesse linee guida elaborate dalla Commissione europea nelle quali viene proprio specificato che il *credit scoring* e il *risk scoring* sono aspetti essenziali di alcuni servizi resi da imprese finanziarie e assicurative. Queste pratiche, così come altre pratiche legittime (ad esempio, quelle volte al miglioramento della qualità e dell'efficienza dei servizi, per garantire una gestione più efficiente dei sinistri, per effettuare valutazioni specifiche dei dipendenti, per la prevenzione e l'individuazione delle frodi, per l'applicazione della legge o per la valutazione del comportamento degli utenti sulle piattaforme online), non sono di per sé vietate, se lecite e intraprese in linea con l'*AI Act* e con il diritto europeo e nazionale applicabile [50]. Infine,

---

LICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Milano, Giuffrè, 2025, 171.

[49] *Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, 4 febbraio 2025, 53, consultabile al sito www.digital-strategy.ec.europa.eu

[50] *Commission Guidelines on prohibited artificial intelligence practices,* cit., 61-61. Nelle linee guida vengono poi riportati nove esempi di pratiche che si rivelerebbero lecite e, quindi, non andrebbero a ricadere nel divieto. Il primo esempio riguarda proprio i

ancorché ovvio, ma contrastante col principio di neutralità tecnologica professato, va puntualizzato che, affinché possa operare qualsivoglia divieto sancito nell'*AI act* è necessario vi sia l'utilizzo di un sistema di IA così come definito nella normativa in questione.

9.2 *Il diritto di accesso ai dati personali e la nozione di informazioni significative sulla "logica utilizzata" nell'ambito di un processo decisionale automatizzato. Il caso "Dun & Bradstreet" (CGUE C-203/2022)*

Un altro importante diritto dell'interessato, sancito nel GDPR, è quello di accesso ai propri dati personali. Un diritto che, per logiche sistematiche, non è stato trattato in apertura insieme agli altri diritti e obblighi previsti dalla normativa europea e che si lega (come si è visto nel caso Schufa) anche con l'art. 22 GDPR.

L'art. 15 GDPR garantisce all'interessato il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati personali e a una serie di informazioni [51]. Tra queste informazioni, la

---

sistemi di *credit scoring* finanziario utilizzati dai creditori o da agenzie di informazioni creditizie per valutare il merito del credito finanziario o i debiti insoluti di un cliente, fornendo un punteggio di credito o determinando la valutazione del suo merito di credito, i quali si basano sul reddito e sulle spese del cliente e su altre circostanze finanziarie ed economiche. Queste pratiche esulano dall'ambito di applicazione dell'art. 5, par. 1, lett. c), *AI Act* se rilevano per uno scopo legittimo perseguito con il *credit scoring* e se vengono rispettate le leggi sulla protezione dei consumatori che specificano il tipo di dati e le garanzie necessarie poste a garanzia di un trattamento equo dei consumatori nella valutazione del merito di credito.

[51] Al considerando n. 63 del GDPR si legge che l'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 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

lett. h) indica espressamente «l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato» [52]. Questo diritto, nell'architettura del rapporto tra il titolare del trattamento e l'interessato, acquisisce un peso determinante, anche per risvolti di natura concorrenziale, oltre che puramente contrattuali, generando un vero e proprio obbligo in capo al primo.

Il dibattito che si genera, quindi, si incentra sul delineamento di ciò che si intende con «informazioni significative sulla logica utilizzata» nell'ambito di un processo decisionale automatizzato, soprattutto allorché si discetti di processi decisionali elaborati tramite algoritmi tecnicamente sofisticati e, conseguentemente, sul corretto bilanciamento con i diritti e gli interessi di altri soggetti.

Il tema è recentemente affiorato con il caso "Dun & Bradstreet" (CGUE C-203/2022), oggetto di una recente pronuncia della Corte di giustizia [53].

Il caso origina da un contenzioso instaurato in Austria tra un con-

---

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».

[52] Le altre informazioni che ha diritto di ottenere sono: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine.

[53] CGUE, C-203/2022, 27 febbraio 2025, *Dun & Bradstreet Austria GmbH*, eurlex.europa.eu

sumatore e la società Dun & Bradstreet (D&B) incentrato sul fatto che il primo si è visto negare la conclusione di un contratto di telefonia mobile a causa dell'esistenza di un rischio di insolvibilità ricavato da valutazioni fornite dalla D&B, la quale non avrebbe dato sufficienti informazioni sulla logica utilizzata nel processo decisionale (algoritmico) di cui si è avvalsa.

La logica sottesa all'ottenimento delle informazioni previste alla lett. h) dell'art. 15 GDPR è collegata all'esercizio anche dei diritti previsti all'art. 22 GDPR [54]. In altri termini, affinché l'interessato possa esercitare i propri diritti, è necessario che abbia un'effettiva contezza della logica interna utilizzata nel processo decisionale da parte del titolare del trattamento. Per i diritti di cui all'art. 22 GDPR, in particolare, il riferimento coinvolge l'ottenimento di un intervento umano, l'espressione di una propria opinione e la contestazione della decisione assunta.

Nel processo austriaco dal quale è stato disposto il rinvio alla CGUE è stato nominato un consulente tecnico per stabilire le informazioni che la società sarebbe tenuta a comunicare all'interessato.

Sono state, quindi, individuate le seguenti informazioni minime: a) i dati personali trattati nell'ambito della determinazione dei fattori; b) le parti essenziali dell'algoritmo su cui si fonda il processo automatizzato, inclusa la formula matematica in cui possono essere inserite le informazioni per il calcolo del *rating* e la spiegazione comprensibile di tutti i valori utilizzati nella formula; c) le informazioni che consentono di stabilire la correlazione tra i dati trattati e la valorizzazione compiuta.

Le conclusioni dell'avvocato generale evidenziano il fatto che le informazioni che devono essere rese ai sensi dell'art. 15 GDPR devono tenere in debita considerazione anche il contesto nel quale i dati sono oggetto di un trattamento automatizzato e la complementarità tra il

[54] Sul diritto di accesso dell'interessato collegato all'esercizio dei suoi diritti, si veda la decisione CGUE, C-487/21, 4 maggio 2023, *Österreichische Datenschutzbehörde*, eur-lex.europa.eu

concetto di "significativo" con il carattere "comprensibile" delle informazioni fa sì che le informazioni da fornire devono essere non solo chiare e accessibili, ma accompagnate da spiegazioni tali da permettere una loro adeguata comprensione [55]. L'interessato deve essere in grado di verificare l'esattezza dei dati, oltre alla coerenza e al nesso causale tra il metodo e i criteri utilizzati con il risultato che viene generato. Dunque, ancora una volta emerge in tutta la sua rilevanza il più volte citato principio di trasparenza.

La Corte di giustizia si è espressa ritenendo infatti che l'art. 15, par. 1, lett. h), GDPR deve essere interpretato nel senso che, in caso di processo decisionale automatizzato, l'interessato può pretendere dal titolare del trattamento, a titolo di «informazioni significative sulla logica utilizzata», che quest'ultimo gli spieghi, mediante informazioni pertinenti e in forma concisa, trasparente, comprensibile e facilmente accessibile, la procedura e i principi concretamente applicati per utilizzare, con mezzi automatizzati, i dati personali relativi a tale interessato al fine di ottenerne un risultato determinato, come un profilo di solvibilità.

L'intera ricostruzione non deve portare a ritenere che il titolare del trattamento sia tenuto a divulgare informazioni che presentano un livello di complessità tale da non essere comprese da soggetti che non possiedono conoscenze tecniche adeguate [56].

L'altro profilo rilevante della vicenda riguarda la portata effettiva del diritto di accesso in un'ottica di bilanciamento con la protezione dei segreti commerciali e con i diritti di terzi in considerazione del fatto che la protezione dei dati non costituisce una prerogativa assoluta ma deve essere contemperata con altri diritti [57].

---

[55] Conclusioni dell'avvocato generale J. R. De La Tour, 12 settembre 2024, C-203/2022, § 61-67, curia.europa.eu.

[56] *Ivi*, § 72-74. Nel successivo § 75, invece, si sottolinea come la complessità del processo decisionale non possa costituire una scusante per non fornire informazioni all'interessato.

[57] Al considerando n. 4 del GDPR si legge che «Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce

In questo difficile contemperamento di diritti e di interessi in gioco per il caso in questione l'avvocato generale propone uno strumento già consentito dalla Corte per altri casi [58]. Il riferimento è alla possibilità di comunicare le informazioni potenzialmente lesive di interessi altrui all'autorità di controllo o all'organo giurisdizionale competente affinché si possano ponderare gli interessi in gioco e stabilire la portata del diritto di accesso da riconoscere all'interessato [59]. La Corte, infatti, si esprime proprio in questo senso [60]. Una soluzione di questo

---

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». Al considerando n. 63 del GDPR si legge che il diritto di accesso «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». Il limite costituito dai diritti e dalle libertà altrui è poi sancito a chiare lettere all'art. 15, par. 4, GDPR.

[58] CGUE, C-268/21, 2 marzo 2023, *Norra Stockholm Bygg*, eur-lex.europa.eu

[59] cfr. conclusioni avvocato generale, cit., § 93-95.

[60] La Corte di giustizia con la citata pronuncia del 27 febbraio 2025 ha stabilito a tal riguardo che «Nell'ipotesi in cui il titolare del trattamento ritenga che le informazioni da fornire all'interessato conformemente a tale disposizione contengano dati di terzi protetti da tale regolamento o segreti commerciali, ai sensi dell'articolo 2, punto 1, della direttiva 2016/943 (UE) del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, detto titolare è tenuto a comunicare tali informazioni asseritamente protette all'autorità di controllo o al giudice competenti, cui spetta ponderare i diritti e gli interessi in gioco al fine di determinare la portata del diritto di accesso dell'interessato previsto all'articolo 15 di tale regolamento». Per completezza, l'art. 2,

genere, tuttavia, deve essere rapportato anche in virtù del sistema giuridico e processuale del singolo Stato membro il quale, come nel caso italiano, prevede garanzie di contraddittorio piuttosto rigorose e di garanzia.

Quest'ultima controversia, quindi, ha le sue peculiarità poiché coinvolge ulteriori questioni su cui non ci si è focalizzati nel volume ma rende evidente, ancora una volta, che l'intero sistema, sebbene ormai complesso e bisognoso di un'importante opera di coordinamento, si fonda sul principio di trasparenza. Tale principio è il primo e fondamentale presupposto che può consentire all'interessato una libera scelta.

---

punto 1, della direttiva (UE) 2016/943 citato dalla CGUE stabilisce la definizione di segreto commerciale includendo: «informazioni che soddisfano tutti i seguenti requisiti: a) sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; b) hanno valore commerciale in quanto segrete; c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete».

BIBLIOGRAFIA

ACQUISTI A., *l'economia della privacy*, in *Il codice del trattamento dei dati personali*, in D'ORAZIO R., RICCIUTO V. (a cura di), Torino, 2007

ADDANTE A., *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *giustizia civile*, 4/2020

AFFERNI G., *Digital Services Act e Digital Markets Act*, L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), Milano, Giuffrè, 2023

AINIS M., *L'Autorità Antitrust alla prova dei mercati digitali*, in *dir. inf. e inform.*, 1/2022

ALPA G., *Quale modello normativo europeo per l'intelligenza artificiale?*, in *Contratto e impresa*, 4/2021

ALPA G., *Amazon in Tribunale*, in *Contratto e impresa*, n 4/2024

ALPA G., *Aspetti della nuova disciplina delle vendite nell'Unione europea*, in *Contratto e impresa*, 3/2019

ALPA G., *La proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati: riflessioni sul GDPR,* Cedam*,* 5/2019

ALPA G., *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021

ALPA G., *Il diritto di essere se stessi*, Milano, 2021

ALPA G., *Sul potere contrattuale delle piattaforme digitali*, in *Contratto e Impresa*, 3/2022

AMMANNATI L.*, La circolazione dei dati: dal consumo alla produzione*, in *Riv. Trim. dir. economia*, 4/2020

AMMANNATI L., *Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?*, in *Riv. Trim. dir. economia*, 1/2019

ANANTHARAMAIAH K. B., *YouTube Analytics Using Google Data Studio*, 2020, ssrn.com

ASTONE M. A., *Digital services act e nuovo quadro di esenzione dalla respon-*

sabilità dei prestatori di servizi intermediari: quali prospettive?, in *Contratto e impresa*, 4/2022

AULINO L., *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come un rimedio ex ante*, in *Dir. inform.*, 2/2020

BAKER S., '*How Can the U.S. Respond to Schrems II?'*, *Lawfare,* 2020

BAGNOLI V., *The big data relevant market*, in *Conc. e mercato*, n. 23/2016

BARENGHI A., *Osservazioni sulla nuova disciplina delle garanzie nella vendita di beni di consumo*, in *Contratto e impresa*, 2/2020

BASHENHOF P., *The digital Markets act (DMA): A Procompetitive Recalibration of Data Relations?*, in *Journal of Law, Technology and Policy*, 2022

BASSINI M., *La rilettura giurisprudenziale della disciplina sulla responsabilità degli* Internet service provider. *Verso un modello di responsabilità "complessa"?*, in *federalismi.it*, n. 3/2015

BASUNTI C., *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *contratto e impresa*, 2/2020

BELLOMIA V. – FONSI G., *comm. Articolo 1*, in *Dalla* Data Protection *alla* Data Governance*: il Regolamento (UE) 2022/868*, *Commentario al* Data Governance Act, A. MORACE PINELLI (a cura di), Pisa, 2024

BELLOMIA V., *comm. Articolo 2*, in *Dalla* Data Protection *alla* Data Governance*: il Regolamento (UE) 2022/868*, *Commentario al* Data Governance Act, A. MORACE PINELLI (a cura di), Pisa, 2024

BENEKE F., MACKERODT M. O., *Remedies for algorithmic tacit collusion*, in *Jour. Antitrust Enforcement*, 2020

BEYLEVELD A., SUCKER F., *Cross-border data flows in Africa: policy considerations for the afcfta protocol on digital trade,* 2022

BIANCA C.M.*, Diritto civile*, Milano, 1993

BOLOGNINI L., *Il trasferimento dei dati verso paesi terzi o organizzazioni internazionali*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il Regolamento privacy europeo*, Milano, 2016

BONINI P., *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in *Federalismi.it*, 11/2020

BORGHI M., *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, 2/2018

BORGOGNO O., *Regimi di condivisione dei dati e interoperabilità: il ruolo e la*

disciplina delle A.P.I., in *Il diritto dell'informazione e dell'informatica*, 3/2019

Bravo F., *Rating reputazionale e trasparenza dell'algoritmo. Il caso «Mevaluate»*, in *Dir. inform.*, 6/2021

Bravo F., *Le cooperative di dati*, in *Contratto e impresa*, 3/2023

Bravo F., *Lo scambio dei dati personali nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 1/2019

Bravo F., *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?,* in *Contratto e impresa,* 1/2018

Bravo F., *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018

Bravo F., *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in Contratto e impresa Europa, 1/2021

Bravo F., *EU Data Cooperatives, l'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, 2024

Burgess M., *Europe's Move Against Google Analytics Is Just the Beginning*, WIRED, 2022, wired.com

Buttarelli G., *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale dir. amministrativo*, 1/2023

Caggia F., *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. Dir. Comm.*, 3/2019

Calia D., *Schrems II: the EU's influence on U.S. data protection and privacy laws, in Washington University Global Studies Law Review*, 21/2022

Caloiaro L. A., *Il prezzo personalizzato, il consumatore e le insidie del mercato digitale*, Torino, 2024

Camardi C., *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust. Civ.*, 3/2019

Canepa A., *I mercati digitali*, Torino, Giappichelli, 2020

Carnovale P., *La funzione sinallagmatica del trattamento dei dati personali nella fornitura di servizi digitali,* in *giustiziacivile.com,* 10/2021

CATALANO F., *Il diritto alla portabilità de dati tra interessi individuali e prospettiva concorrenziale*, in *Europa e diritto privato*, 3/2019

CEREA F., *Trattamento algoritmico dei dati a fini reputazionali tra consenso dell'interessato e controllo ex ante di conformità al GDPR e all'AI Act*, in *Resp. civ.*, 6/2023

CERQUITELLI T, QUERCIA D., PASQUALE F., *Trasparent Data Mining for Big and Small Data*, New York, 2017

CHANDER A., *Is data localization a Solution for Schrems II?,* in *Journal of International Economic Law,* 23*,* 3/2020

CHOROMIDOU A., *EU data protection under the TCA: the UK adequacy decision and the twin GDPRS,* in *International Data Privacy Law*, Vol. 11, 4/2021

CHURCHES G. – ZALNIERIUTE A., *"Contracting Out" Human rights in International Law: Schrems II and The Fundamental Flaws of U.S. Surveillance Law*, in *Harvard International Law Journal Online*, 2020

CLARKE L., *After a Year of Limbo a EU-US Data Privacy Agreement Still Hangs in the Balance*, in *Tech Monitor,* 2021, techmonitor.ai

COCUCCIO M., *Dimensione "patrimoniale" del dato personale e tutele risarcitorie*, in *dir. di famiglia e delle persone*, 1/2022

CODIGLIONE GIANNONE G., *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transazionale dei dati personali*, in *dir. inf. e inform.*, 4-5/2015

COLANGELO M., *La regolazione ex ante delle piattaforme digitali: analisi e spunti di riflessione sul regolamento sui mercati digitali*, in NLCC, 2/2023

COMANDÉ G., *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e resp.*, 1/2022

CREMONA E., *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in *Osservatorio sulle fonti*, 2/2021

CRISPI A., *Sicurezza nazionale e diritti fondamentali alla luce della giurisprudenza UE in materia di tutela dei dati personali*, in *Riv. Ital. Dir. Pubbl. Comunitario*, 5/2017

CUFFARO V., *Il diritto europeo sul trattamento dei dati*, in *Contratto e impresa*, 3/2018

CZUBIK A., *"The right to Privacy" by S. Warren and L. Brandeis – The story*

of a Scientific Article in the United States, *Journal of American Studies* 17 (2016)

Davola A. – Malgieri G., *Data-Powerful. Un'indagine sulla nozione di potere e il suo rapporto con la vulnerabilità nel mercato digitale*, in *Concorrenza e mercato*, 1/2022

D'Alberti D., *Google e le nuove autorità private: la metamorfosi dal fatto al diritto*, in *Riv. dir. civ.*, 4/2021

D'Ippolito G., *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. il caso dell'uso secondario di big data*, in *Dir. inform.*, 6/2018

D'Ippolito G., *Commercializzazione dei dati personali: dato personale tra approccio morale e negoziale*, in *Dir. inform.*, 3/2020

D'Ippolito G., *Data economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata*, in *Media Laws*, 2/2023

D'Ostuni, Beretta, *Il diritto della concorrenza in Italia*, Torino, 2021

De Franceschi A., *Il pagamento mediante dati personali*, in *I dati personali nel diritto europeo*, AA. VV., *I dati personali nel diritto europeo*, Cuffaro, D'Orazio, Ricciuto (a cura di), Torino, 2019

De Franceschi A., *La circolazione dei dati personali tra privacy e contratto,* Napoli, 2017

Dell'Utri M., *Principi generali e condizioni di liceità del trattamento dei dati personali*, in AA. VV., *I dati personali nel diritto europeo*, Cuffaro V., D'Orazio R., Ricciuto V. (a cura di), Torino, 2019

Del Vicario M. – Bessi A. – Zollo F. – Quattrociocchi W., *The spreading of misinformation online*, in PNAS, Vol. 13, 3/2016

Denozza F., *Il progetto teorico dell'analisi economica del diritto antitrust e il suo fallimento, in 20 anni di antitrust – L'evoluzione dell'Autorità Garante della Concorrenza e del Mercato*, (a cura di) C. Rabitti Bedogni, P. Barucci, Torino, 2010

Di Majo A. – Inzitari B., *Obbligazioni alternative*, in Enc. Dir., XXIX, Milano, 1979

Di Porto F., *La rivoluzione big data. Un'introduzione*, in *Concorrenza e Mercato*, n. 23/2016

DRECHSLER L, *Comparing LED and GDPR Adeguacy: One Standard Two Systems*, in *Global privacy law review*, vol. 1, 2/2020

DRECHSLER L, KAMARA I., *Essential equivalence as a benchmark for international data transfers after Schrems II*, in *Research Handbook on EU data protection law*, 2022

EBERS M., *Regulating AI and Robotics: Ethical and Legal Challenges*, in *Cambridge University Press*, 2019

ECONOMIDES N., LIANOS I., *Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective*, in *Journal of Competition Law and Economics*, Forthcoming, NET Institute Working, 2021

ECONOMIDES N., LIANOS I., *Antitrust and Restrictions on Privacy in the Digital Economy*, in *Concurrences Review*, 2020

EDWARDS L., VEALE M., *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, 2017

ESPOSITO F., *Dove sono i miei dati? Privacy e reificazione nell'era digitale*, in *Etica & Politica / Ethics & Politics*, 1/2021

FABER S., *Does the GDPR Allow for the Use of Consent for the International Transfer of Data?,* in *National Law Review,* Vol. IX, 2022

FAILLACE S., *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*, 4/2022

FALCE V., *L'abuso di dipendenza economica nel digitale. Perché no?*, in *Filodiritto*, 2022

FALCE V., *Appunti sul regolamento europeo sul geo-blocking e la neutralità geografica. In cammino verso il mercato unico digitale,* in *Contratto e impresa*, 4/2019

FALCE V., *Piattaforme ed ecosistemi digitali. Scelte pro-concorrenziali*, in *riv. dir. industriale*, 4-5-6/2022

FARAONE N. M., *Della serie "a volte ritornano" (o non se ne sono mai veramente andati): il principio del ne bis in idem alla prova delle piattaforme digitali*, in *federalismi.it*, 6/2023

FELICI S., *La tutela dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo: brevi riflessioni introduttive, in Mercato unico digitale,*

dati personali e diritti fondamentali, F. Rossi Dal Pozzo (a cura di), *Eurojus*, fasc. speciale, 2020

Ferri G.B., *Persona e privacy*, in *Persona e formalismo giuridico*, Rimini, 1987

Filippelli M., *La collusione algoritmica*, in *Orizzonti del Diritto Commerciale*, Fasc. Sp., 2021

Finocchiaro G., *Il principio di accountability*, in *Giur. It.*, 12/2019

Finocchiaro G., *Considerazioni su intelligenza artificiale e protezione dei dati personali*, in *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021

Finocchiaro G., *Responsabilità delle piattaforme e tutela dei consumatori*, in *Giornale di diritto amministrativo*, 6/2023

Floridi L., *Infosfera. Etica e filosofia nell'età dell'informazione,* Torino, 2009

Franzoni M., *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in *Jus civile*, 1/2021

Franzoni M., *Lesione dei diritti della persona e tutela della privacy*, in *XXVI lezioni di diritto dell'intelligenza artificiale*, Ruffolo (a cura di), Torino, 2021

Frosini T. E., *Le sfide attuali del diritto ai dati personali*, in *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020

Galli F., *La pubblicità mirata al tempo dell'intelligenza artificiale: quali regole a tutela dei consumatori?*, in *Contratto e Impresa*, 3/2022

Gallo P., *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. Dir. civ.*, 6/2022

Geraci A., *Condotta anticoncorrenziale e perimetrazione del mercato rilevante*, in *dir. industriale*, 6/2015

Giordano G., *Il Digital Markets Act e la centralizzazione dei poteri in capo alla Commissione europea: quale ruolo per le Autorità antitrust nazionali?*, in *Comparazione e diritto civile*, 3/2022

Giorgianni M., *Art. 20 – diritto alla portabilità dei dati*, in *Commentario del codice civile*, Milano, 2019

Giuliano M., *Dati personali, consenso e privacy nell'era digitale: sfide legali e implicazioni negoziali*, in *giustiziacivile.com*, 5/2023

Goodman M., Flaxman S., *European Union Regulations on algorithmic de-*

cision-making and a "right to explanation", in *AI Magazine*, vol 38, 3/2017

GRAEF I., HUSOVEC M., PURTOVA N., *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German Law Journal,* vol. 19, 6/2019

GRAZZINI B., *Piattaforme e content moderation - Fake news e disinformazione*, in *Giur. It.*, 2/2024

GRECO L., MANTELERO A., *Industria 4.0, robotica e privacy by design*, in *Dir. inform.*, 6/2018

GRÖGER G.**,** *There Is No AI Without Data*, in *Communications of the ACM*, Vol 64, 11/2021

GUIDOTTI R., MONREALE A., RUGGIERI S., PEDRESCHI D., TURINI F., GIANNOTTI F., *Meaningful Explanations of Black Box AI Decision System, Proceedings of the AAAI Conference on Artificial Intelligence, 33(01), 9780-9784,* 2019

GUIDOTTI R., MONREALE A., RUGGIERI S., PEDRESCHI D., TURINI F., GIANNOTTI F, *Local Rule-Based Explanations of Black Box Decision Systems*, in arXiv:1805.10820, 2018

GUZZARDI G., *L'abuso di posizione dominante nel mercato dei servizi digitali*, in NGCC, 2/2023

HARRINGTON J. E., *Developing Competition Law for Collusion by Autonomous Artificial Agent*, in *14 Jour. Comp. L. & Econ.*, 2018

ITTOO A., PETIT N., *Algorithmic pricing agents and tacit collusion: A technological perspective*, *TILEC discussion Paper*, Vol. 54, 2010

KERBER W., *Digital Markets, data and a privacy: competition law, consumer law and data protection*, in *MAGKS Joint Discussion Paper Series in Economics*, 14/2016,

KOCHELEK D. M., *Data Mining and Antitrust*, 22 *Harv. J.L. & Tech.*, 2009

KOKOTT J., SOBOTTA C., *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, vol. 3, n. 4/2013

KUNER C., *Reality and illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal*, vol. 18, 4/2017

IANNOTTI DELLA VALLE A., *Il digital Markets Act e il ruolo dell'unione europea verso un costituzionalismo digitale*, in *Giur. costituzionale*, 3/2022

Irti C., *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021

Irti N., *L'età della decodificazione*, Milano, 1989

Ittoo A., Petit N., *Algorithmic Pricing Agents and Tacit Collusion: A Technological Perspective*, in *L'intelligence artificielle et le droit, Hervé Jacquemin and Alexandre De Streel (eds), Bruxelles: Larcier,* 2017

Iuliani A., *Note minime in tema di trattamento dei dati personali*, in *Europa e diritto privato*, 1/2018

Jones M. L., Kaufman E. – Edenberg E., *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy*, 2018

Jullien B., Pavan A., Rysman M., *Two-sided Markets, Pricing, and Network Effects*, in *Toulouse School of Economics,* 1238/2021

Jurcys P., Compagnucci M. C., Fenwick M., *The Future of International Data Transfers: Managing New Legal Risk with a 'User-Held' Data Model*, in *the Computer Law and Security Review*, Vol. 46, 2022

Landi A., *I fornitori di servizi di intermediazione molto grandi*, in *Digital Services Act e Digital Markets Act,* L. Bolognini - E. Pelino - M. Scialdone (a cura di), Milano, 2023

La Rosa M. V., *Lo scopo della regolamentazione*, in *Digital Services Act e Digital Markets Act*, L. Bolognini - E. Pelino - M. Scialdone (a cura di), Milano, 2023

Lener R., *Tecnologie e attività finanziaria*, in *Il trattamento dei dati tra etica, diritto ed economia, Atti del XIV Convegno nazionale della Società Italiana degli Studiosi del Diritto Civile*, Napoli, ESI, 2020

Lener S.M., *Diritto alla deindicizzazione - La domanda di deindicizzazione e le interferenze tra la Dir. 2000/31 e il Reg. 2016/679*, in *Giur. It.*, 3/2022

Levantino F. P., Neroni Rezende I., *Rischio inaccettabile: usi proibiti*, in *La disciplina dell'intelligenza artificiale*, in (a cura di), O. Pollicino - F. Donati - G. Finocchiaro - F. Paolucci, Milano, 2025

Libertini M., *Abuso del diritto e abuso di posizione dominante*, in *Orizzonti del diritto commerciale*, 3/2018

Libertini M., *Digital markets and competition policy. Some remarks on the suitability on the antitrust toolkit*, in *Orizzonti del Diritto Commerciale*, fasc. Sp., 2021

LIBERTINI M., *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *riv. Trim. dir. pubblico*, 4/2022

LICASTRO A., *Il* self-preferencing *come illecito antitrust?*, in *Il diritto dell'economia*, 2/2021

LIEBER R., CHANEY K., *Google Analytics*: *Analyzing the Latest Wave of Legal Concerns for Google in the US and the EU*, in *Buffalo Intellectual Property Law Journal*, 7/2010

LIONELLO L., *La creazione del mercato europeo dei dati: sfide e prospettiva,* in *Riv. Comm. Int.*, 3/2021

LITMAN J., *Information Privacy/Information Property*, in *SSRN Scholarly Paper* n. ID 218274, Rochester, NY, 2000

LLOYD I., *Moving UK Data Protection Law Away from EU Standards – Legislative Focus Areas in 2022 — New Directions Forward or Steps Backwards in UK Data Protection and Digital Information Bill?,* in *Computer Law Review International,* 6/2022

LUBIN A., *'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,* in *Chicago Journal of International Law*, Vol. 18, 2/2018

LUCANTONI P., *Strumenti digitali e finanza*, in *Banca d'Italia, Quaderni di ricerca giuridica n. 87*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, 2019

LYNSKEY O., *Aligning data protection right with competition law remedies? The GDPR right to data potability,* in *European Law Review*, 2017

MAGGIOLINO M., *I Big Data e il diritto antitrust*, Milano, 2018

MALGIERI G. – COMANDÉ G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7, in *International Data Privacy Law*, 4/2017

MANGANELLI A., *La condivisione dei dati fra rimedi antitrust, privacy e regolazione pro-concorrenziale: un bilanciamento dinamico e cooperativo*, in *Concorrenza e mercato*, 1/2022

MANGINI V., OLIVIERI G., *Diritto Antitrust*, Torino, 2000

MANNONI S., STAZI G., *Is Competition a Click Away*?, Napoli, 2018

MANTELERO A., *Privacy*, in *Contratto e impresa*, 3/2008

Mantelero A., *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007

Manzini P., *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, in AISDUE, III, 2021

Marino G., *Internet e tutela dei dati personali: il consenso ai cookie*, in *Jus civile,* 2/2020

Martinelli S., *Il parere dell'EDPS sulla tutela dei diritti fondamentali nell'era dei Big Data*, in *Quot. Giur.,* 11/2018

Martìnez A. R., *The DMA's Ithaca: Contestable and Fair Markets*, in *World Competition* 46, n. 4/2023

Mastracci M., *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La Comunità int.*, 4/2016

Mazur Z., *Il dato personale nella disciplina del mercato e della concorrenza l'esperienza tedesca*, in V. Ricciuto, C. Solinas (a cura di), *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali,* III, Milano, 13/2022

Meneghetti M. C., *L'adeguatezza dei trasferimenti di dati personali negli USA, anche alla luce del nuovo Regolamento privacy,* in *giustiziacivile.com*, 9/2017

Mersack A. A., *Right of Privacy – Civil Rights Law,* 50, 51, St. John's Law Review, Vol. 9, 1/2014

Messinetti R., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998

Michinelli A., *L'interazione del DSA con altre regole sui servizi digitali*, in *Digital Services Act e Digital Markets act,* L. Bolognini, E. Pelino, M. Scialdone (a cura di), Milano, 2023

Michinelli A., *La gestione dei contenuti: illegali e non, la loro moderazione*, in *Digital Services Act e Digital Markets Act,* (a cura di) L. Bolognini, E. Pelino, M. Scialdone (a cura di), Milano, 2023

Midiri M., *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in *Dir. inform.*, 2/2021

Midiri M., *I Signori del Tech e la sfida sulle regole: il caso Amazon*, in *federalismi.it*, 28/2023

Miller A., *What Do We Worry About When We Worry About Price Discri-*

mination? The Law and Ethics of Using Personal Information for Pricing, 19 *J. Tech. L. & Pol'y*, 2014

S. MILLS, *Finding the 'nudge' in hypernudge*, in *Technology in Society*, Vol. 71, 2022

MIRABELLI G., *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 2/1993

MIRONE M., MARTORANA M., *I diritti dell'interessato*, in *GDPR e decreto legislativo 101/2018*, (a cura di) M. MARTORANA, Padova, 2019

MOBILIO G., *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in *federalismi.it*, 16/2020

MONGA G., *Responsabilità degli intermediari. Il Digital Services Act*, in M. Maggiore (a cura di), *Il commercio elettronico*, Torino, 2024

MONTELEONE A. G., *Il diritto alla portabilità dei dati. Tra diritti della personalità e diritti del mercato*, in *Luiss Law Review*, 2/2017

MONTERIN A., *Dell'incertezza nei trasferimenti di dati personali verso gli Stati Uniti*, in NGCC, 1/2021

MONTEROSSI M. W., *La tutela dell'utente commerciale nei mercati digitali*, in *Contratto e impresa*, 3/2021

MOROZOVAITE V., *The future of anticompetitive self-preferencing: analysis of hypernudging by voice assistant under article 102 TFEU*, in *European Competition Journal*, Vol. 19, 3/2023

MUSCOLO G., *Big data e concorrenza: quale rapporto?*, in V. Falce, G. Ghidini, G. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018

NASO N. M., *Abusi di posizione dominante (Anno 2021)*, in *Concorrenza e mercato*, 1/2022

NEWMAN N., *Search, Antitrust, and the Economics of the Control of User Data*, in Yale J. on Reg. Vol. 31/2014.

O'NEIL C., *Weapons of math destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016

OLIVIERI G., *Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali*, in *Orizzonti del Diritto Commerciale*, fasc. speciale, 2021

OPPO G., *Sul consenso dell'interessato*, in AA. VV., *Trattamento dei dati e tutela della persona*, (a cura di) Cuffaro, Ricciuto e Zeno-Zencovich, Milano, 1998

Pagliantini S., *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies – 135 vicies ter c.cons.*, in *NLCC*, 6/2022

Pagliantini S., *L'interferenza ascosa tra GDPR e diritto dei consumatori: appunti per una tassonimia*, in *Giur. It.*, 10/2023

Parenzo B.*, Sull'importanza dl dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali "gratuiti"*, in *dir. fam.*, 2/2021

Pariser E., *The filter bubble: What the internet is hiding from you*, London, 2011

Pasquale F., *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015

Pasquale F., *Privacy, Antitrust, and Power*, 20 *George Mason Law Review*, 2013

Patti S., *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 2/1999

Pellecchia E., *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *NLCC*, 5/2018

Pelleriti S., *La tutela dell'utente ai tempi di Facebook*, in *Algoritmi, Big Data, piattaforme digitali*, Torino, 2021

Peraro C., *Quando la violazione della privacy costituisce un illecito antitrust: quali rimedi nell'ordinamento UE?,* in *Eurojus*, 3/2023

Perel M - Elkin-Koren N., *Accountability in Algorithmic Copyright Enforcement,* in *Tech. L. Rev.*, 2016

Perlingieri P., *L'informazione come bene giuridico*, in *Rass. Dir. civ.*, 1990

Petit N., *Technology Giants, The "Moligopoly" Hypothesis and Holistic Competition: A Primer*, SSRN, 2016

Petrone L., *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 3/2023

Pierucci A. M., *Elaborazione dei dati e profilazione delle persone*, in AA. VV., *I dati personali nel diritto europeo*, Cuffaro, D'Orazio, Ricciuto (a cura di), Torino, 2019

Morace Pinelli A., *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *NGCC*, 6/2022

PIRAINO F., *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. It.*, 12/2019

PIRAINO F., *La responsabilità dei prestatori di servizi di condivisione di contenuti online*, in NLCC, 1/2023

PITRUZZELLA G., *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, 1/2016

PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018

PODDIGHE E. - ZENO-ZENCOVICH V., *La «correttezza» nelle condizioni generali di contratto delle grandi piattaforme online*, in *Comparazione e diritto civile*, 1/2024

POLETTI D., *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. It.*, 12/2019

POLETTI D., *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2/2023

POLETTI D., *Gli intermediari dei dati, in EJPLT*, 1/2022

POLLICINO O., *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider,* in *Percorsi Costituzionali*, n. 1/2014

POPOLI A. R., *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *dir. inform.*, 6/2019

PRINCIPATO A., *Verso nuovi approcci alla tutela della privacy:* privacy by design *e* privacy by default settings, in *Contratto e impresa Europa*, 1/2015

PROIETTI G., *La pubblicità nell'era delle nuove tecnologie*, in aa.vv. *Diritto e intelligenza artificiale*, G. Alpa (a cura di), Pisa, 2020

PROIETTI G., *Una normativa per l'intelligenza artificiale. La proposta di regolamento europeo*, in *Riv. Trim. resp. d'impresa e autoriciclaggio*, 2/2021

PROIETTI G., *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in *Contratto e impresa*, 3/2022

PROIETTI G., *Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un quadro sistematico,* in *Contratto e Impresa,* n. 3/2024

PROPP B., SWIRE P., *After Schrems II: A Proposal to Meet the Individual Redress Challenge,* in *lawfare.com*, 2020

PURPURA A., *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data*, in *Jus civile*, 4/2022

Rato M – Petit N., *Abuse of Dominance in Technology-enabled Markets: Established Standards Reconsidered?,* in *European Competition Journal*, Vol. 9, 2013

Raul A. C., *Why Schrems II Might Not Be a problem for EU-U.S. Data transfers*, *Lawfare*, 21 Dec. 2020

Resta G., *Contratto e diritti fondamentali*, in D'Amico (diretto da), *Enc. Dir., I tematici, Contratto*, Milano, 2021

Resta G., *Diritti esclusivi e nuovi beni immateriali*, Torino, 2011

Resta G., *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. Trim. dir. pubblico*, 4/2022

Resta G., Zeno- Zencovich V., *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ.*, 2018

Resta G., Zeno- Zencovich V., *La protezione transnazionale dei dati personali*, in *Consumatori e mercato*, Roma, 2016

Resta G., *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679*, in *Annuario del contratto*, 2018

Ricci A., *Introduzione al regolamento europeo sull'accesso equo e sul loro utilizzo*, in *NLCC*, 4/2024

Riccio G. M. – Pezza F., *Portabilità dei dati e interoperabilità*, in *I dati personali nel diritto europeo*, Torino, 2019

Riccio G. M., Pezza F., *Trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali*, in Tosi (a cura di) *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019

Riccio G. M., *Model Contractual Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in *Dir. inf. e inform.*, 4-5/2015

Ricciuto V., *L'equivoco della privacy*, Napoli, 2022

Ricciuto V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inform.*, 4/2018

Ricciuto V., *Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali,* V. Ricciuto e C. Solinas (a cura di), III, Milano, 13/2022

Roberts T., Mohamed Ali A., Farahat M., Oloyede R. Mutung'u

G., *Surveillance Law in Africa: a Review of Six Countries*, Brighton: *Institute of Development*, 2021, ssrn.com

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995

ROMANO B., *Civiltà dei dati libertà giuridica e violenza*, Torino, 2020

RUBINSTEIN I. – MARGULIES P., *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the search for Common Ground*, in *Connecticut Law Review*, Vol. 54, 4/2022

RUGGERI F., *Poteri privati e mercati digitali*, Roma tre-press, 2023

SAFJAN M., *Areas of application of the Charter of fundamental rights of the European Union: fields of conflict?,* in *EUI Working Paper*, 22/2012

SALOP S. C., *Question: What is the Real and Proper Antitrust Welfare Standard? Answer: The True Consumer Welfare Standard*, 22 Loy. *Consumer L. Rev.* 336, 2009

SCIALDONE M., *Digital Services Act e Digital Markets Act*, L. Bolognini, E. Pelino, M. Scialdone (a cura di), Milano, 2023

SCIASCIA G., *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale di diritto amministrativo*, 3/2021

SENIGAGLIA R., *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2/2020

SEVIGNANI S., *The Problem of Privacy in Capitalism and Alternative Social Media: The Case of Diaspora*, in C. Fuchs, V. Mosco (eds.), Marx in *the Age of Digital Capitalism*, Brill, Leiden/Boston, 2016

SHAFFER K., *Data versus Democracy: How big data Algorithms Shape Opinions and Alter the Course of History*, Colorado, 2019

SHELANSKI H. A., *Information, Innovation, and Competition Policy for the Internet,* in *University of Pennsylvania Law Review,* Vol. 161, 2013

SCHMITZ A. J.*, Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots*", 2014 *Mich. St. L. Rev.*

SICA S., *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001

SICA S., *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in *La nuova disciplina europea della privacy*, Milanofiori Assago, 2016

Sileoni S., *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Milano, Cedam, 2011

Simeone G., *Machine learning e tutela della Privacy alla luce del GDPR*, in *Diritto e intelligenza artificiale*, Alpa (a cura di), Pisa, 2020

Solinas C., *Autonomia privata e regolazione pubblica nel trattamento dei dati personali,* Bari, 2022

Solinas C., *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in *Giur. It.*, 2/2021

Solinas C., *La circolazione dei dati personali nell'ottica dello scambio tra diritti*, in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali,* V. Ricciuto e C. Solinas (a cura di), III, Milano, 13/2022

Somaini L., *The right to data portability and user control: ambitions e limitations*, in *Rivista di diritto dei media*, n. 2/2018

Stazi A., Corrado F., *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inform.*, 2/2019

Stucke M., Grunes A., *Big Data and Competition Policy*, in *Oxford University Press*, 2016

Tabarrini C., *Comprendere la "big mind": il gdpr sana il divario di intelligibilità uomo-macchina?*, in *dir. inform.*, 2/2019

Terolli E., *Privacy e protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *dir. inf. e inform.*, 1/2021

Thépot F., *Market Power in Online Search and Social Networking: A Matter of Two-Sided Markets*, in *World Competition, Kluwer Law International*, Vol. 36, 2/2013

Thobani S., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media laws*, 3/2019

Tosi E., *Diritto privato delle nuove tecnologie digitali*, Milano, 2021

Troiano S., *Il diritto alla portabilità dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019

Vacchi A., *Intelligenza artificiale, impresa e nuovi modelli di business*, in *XXVI lezioni di diritto dell'intelligenza artificiale,* Ruffolo (a cura di), Torino, 2021

Van Der Sloot B., Van Schendel S., *Ten Questions for Future Regulation*

of Big Data: A Comparative and Empirical Legal Study, in *Journal of intellectual Property, Information Technology and E-Commerce Law*, 2016

VAN LOO R., *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. Pa. L. Rev., Vol. 163, 2015

VERSACI G., *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020

VERSACI G., *Consenso al trattamento dei dati personali e* dark patterns *tra opzionalità e condizionalità*, in *NLCC*, 5/2022

VOSS W., *Transatlantic Data Transfer Compliance*, in *B.U. J. Sci. & Tech. L.*, 28/2022

WACHTER S., MITTELSTADT B., FLORIDI L., *Why a Right to explanation of automated decision-making does not exist in the general data protection regulation*, 7, in *International Data Privacy Law*, 2/2017

WARREN S., BRANDEIS L., *The right to privacy,* in *Harvard Law Review*, 5/1890

WEISS R., MEHROTRA A. K., *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, *Va. J.L. & Tech.*, Vol. 11, 6/2001

WILKINSON S., *UK data protection and digital information bill explained*, in *Journal of Data Protection & Privacy*, Vol. 5, 3/2022

ZALNIERIUTE M., *Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security*, in *Vanderbilt Journal of Transnational Law*, vol. 55, 1/2022

ZARSKY T., *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, vol. 47, 4, 2017

ZENO-ZENCOVICH V., *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in MediaLaw, 2/2018

ZENO-ZENCOVICH V., GIANNONE CODIGLIONE G., *Ten Legal Perspectives on the 'Big Data Revolution'*, in *Concorrenza e mercato*, 23/2017

ZENO-ZENCOVICH V., *Una lettura comparatistica della L. 675/96 sul trattamento dei dati personali*, in CUFFARO V., RICCIUTO, ZENO-ZENCOVICH V. (a cura di) T*rattato dei dati personali e tutela della persona*, Milano, 1998

ZITTRAIN J., *History of Online Gatekeeping*, in *Harvard J. Of Law & Tech.*, 2006

ZOPPINI A., *L'informazione come bene, I problemi dell'informazione nel diritto*

civile, oggi, in M. D'Auria (a cura di), Studi in onore di V. Cuffaro, Roma-Tre-Press, 2022

Zuboff S., *Il Capitalismo della sorveglianza*, Roma, 2019

INFORMATION TECHNOLOGY LAW

Series Editors Fabio Bravo *and* Angelo Giuseppe Orofino

1. Stefano Faillace, *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS* (2025)
2. Daniele Marongiu, *Algoritmi e diritti. Trasparenza, non-discriminazione e proprietà degli output dell'intelligenza artificiale* (2025)
3. Giuseppe Proietti, *Tutela e valorizzazione dei dati nei mercati digitali. Il contratto, la concorrenza e i nuovi soggetti tutelati* (2025)

This volume analyses the right to the protection of personal data and its application in digital markets. It investigates the interplay between issues arising under contract law, competition law and the protection of new legal entities. Employing an interdisciplinary methodology, this work explores the systemic tensions between the protection of individual rights and market dynamics, proposing interpretative approaches aimed at enhancing the value of data while maintaining a sound balance.

The work provides a systematic overview of the intricate European regulatory framework governing data and digital markets through the analysis of the main sources (regulations, directives, national legislation) and the examination of issues addressed in legal literature and case law.

In particular, it covers recent European legislation, including the GDPR, the Digital Markets Act, the Digital Services Act, the Data Governance Act and the Data Act, highlighting the pressing need for systematic coordination of this increasingly complex regulatory maze, which risks undermining legal certainty.

5 000002 690068
9 788813 388317
€ 42,00 I.V.A. INCLUSA