



## **Quando la violazione della privacy costituisce un illecito antitrust: quali rimedi nell'ordinamento UE?**

DI CINZIA PERARO\*

Sommario: 1. Premessa. – 2. Il contesto normativo UE: tra RGPD, regole antitrust e DMA. – 3. La violazione della privacy come elemento dell'illecito antitrust. – 4. I possibili rimedi. – 4.1. Rimedi di *public enforcement*. – 4.2. *Private enforcement* e ricorsi collettivi. – 4.3. Rimedi e trasferimento extraeuropeo dei dati. – 5. Considerazioni conclusive.

1. Il termine “privacy” viene oggi riferito indistintamente al concetto di riservatezza, normalmente connesso alla sfera personale, o a quello di dati personali in quanto tali, riconducibili ai concetti comunemente noti di bene oppure di diritti della personalità<sup>1</sup>. Nell'ordinamento europeo non si rinviene una definizione di privacy, ma compare quella di dato personale<sup>2</sup>, astratta da qualsiasi categorizzazione tradizionalmente operata negli

---

\* Ricercatore a tempo determinato di diritto dell'Unione europea, Università degli Studi di Bergamo.

<sup>1</sup> Il presente lavoro sviluppa le riflessioni svolte nell'ambito del convegno «L'equivoco della privacy. Persona vs dato personale» tenutosi il 14 ottobre 2022 presso l'Università degli Studi di Bergamo. Nel prosieguo si utilizzerà il termine “privacy” in senso generico, per fare riferimento ai dati personali, a prescindere da una precisa categorizzazione, tenuto conto che l'analisi si concentrerà sul trattamento illecito dei dati e dei possibili rimedi a tutela dei diritti dei soggetti interessati in quanto titolari di quei dati. Sul significato da attribuire alla nozione di privacy, si veda, per tutti, V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, p. 15 ss.

<sup>2</sup> Cfr. art. 4, punto 1) del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - RGPD), in *GUUE*, L 119 del 4 maggio 2016, pp. 1-88, la definizione di “dato personale”, in base al quale deve intendersi «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

ordinamenti interni<sup>3</sup>. Ciò che rileva ai fini della regolamentazione delle operazioni che hanno ad oggetto i *data*, nonché per la determinazione dei rimedi azionabili, è infatti il loro trattamento<sup>4</sup>, uso o sfruttamento. Non è in discussione il fatto che ai dati personali viene riconosciuto un valore economico *de facto*<sup>5</sup>, sempre più al centro dell'economia digitale, dove si sono sviluppati modelli di monetizzazione dei dati con cui acquisire informazioni relative ai consumatori e agli utenti in generale<sup>6</sup>, e tale da confermare l'idea della patrimonializzazione dei dati. Sono i diritti dei titolari dei dati che vengono in rilievo in caso di trattamento incompatibile con la normativa applicabile, non rilevando invece la protezione dei dati stessi<sup>7</sup>. È il fenomeno del trattamento dei dati in sé che viene regolato e che deve essere contestualizzato nelle varie dinamiche del mercato, con riguardo al loro utilizzo e alle relative finalità<sup>8</sup>.

L'approccio adottato dall'Unione europea nei confronti dei dati personali, in termini di protezione dei relativi diritti a fronte di usi illeciti, si inserisce nel contesto più ampio che comprende la disciplina rilevante al fine di garantire il buon funzionamento del mercato interno in tutte le sue dimensioni, compresa quella digitale, dando luogo a un *corpus* normativo che governa la "quinta" libertà di circolazione, quella dei dati personali. La necessità di tutelare i soggetti interessati dall'uso dei relativi dati personali nasce infatti nelle situazioni di sfruttamento economico, laddove tale uso sia volto a perseguire finalità di rilevanza economica e quindi di competitività<sup>9</sup>. La protezione delle persone con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale<sup>10</sup> riconosciuto nell'art. 8, par. 1, della Carta dei

---

<sup>3</sup> Il RGPD «prescinde da ogni qualificazione delle situazioni giuridiche soggettive»: V. RICCIUTO, *L'equivoco della privacy*, cit., p. 147.

<sup>4</sup> Per "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, punto 2) del RGPD.

<sup>5</sup> Sulla concezione dei dati personali nell'ambito degli scambi contrattuali, v. V. RICCIUTO, *L'equivoco della privacy*, cit., p. 166 ss., nonché S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – Rivista di Diritto dei Media*, 2019, n. 3, pp. 131-147.

<sup>6</sup> V. RICCIUTO, *L'equivoco della privacy*, cit., p. 76 s.

<sup>7</sup> In tal senso, vedi art. 1 del RGPD, ai sensi del quale: «1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. 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».

<sup>8</sup> Sullo sviluppo della normativa UE in tema di dati e ruolo delle imprese, v. R. CAFARI PANICO, *Le imprese multinazionali, la protezione dei dati nello spazio cibernetico e l'efficacia extraterritoriale del diritto dell'Unione europea*, in *Papers di diritto europeo*, 2021, n. 1, pp. 7-43, reperibile al sito Internet [www.papersdirittoeuropeo.eu](http://www.papersdirittoeuropeo.eu).

<sup>9</sup> Per un inquadramento della tutela dei dati personali in relazione al diritto della concorrenza, v. M. MAGGIOLINO, *Il rapporto tra il diritto antitrust e la tutela dei dati personali*, in V. FALCE (ed.), *Competition law enforcement in digital markets*, Torino, 2021, pp. 227-234; i contributi di A. COLAPS, *Garantire la protezione dei diritti fondamentali nel mercato unico digitale: verso un approccio sinergico tra il diritto della concorrenza e la protezione dei dati*; A. SAJA, *Protezione dei dati personali, tutela del consumatore e concorrenza: un rapporto in evoluzione*, in F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, in *Eurojus*, fascicolo speciale, luglio 2020; M. WASASTJERNA, *Competition, Data and Privacy in the Digital Economy: Towards a Privacy Dimension in Competition Policy?*, Alphen aan den Rijn, 2020; R. CAFARI PANICO, *L'identità digitale quale diritto del cittadino dell'Unione, fra tutela dei dati personali e concorrenza*, in AA.VV., *Temi e questioni di diritto dell'Unione europea. Scritti offerti a Claudia Morviducci*, Bari, 2019, pp. 815-840.

<sup>10</sup> Per un'analisi ricostruttiva del diritto fondamentale in questione, sia consentito il rinvio a C. PERARO, *Legittimazione ad agire di un'associazione a tutela dei consumatori e diritto alla protezione dei dati personali a*

diritti fondamentali dell'Unione europea (nel prosieguo, "Carta") e nell'art. 16, par. 1, TFUE, quest'ultimo base giuridica del regolamento (UE) 2016/679.

Di fronte ai casi di sfruttamento dei dati personali che comportano sia una violazione della privacy, per l'illegittimità del trattamento, sia un illecito antitrust, commesso tramite tale uso illegittimo dei dati e in violazione delle norme poste a tutela della concorrenza, per abuso di posizione dominante oppure in quanto pratica commerciale scorretta, la normativa europea rilevante predispone strumenti di protezione attivabili sia come *public* che come *private enforcement*. Sono azioni che possono svolgersi in modo parallelo, con diversi fondamenti giuridici e con diversi esiti, e che, in ogni caso, tra loro si intersecano, dovendo prendere in considerazione quanto statuito nei rispettivi procedimenti, indagini o giudizi, per evitare esiti discordanti.

Il presente lavoro intende quindi ricostruire, in breve, il quadro normativo e il sistema di rimedi rilevanti nelle situazioni poc'anzi accennate, per poi proporre alcune osservazioni critiche alla luce della giurisprudenza della Corte di giustizia e della casistica interna che si è sviluppata nel quinquennio dall'entrata in applicazione del RGPD, con particolare riguardo alle vicende che hanno coinvolto il popolare social network americano Facebook, ora di proprietà della Meta Platforms<sup>11</sup>.

2. Il bilanciamento tra le diverse esigenze di tutela, che vengono in rilievo nei casi di violazione dei dati personali posta in essere per fini concorrenziali, permea il panorama normativo europeo, dove la privacy, pur rilevando in termini di protezione dei diritti fondamentali, risulta comunque condizionata dalle necessità di *governance* del contesto mercantile.

La normativa a tutela dei dati personali, comunemente nota e che si intende qui solamente accennare, ma che verrà ripresa nel prosieguo con riferimento a profili specifici, si compone di una fonte di matrice eurounitaria, completata da legislazioni nazionali, in attuazione e specificazione della prima, tenuto conto dell'entrata in vigore del regolamento (UE) 2016/679. Quest'ultimo ha sostituito la precedente direttiva del 1995<sup>12</sup>, introducendo norme uniformi applicabili su tutto il territorio dell'Unione e lasciando un ristretto margine di discrezionalità in capo agli Stati membri con riferimento a disposizioni di natura operativa a completamento del quadro europeo.

In generale, è possibile osservare che la legislazione UE applicabile alla protezione della privacy, in relazione ad operazioni che hanno ad oggetto il trattamento dei dati, si fonda su due anime: la tutela, da una parte, del mercato e, dall'altra, dei diritti delle persone che possono

---

*marginale della sentenza Fashion ID*, in *Rivista di diritto internazionale privato e processuale*, 2019, n. 4, pp. 982-999, spec. p. 990 ss.

<sup>11</sup> Ai fini del presente lavoro si precisa che Meta Platforms Inc., con sede legale negli Stati Uniti, è la società controllante a monte del gruppo "Meta" (precedentemente denominato Facebook) costituito da uno stabilimento principale nel territorio UE in Irlanda, la Meta Platforms Ireland Limited, e altre sedi dislocate in altri Stati membri, ed è attivo a livello globale nell'offerta, ai propri utenti, di piattaforme digitali social network (con funzioni di messaggistica, app, servizi, tecnologie e software), tra le quali le più diffuse sono Facebook, Instagram e WhatsApp.

<sup>12</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *GUUE*, L 281 del 23 novembre 1995, pp. 31-50.

venire in considerazione. Emerge senza dubbio la consapevolezza del legislatore europeo di voler regolamentare il mercato dei dati e soprattutto di controllare, nel contesto digitale europeo, il ruolo delle “Big Tech”, piattaforme digitali<sup>13</sup> principalmente americane (le cd. GAFAM – Google Apple Facebook Amazon Microsoft), ma anche altre, come Tik Tok, di origine cinese. Ciò è confermato in particolare dalla recente normativa composta dal *Digital Markets Act* (DMA)<sup>14</sup> e dal *Digital Services Act* (DSA)<sup>15</sup>, al fine di limitare il loro potere di mercato e (provare ad) aprire nuovi spazi sui mercati a piccoli concorrenti.

Nell’ordinamento eurounitario, la disciplina rilevante comprende regole in materia non solo di tutela dei dati personali, ma anche di antitrust e di regolamentazione del mercato digitale. Le diverse fonti vanno quindi coordinate a seconda della situazione che viene in rilievo, pur potendo essere applicate tutte contemporaneamente ad una medesima fattispecie, come nelle vicende su cui ci soffermerà, che concernono violazioni della privacy tramite le quali vengono poste in essere condotte incompatibili con il diritto UE della concorrenza. Con riguardo al loro coordinamento, nel regolamento sui mercati digitali viene da ultimo precisato che esso si applica senza pregiudizio delle norme sulla concorrenza e delle norme sulla tutela dei dati personali, nonché di altre discipline, come quella relativa alle comunicazioni<sup>16</sup>.

Le diverse normative applicabili ad una medesima violazione della privacy che dà luogo a un illecito antitrust comportano così anche l’esperibilità di diversi rimedi di *public* e *private enforcement*, coinvolgendo, nel primo caso, le autorità nazionali indipendenti rispettivamente incaricate e, nel secondo, riguardando competenze giurisdizionali in area civile o amministrativa. Prima di approfondire questi strumenti di protezione, col fine di verificare i rispettivi limiti e i confini dei poteri delle autorità competenti, ci si soffermerà sulla fattispecie della violazione della privacy nel contesto della concorrenza, ripercorrendo alcuni casi significativi.

**3. Quando la violazione della privacy, conseguente ad un uso illecito e sfruttamento dei dati personali<sup>17</sup>, diventa in concreto un mezzo per fare concorrenza sleale<sup>18</sup>, tale comportamento**

---

<sup>13</sup> Per una definizione di piattaforma digitale, si veda, tra gli altri, A. CANEPA, *I mercanti dell’era digitale. Un contributo allo studio delle piattaforme*, Torino, 2020, p. 27 ss.; nonché v. M.A. ROSSI, *Il ruolo delle piattaforme nell’economia dei Big Data*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, pp. 75-92.

<sup>14</sup> Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in *GUUE*, L 265 del 12 ottobre 2022, pp. 1-66, che si applica dal 2 maggio 2023, ad eccezione di alcune disposizioni che trovano applicazione dal 25 giugno 2023.

<sup>15</sup> Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in *GUUE*, L 277 del 27 ottobre 2022, pp. 1-102, applicabile dal 17 febbraio 2024, ad eccezione di alcune norme che si applicano dal 16 novembre 2022.

<sup>16</sup> Considerando 10, 11 e 12, nonché 37 (con riguardo al RGPD) e art. 1, par. 6 del DMA.

<sup>17</sup> I dati personali sono caratterizzati da una natura di controprestazione non pecuniaria e le fattispecie di scambio di dati rientrano nella categoria dei contratti conclusi dai consumatori, ai quali si applica la tutela prevista nei confronti di pratiche commerciali scorrette: V. RICCIUTO, *L’equivoco della privacy*, cit., p. 174 ss.

<sup>18</sup> Per un’analisi del diritto della concorrenza applicato al mercato digitale, v., in senso non esaustivo, 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, 2018, pp. 173-191; nonché W. KERBER, *Digital markets, data and privacy: competition law, consumer law and data protection*, *ivi*, pp. 1-20, spec. p. 3 ss.; A. PEZZOLI, *Big data e*

non solo implica una violazione delle disposizioni contenute nel RGPD ma anche delle norme antitrust, in quanto risultante in un abuso di posizione dominante<sup>19</sup> 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<sup>20</sup>. La fattispecie tocca quindi profili in tema di concorrenza e di tutela dei consumatori. Ciò che può essere sanzionato dalle autorità antitrust non è il trattamento illecito dei dati, ma la condotta anticoncorrenziale perpetrata attraverso tale utilizzo. Spetterà invece al garante per la privacy sanzionare la violazione delle norme sui dati personali, indipendentemente dagli effetti sulla concorrenza.

Non solo, ma simili usi illeciti dei dati potrebbero dare luogo a violazioni delle nuove regole contenute nel DMA, passibili di sanzioni comminate dalla Commissione europea. A tali azioni pubbliche, si aggiunge la possibilità di esperire rimedi di *private enforcement*, con i quali i titolari dei dati possono agire per far valere il proprio diritto alla protezione dei dati personali, richiedendo la cessazione della condotta illegittima, nonché il risarcimento dei danni.

Si potrebbe quindi ipotizzare che, se una piattaforma digitale che ha acquisito un concorrente il quale, nel proprio “patrimonio”, possiede un’estesa massa di dati, procedesse ad incrociare i dati presenti su entrambi i network, senza avere previamente avvisato gli utenti dell’una e dell’altra piattaforma, potrebbe verosimilmente porre in essere (i) sia un comportamento anticoncorrenziale, (ii) sia una violazione della normativa posta a protezione della privacy, (iii) sia, infine, una violazione del DMA. In una tale ipotesi, quando l’impresa che, con un unico comportamento, violi tutti e tre i settori normativi, ogni autorità rispettivamente competente, nei limiti dei regolamenti attributivi dei loro poteri, potrebbe irrogare le proprie sanzioni<sup>21</sup>.

Con riferimento alla violazione della privacy e delle regole antitrust, non sono mancati casi di condotte anticoncorrenziali conseguenti all’uso illecito di dati personali, anche nel

---

*antitrust: un’occasione per tornare ad occuparci di struttura?*, *ivi*, pp. 243-263; G. COLANGELO, M. MAGGIOLINO, *Data Protection in Attention Markets: Protecting Privacy through Competition?*, in *Journal of European Competition Law & Practice*, 2017, n. 8(6), pp. 363-369; G. COLANGELO, *Big data, digital platforms and antitrust*, in *Mercato Concorrenza Regole*, 2016, n. 3, pp. 425-460; G. PITRUZZELLA, *Big Data, Competition and Privacy: a Look from the Antitrust perspective*, in *Concorrenza e mercato*, 2016, n. 23, pp. 15-28; nonché OECD *Handbook on Competition Policy in the Digital Age*, 2022, reperibile al sito Internet [www.oecd.org/daf/competition-policy-in-the-digital-age](http://www.oecd.org/daf/competition-policy-in-the-digital-age); Autorità garante della concorrenza e del mercato (AGCM), Autorità per le garanzie nelle comunicazioni (AGCOM), Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, 2020; French Autorité de la Concurrence, Bundeskartellamt, *Competition Law and Data*, 2016, reperibile al sito Internet [www.bundeskartellamt.de](http://www.bundeskartellamt.de); con riferimento all’uso degli algoritmi, v. A. CANEPA, *I mercanti digitali*, cit., p. 118 ss.; F. BASSAN, *Potere dell’algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi*, Soveria Mannelli (CZ), 2019, p. 58 ss., nonché C. PERARO, *Lo scambio di informazioni tra le imprese nell’epoca di Internet: considerazioni sulle regole*, in *Studi sull’integrazione europea*, 2020, n. 2, pp. 451-471.

<sup>19</sup> In merito, v. G. MUSCOLO, *Big data e concorrenza*, cit., p. 178 ss. In tema, v. anche P. CATALLOZZI, *Abuso di posizione dominante: introduzione all’art. 102*, e M. KADAR, *Abuse of dominance in the IT sector: the European Commission’s recent enforcement practice*, in V. FALCE (ed.), *Competition law enforcement in digital markets*, cit., pp. 153-177.

<sup>20</sup> G. MUSCOLO, *Big data e concorrenza*, cit., p. 183 ss.

<sup>21</sup> Per un’analisi di tale fattispecie, nonché sul coordinamento tra le diverse fonti, v. G. CONTALDI, *La proposta della Commissione europea di adozione del “Digital Markets Act”*, in *Papers di diritto europeo*, 2021, n. 1, pp. 73-88, spec. p. 84 ss. Non vengono affrontati in questa sede i procedimenti che coinvolgono le imprese ritenute responsabili di violazioni del diritto UE in materia di privacy, concorrenza o mercati digitali, causate da una medesima condotta. Sulla questione di possibili giudizi paralleli e l’applicazione del principio del *ne bis in idem*, v., per tutti, P. DE PASQUALE, *Uno, nessuno e centomila. I criteri di operatività del principio ne bis in idem*, in *Eurojus*, 2022, n. 2, pp. 248-258.

panorama nazionale<sup>22</sup>, che hanno portato l'autorità italiana per la concorrenza e il mercato (AGCM) a constatare l'esistenza di pratiche commerciali scorrette<sup>23</sup>, piuttosto che abusi di posizione dominante<sup>24</sup>. La determinazione della differente normativa violata, in materia antitrust, rileva ai fini del riconoscimento dei diritti dei consumatori, quali titolari dei dati sfruttati, che potrebbero far valere tali diritti, chiedendo in sostanza il risarcimento dei danni causati dalla violazione.

In questo contesto, è significativa la nota vicenda riguardante l'acquisizione da parte del social network statunitense Facebook Inc. (con stabilimento principale europeo in Irlanda) della piattaforma online di messaggistica WhatsApp Inc., anch'essa con sede negli Stati Uniti, che nel 2014 era stata ammessa da parte della Commissione europea, in quanto, a suo avviso, l'acquirente (la prima) e l'impresa target (la seconda) erano attivi su mercati rilevanti diversi e non ci sarebbe stata minore disponibilità di dati personali. In quella sede, ovvero nell'indagine per verificare la compatibilità con le norme antitrust, l'impatto sulla privacy non era stato verificato<sup>25</sup>. La conclusione si era basata anche sulla dichiarazione di Facebook, secondo cui la raccolta e l'utilizzo dei dati degli utenti di WhatsApp sarebbe stato tecnicamente irrealizzabile e che la politica di tale piattaforma in merito ai dati dell'utente non sarebbe stata modificata. La Commissione, dunque, aveva ritenuto che la fusione non avrebbe sollevato alcun problema nell'ambito della concorrenza, poiché i dati sarebbero stati, ad ogni modo, disponibili per le società concorrenti.

Tuttavia, nel 2016 dopo aver aggiornato i termini del servizio, Facebook aveva disposto il collegamento tra i numeri di telefono della chat e i profili del social network. Nel 2017 l'Antitrust europea irrogava quindi una sanzione di 110 milioni di euro a Facebook perché, in occasione dell'acquisizione, «per quanto riguarda la possibilità di abbinare automaticamente le ID di Facebook con il numero di telefono mobile degli utenti di WhatsApp, Facebook Inc. ha fornito, quantomeno per negligenza, indicazioni inesatte o fuorvianti»<sup>26</sup>.

---

<sup>22</sup> Cfr. anche V. RICCIUTO, *L'equivoco della privacy*, cit., p. 93 ss.

<sup>23</sup> Si vedano ad esempio AGCM, provvedimento n. PS11147 del 26 novembre 2021, *Google*, e provvedimento n. PS11150 del 26 novembre 2021, *Apple*. Il quadro normativo in tema di *unfair commercial practices* si rinviene nel decreto legislativo 2 agosto 2007, n. 146, Attuazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica le direttive 84/450/CEE, 97/7/CE, 98/27/CE, 2002/65/CE, e il Regolamento (CE) n. 2006/2004, in *GU Serie Generale* n. 207 del 6 settembre 2007 (succ. modif.). In generale sulla relazione tra RGPD e la direttiva del 2005, v. da ultimo M. NIŠEVIC, *Profiling through Big Data Analytics. The Interplay between the General Data Protection Regulation and Unfair Commercial Practices Directive*, Cambridge, 2023.

<sup>24</sup> Si veda ad esempio AGCM, provvedimento n. 28162 del 25 febbraio 2020, A514 - *Condotta Fibra Telecom Italia*.

<sup>25</sup> Decisione della Commissione del 3 ottobre 2014 che dichiara la compatibilità con il mercato comune di una concentrazione (Caso n. COMP/M.7217 - Facebook / Whatsapp) in base al Regolamento (CE) n. 139/2004 del Consiglio. Sulla vicenda, v. anche R. CAFARI PANICO, *L'identità digitale*, cit., p. 829 ss.; S. GOBBATO, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *Media Laws - Rivista di Diritto dei Media*, 2019, n. 3, pp. 148-161, spec. p. 153 ss.

<sup>26</sup> Decisione della Commissione del 18 maggio 2017 che infligge ammende a un'impresa, a norma dell'articolo 14, paragrafo 1, del regolamento (CE) 139/2004 del Consiglio, per aver fornito indicazioni inesatte o fuorvianti [Caso n. M.8228 — Facebook/WhatsApp (procedimento ex articolo 14, paragrafo 1)], [notificato con il numero C(2017)3192 final], sintesi in versione italiana pubblicata in *GUUE*, C 286 del 30 agosto 2017, pp. 6-9. In generale sul tema delle concentrazioni nel mercato digitale, v. D. DANIELI, *Il controllo delle concentrazioni nel settore digitale e il nuovo approccio della Commissione europea: fit for purpose?*, in *Quaderno AISDUE serie speciale - Atti del convegno "L'Unione europea dopo la pandemia" Bologna 4-5 novembre 2021, 2022*, pp. 273-291.

Anche l'AGCM ha affrontato il caso Facebook/WhatsApp nel 2017, condannando la prima per pratiche commerciali scorrette in applicazione della disciplina sulle clausole vessatorie contenuta nel Codice del consumo<sup>27</sup>. Infatti, l'autorità italiana ha sanzionato, per un importo pari a 3 milioni di euro, il social network americano per aver indotto utenti ad accettare le modifiche dei termini di utilizzo della funzione Messenger preimpostando l'opzione che consente la condivisione dei dati tra Facebook e WhatsApp, non potendo gli utenti altrimenti, di fatto, continuare ad usufruire dei servizi<sup>28</sup>.

Con riguardo alla medesima vicenda, il garante italiano per la protezione dei dati personali (nel prosieguo anche GPDP o garante privacy) ha adottato una decisione, nell'ottobre 2018, vietando a WhatsApp di comunicare i dati dei propri utenti il cui consenso sia stato ottenuto con modalità illegittime e a Facebook di effettuarne comunque ogni ulteriore trattamento<sup>29</sup>.

Sempre nei confronti di Facebook, l'AGCM è poi intervenuta con un provvedimento nel 2018<sup>30</sup> concernente due comportamenti, vale a dire la mancanza di informazioni sulla gratuità del servizio e il trasferimento dei dati verso terzi senza consenso degli utenti, sanzionati in quanto pratiche commerciali scorrette<sup>31</sup>, con un importo pari a 10 milioni di euro. Il provvedimento era stato poi impugnato davanti al giudice amministrativo, che sia in primo grado sia in secondo grado ha confermato la legittimità della sanzione<sup>32</sup>.

La violazione della privacy può costituire anche un comportamento attraverso il quale un'impresa incorre in un abuso di posizione dominante ai sensi dell'art. 102 TFUE. Si prenda ad esempio la causa SEN<sup>33</sup>, dove era stata impugnata la decisione dell'AGCM di infliggere una sanzione pecuniaria per un importo superiore a 90 milioni di euro per abuso di posizione dominante alle società di energia elettrica Servizio Elettrico Nazionale SpA (SEN), la ENEL SpA, sua società madre, e la ENEL Energia SpA (EE), una società consorella. L'autorità aveva accertato che suddette società avevano attuato una strategia escludente volta a trasferire la

---

<sup>27</sup> Decreto legislativo 6 settembre 2005, n. 206, Codice del consumo, in *GU* n. 235 dell'8 ottobre 2005 - Suppl. Ordinario n. 162, succ. modif.

<sup>28</sup> AGCM, n. 26597 dell'11 maggio 2017, PS10601, *WhatsApp – Trasferimento dati a Facebook*. Su cui v. A. SAIJA, *Protezione dei dati personali*, cit., p. 104 ss.; S. GOBBATO, *Big data*, cit., p. 156 ss.

<sup>29</sup> Garante privacy, provvedimento reg. n. 462 del 4 ottobre 2018, *WhatsApp: divieto di cessione dei dati degli utenti a Facebook*.

<sup>30</sup> AGCM, provvedimento n. 27432 del 29 novembre 2018, caso PS11112, *Facebook – Condivisione dati con terzi*.

<sup>31</sup> In base alla prima pratica, Facebook aveva ingannevolmente indotto gli utenti consumatori a registrarsi sulla Piattaforma Facebook non informandoli adeguatamente e immediatamente, in fase di attivazione dell'account, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti, e, più in generale, delle finalità remunerative che sottendono la fornitura del servizio di social network enfatizzandone la sola gratuità, così da indurli ad assumere una decisione di natura commerciale che non avrebbero altrimenti preso (registrazione al social network, tramite sito e app, e permanenza nel medesimo). Con la seconda pratica, il Professionista esercitava un indebito condizionamento nei confronti dei consumatori registrati, i quali subiscono, senza espresso e preventivo consenso, quindi in modo inconsapevole e automatico, la trasmissione e l'uso da parte di FB/terzi, per finalità commerciali, dei dati che li riguardano (informazioni derivanti dall'uso di FB e dalle proprie esperienze su siti e app di terzi). L'indebito condizionamento deriva dall'applicazione del sistema di preselezione del più ampio consenso alla trasmissione dei propri dati da/a terzi, sopra descritto, unitamente alla prospettazione, a seguito di deselezionazione, di rilevanti limitazioni di fruibilità del social network e dei siti web/app di terzi, più ampie e pervasive rispetto a quelle effettivamente applicate, conseguenze paventate che condizionano gli utenti a mantenere la scelta preimpostata da FB.

<sup>32</sup> TAR Lazio, sentenza 10 gennaio 2020, n. 260, e Consiglio di Stato, sentenza 29 marzo 2021, n. 2631.

<sup>33</sup> Corte di Giustizia, sentenza del 12 maggio 2022, causa C-377/20, *Servizio Elettrico Nazionale SpA (SEN) e a. c. Autorità Garante della Concorrenza e del Mercato e a.*, EU:C:2022:379 (domanda di pronuncia pregiudiziale proposta dal Consiglio di Stato).

clientela del SEN, il gestore storico del mercato tutelato, alla EE, la quale opera sul mercato libero. Ad avviso della AGCM, l'obiettivo del gruppo ENEL sarebbe stato di scongiurare il rischio di un passaggio in massa dei clienti del SEN verso fornitori terzi. In particolare, il SEN avrebbe raccolto, dal 2012, i consensi dei propri clienti del mercato tutelato a ricevere offerte commerciali relative al mercato libero, con modalità discriminatorie consistenti nel chiedere consensi "separati" per le società del gruppo ENEL, da un lato, e per i terzi, dall'altro. I clienti erano così stati indotti a ritenere che il rilascio di un simile consenso fosse necessario al mantenimento del loro approvvigionamento di elettricità, e, quindi, a negare il loro consenso ad altri operatori. In questo modo, il SEN avrebbe limitato il numero di consensi da parte dei clienti del mercato tutelato alla ricezione di offerte commerciali provenienti dagli operatori concorrenti. La decisione dell'autorità era stata impugnata davanti al TAR Lazio che, con sentenze del 17 ottobre 2019, ha diminuito la sanzione alla SEN e respinto il ricorso dell'ENEL. In sede di appello, il Consiglio di Stato si è rivolto alla Corte di giustizia con domande riguardanti lo sfruttamento abusivo in materia di pratiche escludenti. Nella sentenza del 12 maggio 2022, la Corte di Lussemburgo ha affermato che «è sufficiente che la pratica sia idonea a pregiudicare la struttura di effettiva concorrenza sul mercato rilevante, a meno che l'impresa dominante non dimostri gli effetti positivi per i consumatori, in particolare in termini di prezzi, di scelta, di qualità e di innovazione»<sup>34</sup>. La condotta escludente perpetrata dalla SEN, tramite lo sfruttamento dei dati degli utenti, costituiva perciò un illecito antitrust.

Un caso riguardante la violazione delle norme della concorrenza per le modalità di trattamento dei dati da parte del social network Facebook pende davanti ai giudici tedeschi dal 2019<sup>35</sup>. La vicenda è oggetto anche di rinvio pregiudiziale alla Corte di giustizia nella causa *Meta Platforms*<sup>36</sup>, con cui il giudice tedesco adito ha richiesto di definire i confini dei poteri delle autorità coinvolte, vale a dire l'antitrust e il garante privacy, su cui si tornerà nel prosieguo in tema di *public enforcement*. Si tratta di una controversia tra alcune società del gruppo americano Meta Platforms (successori di Facebook, dopo aver acquisito WhatsApp e Instagram) e il Bundeskartellamt (autorità federale garante della concorrenza della Germania) in merito alla decisione con la quale quest'ultimo ha vietato a Meta Platforms il trattamento dei dati previsto dalle condizioni d'uso della sua rete sociale Facebook, nonché l'attuazione di tali condizioni, e ha imposto misure correttive. L'autorità contestava la prassi consistente, in primo

---

<sup>34</sup> In merito alle altre questioni sollevate, la Corte di giustizia ha sostenuto che per escludere il carattere abusivo di una condotta di un'impresa in posizione dominante non è sufficiente, di per sé, la prova che la condotta non ha prodotto effetti restrittivi concreti, in quanto può costituire solo un indizio dell'incapacità della condotta in questione di produrre effetti anticoncorrenziali; l'autorità garante della concorrenza non è tenuta a dimostrare l'intento dell'impresa di escludere i propri concorrenti ricorrendo a mezzi o risorse diversi da quelli su cui si impernia una concorrenza basata sui meriti, ma tale prova può costituire una circostanza di fatto da prendere in considerazione ai fini della determinazione di un abuso di posizione dominante; una pratica può essere qualificata come abusiva se può produrre un effetto escludente e se si basa sull'utilizzo di mezzi diversi da quelli propri di una concorrenza basata sui meriti, a meno che l'impresa in posizione dominante dimostri che la pratica era obiettivamente giustificata e proporzionata a tale giustificazione oppure controbilanciata, se non superata, da vantaggi in termini di efficienza, a beneficio anche dei consumatori; quando una posizione dominante è sfruttata in modo abusivo da una o più società figlie appartenenti a un'unità economica, l'esistenza di tale unità è sufficiente per ritenere che la società madre sia anch'essa responsabile di tale abuso, a meno che non dimostri che essa non aveva il potere di definire i comportamenti delle società figlie, le quali agivano autonomamente.

<sup>35</sup> Su questa vicenda, v., tra i molti, V. ROBERTSON, *Excessive data collection: privacy considerations and abuse of dominance in the era of big data*, in *Common Market Law Review*, 2020, n. 57, pp. 161-190.

<sup>36</sup> Corte di giustizia (Grande Sezione), sentenza del 4 luglio 2023, causa C-252/21, *Meta Platforms e a. c. Bundeskartellamt*, EU:C:2023:537.

luogo, nella raccolta di dati generati da altri servizi propri del gruppo, nonché da siti Internet e da applicazioni di terzi tramite interfacce in essi integrate oppure mediante cookies memorizzati nel computer o nel dispositivo mobile dell'utente; in secondo luogo, nel collegamento di tali dati con l'account Facebook dell'utente interessato; e, in terzo luogo, nell'utilizzo di detti dati. Ad avviso dell'autorità tedesca, il trattamento di cui trattasi costituiva uno sfruttamento abusivo della posizione dominante da parte di Meta Platforms sul mercato delle reti sociali per gli utenti privati in Germania, ai sensi dell'art. 19 del GW<sup>37</sup>. In altri termini, una violazione delle norme sulla tutela dei dati personali si concretizzava, di fatto, in una violazione delle norme antitrust. Meta Platforms ha proposto ricorso contro la decisione dell'autorità tedesca dinanzi al Tribunale superiore del Land di Düsseldorf, che ha presentato il rinvio, su cui la Corte di giustizia si è pronunciata in data 4 luglio 2023 richiamando, come si avrà modo di precisare, le diverse autorità interessate alla necessaria collaborazione<sup>38</sup>. Basti qui osservare che la vicenda si inserisce nella annosa saga Facebook–Meta Platforms con riguardo al trattamento dei dati personali, sotto diversi profili, dove le sentenze pregiudiziali dei giudici di Lussemburgo hanno contribuito a fornire interpretazioni utili per l'attuazione della normativa in tema sia di dati personali sia di concorrenza.

I casi poc'anzi riportati hanno visto come parti opposte, da un lato, l'autorità antitrust e, dall'altro, le imprese ritenute responsabili di aver posto in essere pratiche anticoncorrenziali. Tali procedimenti possono sfociare in sanzioni nei confronti di queste ultime, senza tuttavia incidere sul riconoscimento dei danni eventualmente sofferti dai soggetti titolari dei dati usati illecitamente, per i quali si rende necessario promuovere azioni giudiziarie.

4. Le questioni trattate nelle vicende ricordate sono significative per i diversi profili che vengono in gioco, in sede di trattamento illecito di dati personali, con riguardo, in specie, al quadro dei rimedi esperibili in questi casi. Non solo è possibile che la violazione della privacy dia luogo a un comportamento in contrasto con le regole antitrust oppure a un'infrazione della normativa a tutela del consumatore, ma la medesima violazione della privacy potrebbe essere perseguita in quanto tale, quindi in base alla disciplina in tema di tutela dei diritti dei titolari dei dati personali, quali utenti vittime dello sfruttamento illecito. Sempre più di frequente si assiste a simili situazioni in un mercato digitale in continua evoluzione, dove l'Unione, per tale motivo, ha adottato disposizioni legislative, in particolare i recenti regolamenti DMA e DSA, che mirano a disciplinare *ex ante* le condotte delle imprese, imponendo loro obblighi, per assicurare il buon funzionamento del mercato<sup>39</sup>.

Le normative, sopra ricordate, che vengono in rilievo in situazioni di violazione della privacy che comportano un illecito antitrust, prevedono strumenti di *public* e *private*

---

<sup>37</sup> Bundeskartellamt, decisione n. B6-22/16 del 6 febbraio 2019. A tal riguardo, v. A. COLAPS, *Garantire la protezione dei diritti fondamentali*, cit., p. 88 ss.; A. SAIJA, *Protezione dei dati personali*, cit., p. 104 ss.

<sup>38</sup> V. *infra*, par. 4.1.

<sup>39</sup> Si nota che entrambi i nuovi regolamenti hanno come base giuridica l'art. 114 TFUE (su cui v. per il DMA la Proposta della Commissione COM(2020) 842 final del 15 dicembre 2020, par. 2; e per il DSA la Proposta della Commissione COM(2020)825 final del 15 dicembre 2020, par. 2).

*enforcement*, esperibili parallelamente per le diverse caratteristiche e finalità<sup>40</sup>, dando luogo a un «contesto sempre più complesso e sempre più diversificato di tutela multilivello sul piano sia amministrativo sia giurisdizionale, sia nazionale sia europeo»<sup>41</sup>.

In generale, nello stesso ambito materiale, le *private actions* dovrebbero prendere in considerazione gli atti del procedimento condotto dall'autorità indipendente, anche quando ancora pendente, al fine di non giungere a conclusioni incompatibili<sup>42</sup>, oppure riferirsi agli esiti di questo come prova dell'accertamento della violazione. In caso di diverso ambito, i procedimenti delle varie autorità coinvolte potrebbero comunque essere coordinati tra loro<sup>43</sup>, come pure questi con le azioni giudiziali, oppure ancora tra queste ultime promosse davanti a tribunali nazionali competenti per le diverse materie, sempre al fine di evitare decisioni e conclusioni contrastanti alla luce del principio del *ne bis in idem*.

Ci si propone quindi di affrontare il sistema di rimedi rilevanti in tema di privacy e antitrust secondo tre profili di interesse: il primo con riferimento ai poteri delle autorità indipendenti, il secondo alle azioni esperibili dagli individui e, infine, alla portata extraterritoriale degli standard europei di protezione nei casi di trasferimento dei dati fuori dall'Unione.

**4.1.** Le disposizioni legislative dell'Unione, che disciplinano la protezione dei dati personali, gli illeciti antitrust e gli obblighi in capo ai *gatekeepers*, contemplanò meccanismi di *public enforcement*.

Ogni autorità incaricata, in un sistema decentrato in cooperazione con la Commissione europea, può essere coinvolta in una medesima situazione di violazione della privacy, nei limiti delle aree di competenza e con gli strumenti a propria disposizione<sup>44</sup>. Ciò comporta una coesistenza delle stesse, che, in ottica collaborativa, potrebbero coordinare le indagini e le valutazioni, nonché la determinazione delle eventuali conseguenti sanzioni. In generale, l'applicazione delle regole è controllata da autorità con analoghi poteri di indagine e simili poteri sanzionatori, pur se con riguardo a campi materiali distinti. Nel contesto di ogni singolo settore sono infatti definiti i compiti di ciascuna autorità, nonché i criteri per la determinazione delle sanzioni.

Nell'ambito della concorrenza, come noto, in base al meccanismo di *enforcement* decentrato, le autorità nazionali, ognuna nel proprio territorio e in cooperazione con la Commissione in caso di situazioni transfrontaliere, sono competenti a vigilare sulla corretta

---

<sup>40</sup> Sulla complementarità dei due sistemi, v. C. SCHEPISI, *Digital Markets Act e private enforcement*, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea sui mercati*, Bari, 2021, pp. 99-167, spec. p. 158 s.

<sup>41</sup> R. CAFARI PANICO, *L'identità digitale*, cit., p. 839.

<sup>42</sup> Sulla complementarità dei procedimenti in tema di concorrenza pendenti uno davanti alla Commissione europea e l'altro davanti al giudice nazionale, pur non riguardante la tutela della privacy, v. Corte di giustizia, sentenza del 12 gennaio 2023, causa C-57/21, *RegioJet a.s. c. České dráhy a.s.*, EU:C:2023:6, con cui ha stabilito che un giudice nazionale può ordinare la produzione di prove, ai fini di un procedimento per il risarcimento del danno conseguente a una violazione del diritto della concorrenza, anche qualora il procedimento relativo a tale infrazione pendente dinanzi alla Commissione sia stato sospeso in attesa di una sua decisione; spetta al giudice nazionale accertarsi che la produzione di prove sia effettivamente necessaria e proporzionata ai fini dell'esame della domanda di risarcimento in questione.

<sup>43</sup> A tal riguardo, v. causa C-252/21, *Meta Platforms*, cit.

<sup>44</sup> Sui poteri delle autorità, v., da ultimo, A. SAIJA, *Protezione dei dati personali*, cit., p. 109 ss.

applicazione della normativa a tutela delle dinamiche del mercato e dei consumatori, con riferimento, in merito a quest'ultimi, alle esigenze di correttezza e trasparenza delle scelte economiche<sup>45</sup>. All'esito del procedimento possono essere irrogate sanzioni, oltre all'imposizione di obblighi relativi alle misure correttive da adottare. Le indagini e i provvedimenti possono essere oggetto di impugnazione da parte delle imprese coinvolte davanti al giudice amministrativo nazionale oppure, in caso di decisione della Commissione europea, davanti al Tribunale dell'Unione europea.

Un aumento dei poteri delle autorità antitrust è stato riconosciuto con la direttiva (UE) 2019/1 dell'11 dicembre 2018 (cd. *Direttiva Ecn+*)<sup>46</sup>, attuata in Italia con decreto legislativo 8 novembre 2021, n. 185<sup>47</sup>, finalizzata ad assicurare che tali autorità dispongano delle necessarie garanzie di indipendenza, delle risorse e dei poteri di indagine e sanzionatori, allo scopo di vigilare che la concorrenza nel mercato interno non sia falsata e che i consumatori e le imprese non siano svantaggiati da leggi e misure nazionali<sup>48</sup>.

Quando si tratta di protezione dei consumatori l'effetto deterrente associato alle pene pecuniarie è ancora più rilevante. Da ultimo con la direttiva (UE) 2019/2161 del 27 novembre 2019 (cd. *Direttiva Omnibus*)<sup>49</sup> il legislatore europeo è intervenuto per migliorare la conoscenza dei diritti dei consumatori stessi, nonché per rafforzare l'attuazione dei diritti medesimi e dei rimedi ad essi collegati, introducendo modifiche alle disposizioni esistenti. La direttiva, che si applica dal 28 maggio 2022, è stata recepita in Italia solo recentemente con il decreto legislativo 7 marzo 2023, n. 26<sup>50</sup>, dopo che era stata avviata la procedura di infrazione n. 2022/0107 per mancato recepimento.

A fini di completezza, si evidenzia che rientra nelle competenze del garante antitrust anche il potere di controllo della dipendenza economica delle imprese al fine di rafforzare il contrasto all'abuso, introdotto con la Legge annuale per il mercato e la concorrenza 2021<sup>51</sup>. In base alla modifica apportata all'art. 9 della Legge sulla disciplina della subfornitura nelle

---

<sup>45</sup> Sul ruolo delle autorità antitrust, v., tra i molti, M. PIGNATTI, *L'effettività del diritto della concorrenza: il ruolo delle Autorità nazionali garanti della concorrenza e i profili evolutivi della disciplina*, in *DPCE online*, 2021, n. 2, pp. 2649-2665; M. RAJOLI, *La tutela antitrust nel XXI secolo. Competition Law and Consumer Protection in the 21st Century*, in *Rivista della Regolazione dei mercati*, 2020, n. 2, pp. 221-229; A. SCOGNAMIGLIO, *L'European Competition Network: dal Regolamento sulla "modernizzazione" (Reg. 1/2003) alla Direttiva "ECN+" (Dir. 1/2019)*, in L.F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*, Milano, 2020, pp. 239-254; B. CORTESE, *EU Competition Law: Between Public and Private Enforcement*, AH Alphen aan den Rijn, 2013.

<sup>46</sup> Direttiva (UE) 2019/1 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno, in *GUUE*, L 11 del 14 gennaio 2019, pp. 3-33, con applicazione delle disposizioni dal 4 febbraio 2021. Per un commento, v. A.M. ROMITO, *La direttiva (UE) 1/2019: l'evoluzione del public enforcement del diritto europeo della concorrenza*, in *Studi sull'integrazione europea*, 2020, n. 2, pp. 341-358.

<sup>47</sup> Decreto legislativo 8 novembre 2021, n. 185, Attuazione della direttiva (UE) 2019/1, in *GU Serie Generale* n. 284 del 29 novembre 2021 - Suppl. Ordinario n. 40, con entrata in vigore il 14 dicembre 2021.

<sup>48</sup> In merito, v., per tutti, A. SCOGNAMIGLIO, *L'European Competition Network*, cit., p. 239 ss.

<sup>49</sup> Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, in *GUUE*, L 328 del 18 dicembre 2019, pp. 7-28.

<sup>50</sup> Decreto legislativo 7 marzo 2023, n. 26, Attuazione della direttiva (UE) 2019/2161, in *GU Serie Generale* n. 66 del 18 marzo 2023, entrata in vigore il 2 aprile 2023, alcune norme si applicano invece dal 1° luglio 2023. In sostanza, sono state introdotte modifiche al Codice del consumo.

<sup>51</sup> Legge 5 agosto 2022, n. 118, in *GU Serie Generale* n. 188 del 12 agosto 2022 (Legge annuale per il mercato e la concorrenza 2021), entrata in vigore il 27 agosto 2022.

attività produttive<sup>52</sup>, «si presume la dipendenza economica nel caso in cui un'impresa utilizzi i servizi di intermediazione forniti da una piattaforma digitale che ha un ruolo determinante per raggiungere utenti finali o fornitori, anche in termini di effetti di rete o di disponibilità dei dati»<sup>53</sup>. La norma prevede anche un elenco esaustivo di pratiche abusive, contro le quali le imprese interessate potranno ricorrere davanti al giudice ordinario al fine di far accertare la natura abusiva e chiedere il risarcimento del danno, nonché riconosce alla AGCM la facoltà di sanzionare le piattaforme digitali che risultano inottemperanti.

Nel contesto riguardante la tutela della privacy, oltre alle autorità di controllo, vale a dire i garanti nazionali per la protezione dei dati personali (GPDP)<sup>54</sup>, due organi svolgono un ruolo importante nell'applicazione del regolamento (UE) 2016/679: il Comitato europeo per la protezione dei dati (EDPB)<sup>55</sup>, che ha il potere di adottare orientamenti generali per chiarire le disposizioni, nonché di emanare decisioni vincolanti ai sensi del RGPD nei confronti delle autorità nazionali di controllo al fine di garantire un'applicazione coerente e uniforme delle norme; e il garante europeo per la protezione dei dati personali (EDPS)<sup>56</sup>, incaricato di esaminare il rispetto della protezione dei dati da parte delle istituzioni e degli organi UE, con funzioni consultive per gli stessi su tutti gli aspetti del trattamento dei dati personali e delle relative politiche e legislazioni.

Accanto alla definizione dei compiti e dei poteri dei garanti nazionali ed europeo, il regolamento 2016/679 stabilisce, per le situazioni di trattamento illecito dei dati con portata transfrontaliera, un meccanismo di cooperazione ai sensi dell'art. 60<sup>57</sup>, definito come “sportello unico”<sup>58</sup>, che prevede il ruolo di “autorità capofila” in capo al garante nazionale dello Stato dove si trova la sede principale (nell'Unione europea) del soggetto responsabile del trattamento dei dati. Ogniquale volta un'autorità di controllo di uno Stato membro affronti un caso di violazione dei dati commesso da una società con sede principale in un altro Stato UE, questa

---

<sup>52</sup> Legge 18 giugno 1998, n. 192, Disciplina della subfornitura nelle attività produttive, in *GU* n. 143 del 22 giugno 1998.

<sup>53</sup> Art. 33 della Legge annuale per il mercato e la concorrenza 2021, che introduce modifiche all'art. 9 della Legge n. 192/1998, che si applica dal 31 ottobre 2022. Per una recente indagine avviata in base a questa norma, si veda la vicenda *Meta/SIAE*: in sede di rinnovo della licenza per la diffusione di contenuti musicali in Italia sulle piattaforme di proprietà di Meta, le parti non raggiungevano un accordo; come risulta dal provvedimento della AGCM n. 30570 del 4 aprile 2023 di avvio del procedimento istruttorio (A559), Meta «potrebbe aver abusato dello squilibrio del potere di negoziazione di cui beneficia rispetto a SIAE e potrebbe aver posto in essere una pratica abusiva consistente nell'aver violato i doveri di buona fede, correttezza e trasparenza nella negoziazione della nuova licenza con SIAE»; Meta aveva anche interrotto le negoziazioni ed eliminato progressivamente contenuti musicali, riconducibili agli autori rappresentati da SIAE, dalle piattaforme di Instagram e Facebook; da ultimo, l'AGCM, nell'ambito del procedimento cautelare avviato parallelamente, con delibera del 20 aprile 2023 ha adottato misure cautelari imponendo la ripresa delle trattative con SIAE al fine di ripristinare la disponibilità dei contenuti musicali su Facebook e Instagram (cfr. AGCM, provvedimento n. 30606 del 20 aprile 2023).

<sup>54</sup> Per l'Italia, v. [www.garanteprivacy.it](http://www.garanteprivacy.it). In generale, sulle norme che riguardano le autorità di controllo, v. E. BELISARIO, G.M. RICCIO, G. SCORZA (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2<sup>a</sup> ed., 2022, p. 534 ss.

<sup>55</sup> *European Data Protection Board (EDPB)*, v. [https://edpb.europa.eu/edpb\\_it](https://edpb.europa.eu/edpb_it). In merito, v. E. BELISARIO, G.M. RICCIO, G. SCORZA (a cura di), *GDPR e Normativa Privacy. Commentario*, cit., p. 669 ss.

<sup>56</sup> *European Data Protection Supervisor (EDPS)*, v. <https://edps.europa.eu/en>.

<sup>57</sup> Sul meccanismo, v. EDPB, *Linee-guida 02/2022 sull'applicazione dell'articolo 60 del regolamento generale sulla protezione dei dati*, adottate il 14 marzo 2022, reperibili al sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr\\_it](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_it). Per una analisi della norma in esame, v. E. BELISARIO, G.M. RICCIO, G. SCORZA (a cura di), *GDPR e Normativa Privacy. Commentario*, cit., p. 617 ss.

<sup>58</sup> Cfr. considerando 127 e 128 del RGPD.

deve riferire il caso al garante di tale secondo Stato e collaborare con esso al fine di giungere a una decisione. Con riguardo alla cooperazione tra i garanti nazionali della privacy, si è pronunciata la Corte di giustizia nella causa *Facebook Ireland*<sup>59</sup>, adita in via pregiudiziale dal giudice belga al fine di verificare la portata delle competenze del garante del proprio paese nei confronti della nota società americana con sede, secondaria, in un altro Stato UE (vale a dire in Irlanda). La Corte ha chiarito che l'autorità belga, nello svolgimento delle sue funzioni, deve agire nel rispetto delle condizioni previste dal RGPD relative alla cooperazione con l'autorità capofila.

Laddove, sempre in una situazione con profili transfrontalieri, tra le autorità nazionali di controllo interessate non vi sia accordo sulla decisione, può essere attivato il meccanismo di coerenza, che prevede l'intervento dello *European Board*<sup>60</sup>. Significativa a tal riguardo è la vicenda che concerne, ancora, la società americana Meta Platforms, relativa a taluni trattamenti di dati personali di utenti minorenni nel contesto del servizio di rete di media sociali "Instagram"<sup>61</sup>, oggetto di indagine avviata di propria iniziativa dal garante irlandese (*Data Protection Commissioner* – DPC). Con provvedimento del 30 settembre 2022, il DPC ha comminato al social network una sanzione di oltre 400 milioni di euro, dopo che sul progetto di decisione erano state formulate diverse obiezioni da parte di altre autorità di controllo nazionali interessate<sup>62</sup> e dopo che, al fine di dirimere la controversia, il Comitato europeo aveva adottato una decisione vincolante in data 28 luglio 2022 *ex art.* 65 del RGPD<sup>63</sup>.

---

<sup>59</sup> Corte di giustizia (Grande Sezione), sentenza del 15 giugno 2021, causa C-645/19, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit (autorità per la protezione dei dati, Belgio)*, EU:C:2021:483. Per alcuni commenti, v. S. BRETTHAUER, *Extended powers for other supervisory authorities concerned in the case of cross-border data processing: Facebook Ireland*, in *Common Market Law Review*, 2022, n. 59, pp. 1543-1556; F. JAULT-SESEKE, *Protection des données : la mise en oeuvre du guichet unique ou les limites de l'intégration européenne*, in *Revue trimestrielle de droit européen*, 2022, n. 1, pp. 81-91; L. WOODS, *Facebook Ireland and the one stop shop under the GDPR*, in *European Law Review*, 2021, n. 5, pp. 685-691; nonché sia consentito il rinvio a C. PERARO, *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione europea verso Paesi terzi*, in *Ordine internazionale e diritti umani*, 2021, n. 3, pp. 666-691, spec. p. 687 ss.

<sup>60</sup> Per una analisi della disciplina in parola, v. E. BELISARIO, G.M. RICCIO, G. SCORZA (a cura di), *GDPR e Normativa Privacy. Commentario*, cit., p. 643 ss. È anche prevista, in base all'art. 66, par. 1, del RGPD, la possibilità per un'autorità nazionale di controllo (che non sia la capofila) di adottare immediatamente misure provvisorie intese a produrre effetti giuridici nel proprio territorio, con un periodo di validità determinato che non supera i tre mesi, qualora, in presenza di circostanze eccezionali, ritenga che urga intervenire per proteggere i diritti e le libertà degli interessati, in deroga quindi al meccanismo di coerenza di cui agli artt. 63, 64 e 65 del RGPD, o alla procedura di cui all'art. 60 del RGPD. In questo caso, l'autorità di controllo può poi chiedere un parere d'urgenza o una decisione vincolante d'urgenza del Comitato. Si veda, ad esempio, EDPB, *Decisione vincolante d'urgenza 01/2021 su richiesta dell'autorità di controllo di Amburgo (Germania) presentata ai sensi dell'art. 66, par. 2, del RGPD, ai fini di un'ordinanza per l'adozione di misure definitive nei confronti di Facebook Ireland Limited*, adottata il 12 luglio 2021, pubblicata il 29 giugno 2022.

<sup>61</sup> In particolare, riguardava il trattamento di dati personali da parte di Meta Platforms in relazione alla divulgazione al pubblico di indirizzi di posta elettronica e/o numeri di telefono di minorenni utenti della funzionalità «account Instagram Business» (account Instagram professionale), nonché un'impostazione predefinita come pubblica per gli account personali di utenti minorenni su Instagram.

<sup>62</sup> Tenuto conto della portata dei trattamenti effettuati dalla piattaforma social, ed il relativo impatto della decisione sugli interessati di differenti Stati membri.

<sup>63</sup> Decisione vincolante 2/2022 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Meta Platforms Ireland Limited (Instagram) ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, reperibile al sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen\\_it](https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen_it). L'EDPB ha adottato il 24 maggio 2023 le Linee guida 3/2021 sull'applicazione dell'art. 65 del RGPD, reperibili al sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032021-application-article-65-1a-gdpr\\_it](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032021-application-article-65-1a-gdpr_it).

Il Comitato europeo è stato coinvolto anche in un'altra occasione: in merito al trasferimento extraeuropeo dei dati<sup>64</sup> da parte di Meta Platforms Ireland verso la casa madre statunitense, l'autorità capofila irlandese, sostenendo che tale operazione fosse in violazione dell'art. 46 RGPD come interpretato dalla Corte di giustizia nella sentenza *Schrems II*<sup>65</sup>, aveva presentato un progetto di decisione, alla quale ha fatto seguito la decisione vincolante del Comitato del 13 aprile 2023<sup>66</sup>, resa appunto nell'ambito del meccanismo di coerenza, attivato poiché erano state sollevate obiezioni da parte di altre autorità nazionali in merito al contenuto di quel progetto. Il 12 maggio 2023 è stata adottata la decisione da parte dell'autorità irlandese<sup>67</sup> con cui ha definitivamente condannato la Meta Platforms al pagamento di una sanzione di oltre un miliardo di euro<sup>68</sup> e imposto di sospendere ogni futuro trasferimento dei dati fuori dai confini dell'Unione, nonché richiesto di adottare misure per conformare le sue operazioni di trattamento al Capitolo V del RGPD, in particolare cessando il trattamento illecito, compresa la conservazione, negli Stati Uniti dei dati personali di utenti UE/SEE trasferiti in violazione del RGPD. Si tratta quindi di una sanzione, parametrata ai continui trasferimenti illeciti, senza precedenti, che avrà anche un impatto deterrente per tutti i soggetti coinvolti in operazioni oltreoceano<sup>69</sup>. Si attende quindi la reazione di Meta Platforms, che potrebbe impugnare la decisione del garante irlandese per contestare gli addebiti, potendo verosimilmente fare richiamo anche alle difficoltà per la Commissione stessa incontrate in sede di negoziazioni per concludere un accordo con il governo americano sugli standard minimi che devono essere implementati, negli Stati Uniti, per offrire garanzie di protezione.

Al complesso sistema di collaborazione tra autorità privacy si aggiunge il possibile coordinamento tra le diverse autorità competenti quando il trattamento dei dati comporta una violazione sia della privacy sia delle regole antitrust. Tale aspetto è stato portato all'attenzione della Corte di giustizia nella causa *Meta Platforms*, cui si è già fatto riferimento. Una delle

---

<sup>64</sup> Sul punto, v. anche *infra*, par. 4.3.

<sup>65</sup> Corte di giustizia (Grande Sezione), sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximilian Schrems*, EU:C:2020:559 (nota come *Schrems II*). Seguendo l'interpretazione dei giudici europei, il DPC irlandese ha ritenuto il trattamento in questione, ovvero il trasferimento dei dati extraeuropeo incompatibile con il RGPD, nonostante Meta Platforms Ireland lo abbia effettuato sulla base delle clausole contrattuali standard adottate dalla Commissione europea, unitamente a misure supplementari, in quanto tali accordi non affrontavano adeguatamente i rischi per i diritti e le libertà fondamentali degli interessati.

<sup>66</sup> Binding Decision 1/2023 on the dispute arisen on the draft decision of the Irish Supervisory Authority on transfers of personal data carried out by Meta Platforms Ireland Limited in the context of their Facebook service (Art. 65(1)(a) GDPR): cfr. Il sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted\\_it](https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_it).

<sup>67</sup> In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited), 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, reperibile al sito Internet [https://edpb.europa.eu/system/files/2023-05/final\\_for\\_issue\\_ov\\_transfers\\_decision\\_12-05-23.pdf](https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf).

<sup>68</sup> Data la gravità della violazione, l'EDPB aveva ritenuto che il punto di partenza per il calcolo della multa dovesse essere compreso tra il 20% e il 100% del massimo legale applicabile: cfr. press release [https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision\\_en](https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en). Il 24 maggio 2023 sono state adottate dall'EDPB le Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie, reperibili al sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under\\_it](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_it).

<sup>69</sup> *Ibidem*. Secondo il Presidente dell'EDPB, Andrea Jelinek, «Meta IE's infringement is very serious since it concerns transfers that are systematic, repetitive and continuous. Facebook has millions of users in Europe, so the volume of personal data transferred is massive. The unprecedented fine is a strong signal to organisations that serious infringements have far-reaching consequences».

questioni pregiudiziali sollevate dal giudice del rinvio riguardava appunto la competenza di un'autorità nazionale garante della concorrenza ad esaminare, in via principale o incidentale, i comportamenti di un'impresa alla luce di talune disposizioni del regolamento 2016/679.

In base alla sentenza del 4 luglio 2023 della Grande Sezione, l'autorità antitrust, nell'ambito dell'indagine relativa all'abuso di posizione dominante da parte di un'impresa, può verificare anche la conformità del comportamento di tale impresa a norme diverse da quelle rientranti nel diritto della concorrenza, quali quelle contenute nel RGPD<sup>70</sup>. Qualora venga riscontrata una violazione di tale regolamento, l'autorità competente per la concorrenza non si sostituisce comunque ai garanti della privacy<sup>71</sup>. La valutazione del rispetto del RGPD, operata dalla prima, è infatti limitata al solo fine di constatare un abuso di posizione dominante e di imporre misure volte a far cessare tale abuso secondo le regole proprie del diritto della concorrenza<sup>72</sup>. Tuttavia, sebbene non vi siano disposizioni specifiche nel RGPD in merito al coinvolgimento di autorità competenti in diversi ambiti, esse sono tutte vincolate dal principio di leale collaborazione sancito dall'art. 4, par. 3, TUE, in modo da rispettare gli obblighi e gli obiettivi del regolamento e salvaguardare così il loro *effet utile*<sup>73</sup>.

Ne deriva che, da un punto di vista operativo, qualora l'autorità nazionale garante della concorrenza ritenga che sia necessario esaminare la conformità di un comportamento di un'impresa al RGPD, essa deve verificare se tale comportamento sia già stato oggetto di una decisione da parte del garante della privacy competente oppure della capofila, o, ancora, della Corte<sup>74</sup>. Se così fosse, l'autorità antitrust non può discostarsene, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza<sup>75</sup>. In caso di dubbi sulla portata di suddetta decisione, qualora il comportamento dell'impresa risulti essere oggetto di un'indagine da parte dei garanti della privacy coinvolti oppure se, in assenza di un'indagine o di una decisione da parte di tali autorità, il garante della concorrenza ritiene che vi sia una violazione del RGPD, questi deve consultare le suddette autorità di controllo e chiedere la loro collaborazione, allo scopo vuoi di dissipare i propri dubbi vuoi di stabilire se sia opportuno attendere una loro decisione prima di adottare la propria valutazione. In assenza di obiezioni da parte loro o di una risposta entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine<sup>76</sup>.

In altri termini, quando si verifica una violazione della privacy che integra anche un illecito antitrust, le autorità rispettivamente competenti devono cooperare lealmente e coordinare le proprie indagini, la conseguente adozione di provvedimenti e comminazione di sanzioni<sup>77</sup> affinché venga garantita l'applicazione uniforme del diritto UE rilevante.

---

<sup>70</sup> Corte di giustizia (Grande Sezione), sentenza del 4 luglio 2023, *Meta Platforms*, cit., punto 48.

<sup>71</sup> *Ivi*, punto 49.

<sup>72</sup> *Ibidem*.

<sup>73</sup> *Ivi*, punti 42 ss., 53 ss. e 62. Cfr. anche le conclusioni dell'Avvocato generale Rantos presentate il 20 settembre 2022, causa C-252/21, *Meta Platforms e a. c. Bundeskartellamt*. EU:C:2022:704, punto 28 (su cui v. A.R. MARTINEZ, *Processing of Personal Data Inside Out: the Opinion of AG Rantos in C-252/21*, in *Kluwer Competition Law Blog*, 22 September 2022).

<sup>74</sup> Corte di giustizia (Grande Sezione), sentenza del 4 luglio 2023, *Meta Platforms*, cit., punto 56.

<sup>75</sup> *Ibidem* e punto 63.

<sup>76</sup> *Ivi*, punti 57-59 e 63.

<sup>77</sup> Sul coordinamento tra procedimenti e autorità, nonché sulla determinazione delle sanzioni alla luce del divieto di duplice incriminazione - non affrontati in queste sede - si vedano le sentenze del 22 marzo 2022 della Corte di giustizia (Grande Sezione), causa C-117/20, *bpost SA c. Autorité belge de la concurrence*, EU:C:2022:202, spec. punto 51 ss., e causa C-151/20, *Bundeswettbewerbsbehörde (Autorità federale garante della concorrenza*

Da ultimo occorre fare riferimento alla nuova normativa indirizzata alle piattaforme digitali contenuta nel *Digital Markets Act*<sup>78</sup>. In base a questo regolamento, spetta alla Commissione il controllo del rispetto delle disposizioni ivi contenute<sup>79</sup>, da esercitare in collaborazione con le autorità degli Stati membri competenti in materia. Vengono così ridefinite le competenze materiali degli organi nazionali mediante un accentramento in capo alla Commissione, rendendo così indispensabile un coordinamento tra le autorità di volta in volta coinvolte quando una fattispecie riguarda diversi profili di violazione<sup>80</sup>.

In generale, la regolamentazione contenuta nel DMA mira a impedire abusi di posizione dominante e contiene infatti disposizioni per disciplinare il funzionamento dei mercati digitali, stabilendo una serie di obblighi in capo alle imprese che si pongono come punti di riferimento centrali nel disciplinare l'accesso al mercato, i cd. *gatekeepers*<sup>81</sup>. Lo scopo del DMA è quello di cercare di contenere la posizione dominante delle grandi piattaforme online e favorire un sistema economico nel quale anche le imprese europee, di minori dimensioni e di ridotto potere

---

*austriaca*) c. *Nordzucker AG e a.*, EU:C:2022:203. Con riguardo alla cooperazione tra autorità, cfr. anche sentenza del 30 marzo 2023, causa C-5/22, *Green Network (Ordine di restituzione di somme addebitate)*, EU:C:2023:273, in merito all'applicazione della direttiva 2009/72/CE del 13 luglio 2009, relativa a norme comuni per il mercato interno dell'energia elettrica e che abroga la direttiva 2003/54/CE, nell'ambito di una controversia riguardante la decisione dell'Autorità italiana di regolazione per energia reti e ambiente (ARERA) adottata nei confronti della Green Network S.p.A., condannata a pagare una sanzione amministrativa pecuniaria e a restituire ai clienti finali la somma corrispondente a costi di gestione amministrativa riscossi in base a clausole ritenute illegittime. Su tale aspetto, la Corte di giustizia ha chiarito che, in base all'art. 36 della direttiva in parola, l'autorità di regolazione nazionale può adottare le misure necessarie «in stretta consultazione con altre autorità nazionali pertinenti, incluse le autorità garanti della concorrenza, se del caso, e fatte salve le rispettive competenze», nonché, ai sensi dell'art. 37, «in collaborazione con altre autorità competenti» (punto 26). Pertanto, non viene imposto che «soltanto una di queste altre autorità nazionali possa ordinare la restituzione delle somme indebitamente riscosse dalle società elettriche presso i clienti finali. Al contrario, l'impiego dei termini “se del caso” implica che tale consultazione è necessaria unicamente qualora la misura che si intende adottare possa avere implicazioni per altre autorità competenti» (*ibidem*).

<sup>78</sup> Per un inquadramento del DMA, v. i contributi di P. MANZINI, *Equità e contendibilità dei mercati digitali: il Digital Markets Act*; C. OSTI, *Il Digital Markets Act tra regolazione e concorrenza*; V. FALCE, N. FARAONE, *Digital Markets Act: profili istituzionali*; C. SCHEPISI, *Digital Markets Act e private enforcement*, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea sui mercati*, Bari, 2021, pp. 99-167; nonché T. HOEHN, J. MENEZES, A. YOUNG, *Big Tech remedies - recent antitrust case law and legislative developments*, in *European Competition Law Review*, 2023, n. 44(2), pp. 47-60, spec. p. 54 ss.; A. ANDREANGELI, *The Digital Markets Act and the enforcement of EU competition law: some implications for the application of articles 101 and 102 TFEU in digital markets*, in *European Competition Law Review*, 2022, n. 43(11), pp. 496-504; C. ETTELDORF, *DMA - Digital Markets Act or Data Markets Act? Reports: European Union*, in *European Data Protection Law Review*, 2022, n. 2, pp. 255-261; G. CONTALDI, *La proposta della Commissione europea di adozione del “Digital Markets Act”*, in *Papers di diritto europeo*, 2021, n. 1, pp. 73-88; M. LIBERTINI, *Digital markets and competition policy. Some remarks on the suitability of the Antitrust toolkit*, in *Orizzonti del Diritto Commerciale*, fascicolo speciale, 2021, pp. 337-357; C. MASSA, *Ultimi sviluppi della riforma del digitale in Europa: il Digital Markets Act tra costituzionalismo europeo e concorrenza*, in *Annali AISDUE*, 7, 29 dicembre 2021, pp. 128-152.

<sup>79</sup> Sul punto, v. V. FALCE e N.M.F. FARAONE,  *Mercati digitali e DMA: note minime in tema di enforcement*, in *Il Diritto industriale*, 2022, n. 1, pp. 5-16.

<sup>80</sup> Cfr. artt. 37 e 38 del DMA; nonché v. il considerando 86, dove viene fatto riferimento alla possibilità di procedimenti paralleli nei confronti di una medesima impresa e si prevede che «la Commissione dovrebbe tenere conto di eventuali ammende e penalità irrogate alla stessa persona giuridica per gli stessi fatti mediante una decisione definitiva nei procedimenti relativi a una violazione di altre norme dell'Unione o nazionali, in modo da garantire che l'importo complessivo delle ammende e delle penalità irrogate corrisponda alla gravità delle infrazioni commesse».

<sup>81</sup> Sulla determinazione del mercato rilevante, v., da ultimo, L. SOLEK, *Concept of dominance in the digital age*, in *European Competition Law Review*, 2023, n. 44(5), pp. 194-200; nonché C. OSTI, *Market Power and Market Definition in the Digital Economy*, in V. FALCE (ed.), *Competition law enforcement in digital markets*, cit., pp. 33-44.

di mercato, possano partecipare al mercato dei dati. Come osservato dalla Commissione in sede di proposta, i comportamenti anticoncorrenziali potrebbero portare a «risultati inefficienti nel settore digitale in termini di prezzi più elevati, qualità inferiore, nonché meno scelta e innovazione a scapito dei consumatori europei»<sup>82</sup>.

In caso di violazione del regolamento sui mercati digitali, le imprese inadempienti potrebbero essere perseguite altresì per abuso di posizione dominante, che potrebbe essere concretamente realizzato tramite trattamenti illeciti dei dati. Ne deriva che le autorità nazionali incaricate nei rispettivi ambiti materiali, ma solo la Commissione con riguardo al DMA, possono agire per sanzionare le violazioni e imporre l'adozione di misure riparative. Non solo, gli esiti dei procedimenti e i relativi provvedimenti potrebbero ben essere prodotti nel contesto dei giudizi promossi eventualmente davanti alle autorità giurisdizionali competenti.

**4.2.** Un'altra prospettiva secondo cui ripercorrere il sistema dei rimedi, che emerge dal quadro normativo europeo applicabile in caso di violazioni della privacy e delle regole antitrust, concerne la possibilità di presentare reclami e di instaurare azioni giudiziali individuali oppure collettive, per chiedere l'accertamento della violazione, la sua cessazione e il risarcimento dei danni, la cui esistenza deve essere provata dal ricorrente.

Nel contesto del RGPD<sup>83</sup>, come previsto dall'art. 77, che fa salvo ogni altro ricorso amministrativo o extragiudiziale disponibile<sup>84</sup>, il titolare dei dati può presentare un reclamo all'autorità di controllo nello Stato membro in cui il titolare risiede abitualmente o lavora oppure ove si è verificata la presunta violazione<sup>85</sup>. In base all'art. 78, è possibile impugnare le decisioni del garante nazionale per la privacy<sup>86</sup> davanti al giudice ordinario del luogo dove questo è stabilito. Il successivo art. 79 riconosce la facoltà di presentare ricorso contro il titolare o il responsabile del trattamento, con azioni volte quindi ad accertare la violazione e chiederne la cessazione e che possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui si trova un loro stabilimento. In alternativa, tali azioni possono essere promosse nello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri<sup>87</sup>. È opportuno altresì notare che, come indicato nel considerando 147, le disposizioni specifiche in materia di giurisdizione stabilite nel RGPD prevalgono sulle regole generali già previste nell'ordinamento dell'Unione, quali quelle di cui al regolamento (UE) n. 1215/2012<sup>88</sup>. Per i casi di litispendenza di azioni promosse davanti a giudici di diversi Stati

---

<sup>82</sup> Proposta della Commissione COM(2020)842 final cit., par. 1.

<sup>83</sup> Per un commento alle disposizioni in esame, v. Per una analisi della norma, v. E. BELISARIO, G.M. RICCIO, G. SCORZA (a cura di), *GDPR e Normativa Privacy. Commentario*, cit., p. 703 ss.

<sup>84</sup> Così come ribadito anche negli articoli successivi in materia di diritto di difesa.

<sup>85</sup> Sono disponibili modelli di reclamo ex art. 77 RGPD al sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/other/template-complaint-form-and-template-acknowledgement-receipt\\_it](https://edpb.europa.eu/our-work-tools/our-documents/other/template-complaint-form-and-template-acknowledgement-receipt_it).

<sup>86</sup> Per l'ordinamento italiano, si vedano gli artt. 143 e 152 del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196 e succ. modif., in *GU* n. 174 del 29 luglio 2003 - Suppl. Ordinario n. 123).

<sup>87</sup> Su cui v. anche considerando 144 e 145 del RGPD.

<sup>88</sup> Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (rifusione), in *GUUE*, L 351 del 20 dicembre 2012, pp. 1-32.

membri, l'art. 81 del RGPD prevede la sospensione del giudizio promosso successivamente, quando la competenza del giudice preventivamente adito è stata accertata.

Si aggiunge poi la possibilità, ai sensi dell'art. 82, di richiedere il risarcimento del danno materiale o immateriale<sup>89</sup> causato dalla violazione di una disposizione del RGPD nei confronti del titolare o del responsabile del trattamento<sup>90</sup>. Per l'individuazione del giudice competente si applica la regola di cui all'art. 79, par. 2, poc'anzi descritta<sup>91</sup>. La determinazione del tipo di danno e la quantificazione dello stesso devono avvenire in base alle norme nazionali, secondo le categorie proprie dell'ordinamento coinvolto. Ciò è stato confermato dalla Corte di giustizia con la sentenza del 4 maggio 2023 nella causa *Österreichische Post*<sup>92</sup>. La controversia riguardava l'azione promossa da una persona fisica, UI, nei confronti di un'impresa che raccoglieva informazioni sulle affinità della popolazione austriaca in relazione ai gruppi politici, dalle quali risultava una sua preferenza per un partito. Tuttavia, il ricorrente UI non aveva mai prestato il consenso al trattamento dei propri dati personali. Instaurava perciò un'azione per risarcimento dei danni immateriali, pari a un importo di mille euro, a causa del disagio sofferto per la registrazione di informazioni relative al suo orientamento politico e per l'affinità politica che gli è stata attribuita, in quanto offensiva e lesiva della sua immagine. In primo e secondo grado la domanda veniva però respinta; il ricorrente impugnava quindi la decisione davanti alla Corte suprema austriaca, che sospendeva il giudizio e proponeva il rinvio pregiudiziale relativo all'interpretazione dell'art. 82 RGPD per determinare la natura del danno risarcibile.

I giudici di Lussemburgo hanno osservato che il diritto al risarcimento è dovuto quando tre condizioni cumulative sono soddisfatte, vale a dire la violazione del RGPD, il danno materiale o immateriale derivante da tale violazione e il nesso di causalità tra danno e violazione<sup>93</sup>. Ne consegue che la mera violazione del regolamento di per sé non dà diritto al risarcimento, ma occorre dimostrare i danni sofferti, di qualunque natura, materiale o immateriale, senza che per questo secondo tipo sia necessario raggiungere una determinata soglia di gravità<sup>94</sup>. Spetta agli Stati membri, nel prevedere le azioni esperibili in caso di violazioni del RGPD, fissare anche i criteri che consentono di determinare l'entità del risarcimento, sempre nel rispetto dei principi di equivalenza ed effettività. Ciò deve avvenire alla luce del regolamento, che conferisce al diritto al risarcimento del danno una funzione compensativa e impone di assicurare un risarcimento pieno ed effettivo del danno subito<sup>95</sup>.

---

<sup>89</sup> Cfr. considerando 85 del RGPD dove viene affermato che «[u]na violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifrazione non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata (...)».

<sup>90</sup> V. anche considerando 146 del RGPD.

<sup>91</sup> Per l'ordinamento italiano, competente è sempre il giudice ordinario (art. 152 del Codice della privacy).

<sup>92</sup> Corte di giustizia, sentenza del 4 maggio 2023, causa C-300/21, *UI c. Österreichische Post AG*, EU:C:2023:370, in tal senso, v. anche le conclusioni dell'Avvocato generale Sánchez-Bordona, presentate il 6 ottobre 2022, EU:C:2022:756. Pur essendo la fattispecie puramente interna, l'interpretazione della Corte può essere applicata anche a situazioni transfrontaliere. Per un commento, v. A. LOTTINI, *Risarcimento del danno immateriale a seguito della violazione del regolamento (UE) 2016/679: la sentenza Österreichische Post determina un cambio di paradigma?*, in *BlogDUE*, 7 luglio 2023.

<sup>93</sup> Corte di giustizia, sentenza del 4 maggio 2023, *Österreichische Post*, cit., punto 32 ss.

<sup>94</sup> *Ivi*, punto 43 ss.

<sup>95</sup> *Ivi*, punto 57 ss.

Nel sistema del RGPD, i ricorsi davanti al giudice ordinario possono quindi essere esperiti vuoi per impugnare una decisione del garante, vuoi per far valere la violazione commessa dal titolare o dal responsabile del trattamento dei dati, vuoi, infine, per chiedere il risarcimento del danno. Il rapporto esistente tra tali mezzi di ricorso è stato oggetto della sentenza della Corte di giustizia del 12 gennaio 2023, nella causa *Budapesti Elektromos Művek*<sup>96</sup>. La controversia riguardava una persona fisica, BE, e l'autorità ungherese incaricata della protezione dei dati e della libertà dell'informazione in merito al rigetto della domanda di BE volta a ottenere la comunicazione di segmenti del fonogramma di un'assemblea generale degli azionisti di una società, la Budapesti Elektromos Művek, alla quale questi aveva partecipato. BE si era rivolto al garante nazionale ex art. 77 RGPD per chiedere di dichiarare che, non avendo rilasciato il suddetto fonogramma e neppure fornito chiarimenti, la società aveva agito in modo illegittimo e in violazione del regolamento stesso, nonché di ordinare alla stessa di mettere a disposizione il fonogramma in questione. L'autorità aveva però respinto il reclamo con decisione del 29 novembre 2019, contro la quale BE aveva proposto un ricorso dinanzi alla Corte di Budapest, ai sensi dell'art. 78, par. 1, per ottenere la modifica, in via principale, o l'annullamento, in subordine, di detta decisione. Parallelamente, aveva proposto un secondo ricorso ai sensi dell'art. 79, par. 1, davanti a un giudice civile, la Corte d'appello regionale di Budapest, contro la decisione del responsabile del trattamento dei dati. Con sentenza passata in giudicato era stato accolto questo secondo ricorso riconoscendo che il titolare del trattamento aveva violato il diritto di accesso di BE ai suoi dati personali.

Il primo di tali ricorsi, invece, pende davanti al giudice amministrativo che ha presentato il rinvio, domandando se, in forza delle disposizioni del RGPD, la sentenza definitiva adottata da un giudice, adito ai sensi dell'art. 79, par. 1, di detto regolamento, sia vincolante anche per gli altri organi giurisdizionali per quanto riguarda l'accertamento dell'esistenza o meno di una violazione dei diritti garantiti dal medesimo regolamento. La Corte di giustizia ha interpretato le norme sui rimedi previsti dal RGPD nel senso che «essi consentono un esercizio concorrente e indipendente dei mezzi di ricorso previsti, da un lato, da tale art. 77, par. 1, e da tale art. 78, par. 1, nonché, dall'altro, da tale art. 79, par. 1. Spetta agli Stati membri, in linea con il principio dell'autonomia procedurale, prevedere le modalità di articolazione di tali mezzi di ricorso affinché siano garantiti l'efficacia della protezione dei diritti garantiti da tale regolamento, l'applicazione coerente ed omogenea delle disposizioni dello stesso nonché il diritto a un ricorso effettivo dinanzi a un giudice, come sancito dall'art. 47 della Carta dei diritti fondamentali»<sup>97</sup>.

In altri termini, la disciplina dei mezzi di difesa predisposti negli ordinamenti interni, pur se esperibili parallelamente davanti ad autorità diverse, deve comunque impedire esiti contrastanti dei relativi giudizi, rischiando altrimenti di pregiudicare la tutela dei diritti, nonché l'applicazione coerente e omogenea delle norme del RGPD.

Anche nel sistema antitrust<sup>98</sup>, all'intervento da parte delle autorità preposte si aggiunge la possibilità di instaurare azioni giudiziali per richiedere il risarcimento del danno, disciplinate

---

<sup>96</sup> Corte di giustizia, sentenza del 12 gennaio 2023, causa C-132/21, *BE c. Budapesti Elektromos Művek*, EU:C:2023:2.

<sup>97</sup> *Ivi*, punto 57.

<sup>98</sup> Per un inquadramento del *private enforcement*, v., tra i molti, i contributi in M. CONDINANZI, J. ALBERTI, F. CROCI (a cura di), *Il private antitrust enforcement nelle Corti milanesi: una prospettiva europea*, in *Eurojus*,

dalla direttiva 2014/104<sup>99</sup>, trasposta nell'ordinamento italiano con decreto legislativo 19 gennaio 2017, n. 3<sup>100</sup>. Tale disciplina riconosce la facoltà alle imprese di impugnare le decisioni del garante per la concorrenza davanti al giudice amministrativo. Gli interessati che hanno subito danni possono ricorrere davanti al giudice ordinario<sup>101</sup>, in particolare alle sezioni specializzate in materia d'impresa, per chiederne il risarcimento. Nell'ambito di questi giudizi privati è possibile far valere la violazione delle norme sulla concorrenza producendo la decisione amministrativa divenuta definitiva, quando anche accertata dai giudici competenti<sup>102</sup>.

Per quanto riguarda, infine, il sistema di *enforcement* delineato nel regolamento del 2022 sui mercati digitali, oltre al ruolo della Commissione in collaborazione con le autorità nazionali, manca un riferimento ai rimedi giurisdizionali<sup>103</sup> o almeno una disposizione che imponga agli

---

fascicolo speciale, giugno 2020; F. MUNARI, M. BARBANO, *La Direttiva Damages: dalle origini del sistema europeo di private antitrust enforcement alla Dir. 104/2014*, in L.F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*, cit., pp. 357-372; C. FRATEA, *Il private enforcement del diritto della concorrenza dell'Unione europea. Profili europei, internazionalprivatistici e interni*, Napoli, 2015, spec. p. 47 ss.; nonché A. SAIJA, *Protezione dei dati personali*, cit., p. 111 ss., dove, per quanto rileva ai nostri fini, osserva che le constatazioni di infrazioni antitrust hanno efficacia vincolante nelle azioni risarcitorie follow-on, mentre manca una previsione normativa che stabilisca il valore probatorio dei provvedimenti che accertano pratiche scorrette o violazioni della normativa sulla privacy.

<sup>99</sup> Direttiva 2014/104/UE del Parlamento europeo e del Consiglio, del 26 novembre 2014, relativa a determinate norme che regolano le azioni per il risarcimento del danno ai sensi del diritto nazionale per violazioni delle disposizioni del diritto della concorrenza degli Stati membri e dell'Unione europea, in *GUUE*, L 349 del 5 dicembre 2014, pp. 1-19.

<sup>100</sup> Decreto legislativo 19 gennaio 2017, n. 3 Attuazione della direttiva 2014/104/UE, in *GU Serie Generale* n. 15 del 19 gennaio 2017.

<sup>101</sup> Per la determinazione del giudice competente, v. C. FRATEA, *Il private enforcement del diritto della concorrenza*, cit., p. 109 ss.

<sup>102</sup> Ciò è stato confermato dalla Corte di giustizia, sentenza del 20 aprile 2023, causa C-25/21, *Repsol Comercial de Productos Petrolíferos*, EU:C:2023:298, nell'ambito di una controversia – non in materia di privacy – tra la Repsol e gli eredi di KN, proprietari di una stazione di servizio, che avevano promosso azioni dirette a far dichiarare la nullità dei contratti conclusi con la società, nonché al risarcimento dei relativi danni. L'autorità antitrust spagnola aveva constatato, in due occasioni, la violazione delle norme sulla concorrenza da parte della Repsol per aver fissato, nell'ambito dei suoi rapporti contrattuali con talune stazioni di servizio spagnole, i prezzi di vendita al pubblico dei carburanti. Le decisioni venivano impuginate dalla Repsol, ma i ricorsi erano stati respinti e quindi le decisioni acquisivano carattere definitivo. I proprietari di una stazione di servizio avevano proposto dinanzi al Tribunale del commercio n. 2 di Madrid un'azione diretta a far dichiarare la nullità dei contratti di fornitura esclusiva stipulati con la Repsol e un'azione per il risarcimento del danno asseritamente causato da tali contratti, producendo nell'ambito dei procedimenti le suddette decisioni del garante spagnolo per dimostrare l'esistenza della violazione di cui trattasi. Il giudice nazionale di rinvio però si interrogava sull'effetto vincolante di tali decisioni per quanto riguarda l'esistenza di una violazione delle norme del diritto della concorrenza e su quali conseguenze trarre dall'eventuale nullità dei contratti di fornitura esclusiva stipulati tra i proprietari della stazione di servizio e la Repsol. La Corte di giustizia ha chiarito che «la violazione del diritto della concorrenza constatata in una decisione di un'autorità nazionale garante della concorrenza, che è stata oggetto di un ricorso di annullamento dinanzi ai giudici nazionali competenti ma che è divenuta definitiva dopo essere stata confermata da tali giudici, deve ritenersi dimostrata dal ricorrente, tanto nell'ambito di un'azione di nullità ai sensi dell'art. 101, par. 2, TFUE quanto di un'azione per il risarcimento del danno per una violazione dell'art. 101 TFUE, fino a prova contraria, trasferendo così l'onere della prova definito da tale art. 2 sul convenuto, a condizione che la natura dell'asserita violazione oggetto di tali azioni e la sua portata materiale, personale, temporale e territoriale coincidano con quelle della violazione constatata in detta decisione» (punto 67). Si era espresso in questo senso anche l'Avvocato generale Pitruzzella, il quale aveva proposto di rispondere al quesito in questi termini: «Il principio di effettività e l'esigenza di garantire la piena efficacia dell'art. 101 TFUE, oltre al principio della certezza del diritto, impongono di riconoscere all'accertamento definitivo di una violazione dell'art. 101, par. 1, TFUE compiuto dall'autorità nazionale garante della concorrenza quantomeno un valore di indizio o principio di prova ai fini dell'azione civile» (conclusioni presentate l'8 settembre 2022, EU:C:2022:659, punto 117).

<sup>103</sup> C. SCHEPISI, *Digital Markets Act e private enforcement*, cit., p. 155 ss.

Stati di prevedere mezzi di tutela effettivi<sup>104</sup>. Ciò non esclude tuttavia la possibilità di ricorrere in giudizio, a fini essenzialmente risarcitori, in caso di violazione degli obblighi imposti nel regolamento<sup>105</sup>, valendo il principio generale del diritto a rimedi giurisdizionali effettivi e non essendo pertanto necessaria una disposizione legislativa esplicita in tal senso<sup>106</sup>. D'altro canto, la previsione di cui all'art. 42 del DMA sulle azioni rappresentative, su cui si tornerà tra breve, potrebbe far sorgere dubbi in merito alla loro espressa menzione, contrariamente a quanto avviene per i ricorsi individuali e tenuto conto del fatto che è in vigore una direttiva in materia con portata trasversale<sup>107</sup>. E ancora, sempre nel DMA, compare comunque un riferimento ai giudici interni: è infatti prevista la cooperazione tra Commissione e organi giurisdizionali nazionali qualora vi siano procedimenti relativi all'applicazione del regolamento ai fini dello scambio di informazioni (art. 39, par. 1), nonché tra Commissione e Stati membri per condividere le sentenze emesse in merito al regolamento (art. 39, par. 2). Questa considerazione in relazione al ruolo dei giudici nell'applicazione del regolamento sui mercati digitali richiama così, implicitamente, l'esperibilità di azioni giudiziali.

Nel contesto del *private enforcement* è altresì rilevante esaminare le disposizioni che riconoscono la possibilità di intentare ricorsi collettivi<sup>108</sup>. Un importante sviluppo nel quadro normativo europeo si è ottenuto, come poc'anzi accennato, con l'adozione della direttiva (UE) 2020/1828 sulle azioni rappresentative a tutela dei consumatori<sup>109</sup>, che abroga la precedente direttiva 2009/22 e si applica dal 25 giugno 2023. Nell'ordinamento italiano si è assistito a una riforma importante con la legge 12 aprile 2019, n. 31<sup>110</sup>, applicabile dal 19 maggio 2021, che introduce una disciplina trasversale per le azioni di classe, esperibili in diversi settori, posto che le nuove regole sono state collocate nel Codice di procedura civile<sup>111</sup>. Con decreto legislativo 10 marzo 2023, n. 28<sup>112</sup> è stata data attuazione alla direttiva europea sulle azioni

---

<sup>104</sup> Vale a dire includendo nel regolamento una disposizione che riprende la classica formulazione in tema di diritti di difesa che compare in altri atti normativi UE.

<sup>105</sup> C. SCHEPISI, *Digital Markets Act e private enforcement*, cit., p. 159 ss. per l'individuazione delle disposizioni invocabili in giudizio.

<sup>106</sup> *Ivi*, p. 157. Sul punto, si veda anche R. PODSZUN, *Private Enforcement and Gatekeeper Regulation: Strengthening the Rights of Private Parties in the Digital Markets Act*, in *Journal of European Competition Law & Practice*, 2022, n. 13(4), pp. 254-267.

<sup>107</sup> In merito alla direttiva in parola e alle azioni rappresentative, indicate nell'art. 42, v. *infra*.

<sup>108</sup> Per un inquadramento generale sull'evoluzione della disciplina UE in materia di ricorsi collettivi, v. G. DE CRISTOFARO, *Azioni "rappresentative" e tutela degli interessi collettivi dei consumatori. La "lunga marcia" che ha condotto all'approvazione della dir. 2020/1828/UE e i profili problematici del suo recepimento nel diritto italiano*, in *Le Nuove Leggi Civili e Commentate*, 2022, n. 4, pp. 1010-1051; F. BATTAGLIA, *Recenti novità in materia di azioni rappresentative a tutela degli interessi collettivi dei consumatori nell'Unione europea*, in *Studi sull'integrazione europea*, 2021, n. 2, pp. 335-362; nonché sia consentito rinviare a C. PERARO, *Diritti fondamentali sociali e tutela collettiva nell'Unione europea*, Napoli, 2020, spec. p. 153 ss.

<sup>109</sup> Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE, in *GUUE*, L 409 del 4 dicembre 2020, pp. 1-27.

<sup>110</sup> Legge 12 aprile 2019, n. 31, Disposizioni in materia di azione di classe, in *GU Serie Generale* n. 92 del 18 aprile 2019. Per un commento, v. N. RUMINE, *Natura e forme civilistiche di tutela degli interessi collettivi dei consumatori*, Pisa, 2022, spec. p. 224 ss.

<sup>111</sup> Cfr. Libro IV, Titolo VIII bis, artt. 840 bis - 840 sexiesdecies del Codice di procedura civile.

<sup>112</sup> Attuazione della direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE, in *GU* n. 70 del 23 marzo 2023.

rappresentative, apportando modifiche al Codice del consumo<sup>113</sup>. Pertanto, la normativa nazionale di recepimento riguarda solamente le azioni collettive in rappresentanza degli interessi dei consumatori e prevale, in questi casi, sulla disciplina delineata nel Codice di procedura civile. Nello specifico, ai sensi dell'art. 2, la direttiva (UE) 2020/1828 e, quindi, le norme nazionali di trasposizione si applicano alle azioni rappresentative intentate nei confronti di professionisti per violazioni, nazionali e transfrontaliere, delle disposizioni del diritto dell'Unione di cui all'allegato I, che contiene un elenco di atti UE, nonché delle disposizioni di recepimento nel diritto nazionale, che ledono o possono ledere gli interessi collettivi dei consumatori. Nell'elenco vengono menzionati il RGPD, il DMA<sup>114</sup>, ma anche normative riguardanti le comunicazioni elettroniche, la fornitura di contenuti e servizi digitali<sup>115</sup>, il geoblocking, la portabilità di servizi di contenuti online, alle quali sono perciò applicabili le norme europee sulle *class action*.

Nel regolamento sui dati personali, l'art. 80 è dedicato alla rappresentanza degli interessati<sup>116</sup> e prevede la facoltà di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, costituiti secondo il diritto nazionale, al fine di proporre, per conto degli interessati, il reclamo e di esercitare i diritti di cui agli artt. 77, 78 e 79, nonché, se previsto dal diritto dello Stato membro coinvolto, il diritto di ottenere il risarcimento di cui all'art. 82. Dipende poi dalla normativa nazionale la possibilità per le suddette entità di proporre, indipendentemente dal mandato conferito dall'interessato, reclami o azioni giudiziali.

In una controversia con (ancora) protagonista la Meta Platforms<sup>117</sup>, riguardante la violazione da parte della società della legislazione tedesca in materia di protezione dei dati personali, l'Unione federale tedesca dei consumatori aveva proposto un'azione inibitoria, indipendentemente dalla violazione concreta del diritto alla tutela dei dati di un interessato e senza un mandato<sup>118</sup>. Il Tribunale del Land di Berlino aveva condannato la Meta Platforms, che

---

<sup>113</sup> Cfr. Parte V del Codice del consumo, laddove dopo il Titolo II è stato aggiunto il "Titolo II.1 Azioni rappresentative a tutela degli interessi collettivi dei consumatori", con entrata in vigore il 7 aprile 2023 e applicazione delle disposizioni a decorrere dal 25 giugno 2023.

<sup>114</sup> A tal riguardo, si veda l'art. 42 del DMA ai sensi del quale: «La direttiva (UE) 2020/1828 si applica alle azioni rappresentative intentate contro le violazioni, da parte dei gatekeeper, delle disposizioni del presente regolamento che ledono o possono ledere gli interessi collettivi dei consumatori».

<sup>115</sup> Si veda la Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, in *GUUE*, L 136 del 22 maggio 2019, pp. 1-27, recepita in Italia con decreto legislativo 4 novembre 2021, n. 173, in *GU Serie Generale* n. 282 del 26 novembre 2021, con applicazione dal 1° gennaio 2022, così come indicato nella direttiva stessa. Per alcuni commenti sulla disciplina ivi contenuta con riferimento alla definizione dei tipi di contratti, v. V. RICCIUTO, *L'equivoco della privacy*, cit., p. 161 ss.

<sup>116</sup> Cfr. anche il considerando 142 del RGPD. Per alcune considerazioni in merito, v. M. FEDERICO, *European Collective Redress and Data Protection. Challenges and Opportunities*, in *Media Laws – Rivista di Diritto dei Media*, 2023, n. 1; J. KNETSCH *Les actions civiles en réparation fondées sur une violation du RGPD. Vers un nouveau contentieux de masse?*, in *La semaine juridique*, 26 settembre 2022, n. 38, pp. 1733-1740; nonché, tra i molti, E. BELISARIO, G.M. RICCIO, G. SCORZA (a cura di), *GDPR e Normativa Privacy. Commentario*, cit., p. 712 ss.

<sup>117</sup> Corte di Giustizia, sentenza del 28 aprile 2022, causa C-319/20, *Meta Platforms Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.*, EU:C:2022:322.

<sup>118</sup> La vicenda richiama la controversia oggetto di una *class action* avviata oltreoceano (la cui disciplina si differenzia da quella europea) sempre nei confronti di Meta Platforms per violazione della privacy causata dalla rivelazione di informazioni di milioni di utenti condivise con la società di data analysis Cambridge Analytica. L'accordo di *settlement* era stato raggiunto in dicembre 2022 e a marzo 2023 la Corte distrettuale di San Francisco (California) ha emesso l'«order certifying settlement class; granting preliminary approval of class action settlement

aveva poi impugnato la decisione dinanzi al Tribunale superiore. Respinto l'appello, la Meta Platforms aveva quindi ricorso per cassazione. La Corte federale di giustizia tedesca nutrivava però dei dubbi in merito alla ricevibilità dell'azione dell'Unione federale e quindi sull'interpretazione dell'art. 82, par. 2 del RGPD in tema di ricorso collettivo finalizzato a chiedere il risarcimento del danno.

Con sentenza del 28 aprile 2022, la Corte di giustizia ha stabilito che è compatibile con la disposizione in parola una normativa nazionale che consente ad un'associazione di tutela degli interessi dei consumatori di agire in giudizio, in assenza di un mandato conferitole a tale scopo e indipendentemente dalla violazione di specifici diritti degli interessati, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, al fine di far valere la violazione del divieto di pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle, qualora il trattamento di dati in questione sia idoneo a pregiudicare i diritti riconosciuti da tale regolamento a persone fisiche identificate o identificabili<sup>119</sup>. Occorre dunque verificare la normativa nazionale dell'ordinamento coinvolto per determinare la possibilità di agire per tali entità in assenza di mandato e indipendentemente da una violazione effettiva<sup>120</sup>. La tutela degli interessi collettivi in Europa potrebbe così risultare frammentata proprio a causa della disparità delle disposizioni nazionali degli Stati membri in merito, appunto, alla previsione o meno di un simile potere di agire per gli enti rappresentativi, risultando, laddove esso manchi, più difficile intervenire per proteggere i diritti delle persone.

Nell'elenco di cui alla direttiva del 2020 non viene menzionata la direttiva 2014/104 in materia di azioni antitrust<sup>121</sup>. Tuttavia, compariva un riferimento alla politica della concorrenza nei lavori preparatori all'adozione dell'atto legislativo concernente le azioni rappresentative a tutela di interessi collettivi, specialmente nella raccomandazione della Commissione dell'11 giugno 2013<sup>122</sup>. Questo silenzio non esclude comunque che in base alla direttiva del 2014 sia possibile promuovere azioni collettive<sup>123</sup>, posto che nella definizione di "azione per il

---

pursuant to federal rule of civil procedure 23(e)(1); and approving form and content of class notice», dando quindi avvio alle procedure di "claim" oppure "opt-out" per gli utenti di Facebook residenti negli Stati Uniti dal 24 maggio 2007 al 22 dicembre 2022 (v. <https://facebookuserprivacysettlement.com>).

<sup>119</sup> Sulla causa C-319/20, *Meta Platforms c. Unione federale tedesca*, v. D. SIMON, *Droits fondamentaux - Protection des données*, in *Europe*, 2022, n° 6 Juin, comm. 187; F. D'ATH, *Meta v. BVV : the CJEU clarifies the scope of the representative action mechanism of Article 80(2) GDPR whereby not-for-profit associations can bring judicial proceedings against a controller or processor : C-319/20*, in *European Data Protection Law Review*, 2022, Vol. 22, n° 8 pp. 320-323.

<sup>120</sup> In tal senso, si veda la precedente sentenza del 29 luglio 2019, causa C-40/17, *Fashion ID GmbH & Co.KG c. Verbraucherzentrale NRW eV*, EU:C:2019:629, richiamata anche dalla Corte di giustizia. Per un commento sia consentito rinviare a C. PERARO, *Legittimazione ad agire di un'associazione a tutela dei consumatori e diritto alla protezione dei dati personali*, cit.

<sup>121</sup> Sull'applicazione della direttiva del 2020 in ambito antitrust, in ottica critica, v. Assonime, circolare n. 13 del 26 aprile 2023, *La disciplina delle azioni rappresentative a tutela degli interessi collettivi dei consumatori*.

<sup>122</sup> Cfr. considerando 7 della Raccomandazione della Commissione, dell'11 giugno 2013, relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione (2013/396/UE), in *GUUE*, L 201, 26 luglio 2013, pp. 60-65.

<sup>123</sup> Per una analisi delle azioni collettive in materia antitrust, v. G. AFFERNI, *La nuova azione di classe per violazioni del diritto antitrust*, in L.F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*, cit., pp. 505-524; E. ŞAHIN, *Collective redress and EU competition law*, Abingdon, Oxfordshire, 2019; C. FRATEA, *Il private enforcement del diritto della concorrenza*, cit., p. 80 ss.; nonché, per un inquadramento prima dell'adozione della direttiva, v. B. RODGER (ed.), *Competition Law. Comparative Private Enforcement and Collective Redress across the EU*, Alphen aan den Rijn, 2014.

risarcimento del danno” di cui all’art. 2, punto 4, viene precisato che si tratta di un’azione con cui una domanda di risarcimento del danno può essere proposta dinanzi ad un’autorità giudiziaria nazionale anche da parte di «una persona che agisce per conto di uno o più presunti soggetti danneggiati, qualora quest’ultima possibilità sia prevista dal diritto dell’Unione o nazionale». In ogni caso, sempre ai sensi della medesima direttiva, non viene imposto agli Stati membri un obbligo di introdurre meccanismi di ricorso collettivo per l’applicazione degli artt. 101 e 102 TFUE<sup>124</sup>.

Da quanto sopra osservato, le azioni collettive o rappresentative sono mezzi di tutela esperibili nei diversi ambiti materiali in base alla normativa europea, che tuttavia richiede agli ordinamenti interni di disporre una disciplina specifica.

**4.3.** L’analisi degli strumenti a tutela dei soggetti titolari dei dati personali può essere infine condotta nel contesto del trasferimento extraeuropeo di tali dati<sup>125</sup>, specialmente dall’UE agli Stati Uniti<sup>126</sup>, oggetto di vicende che riguardano, di nuovo, la Meta Platforms. Si tratta di un fenomeno che è governato dalla normativa contenuta nel RGPD, basandosi in sostanza su decisioni di adeguatezza adottate dalla Commissione oppure sulla necessaria previsione di garanzie adeguate circa la protezione offerta nel paese di destinazione<sup>127</sup>, e che interessa, in particolare, le imprese extra-UE operanti nel mercato europeo, con uno stabilimento nel territorio dell’Unione, ogniquale volta trattino dati personali che vengono trasferiti fuori dai suoi confini, perché ad esempio per la raccolta e la conservazione dei dati si affidano a società che forniscono servizi digitali con sede principale oltreoceano.

Al centro dell’evoluzione giurisprudenziale e normativa relativa al profilo in esame troviamo appunto il social network americano Facebook, poi Meta Platforms. Rilevano a tal riguardo alcune sentenze della Corte di giustizia rese nella nota saga *Schrems*, con cui sono state dichiarate invalide le decisioni di adeguatezza cd. *Safe Harbour*<sup>128</sup> e *Privacy Shield*<sup>129</sup>.

---

<sup>124</sup> Cfr. considerando 13 della direttiva 2014/104.

<sup>125</sup> V. RICCIUTO, *L’equivoco della privacy*, cit., p. 68 e p. 99.

<sup>126</sup> Per una analisi dell’approccio delle due giurisdizioni in tema di tutela dei dati, v. G. CONTALDI, *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, 2021, pp. 292-308; M. MAGGIOLINO, *I big data tra Stati Uniti e Unione europea*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, cit., pp. 265-282; nonché v. la proposta dell’*American Data Privacy and Protection Act* (House of Representatives H.R. 8152) del 21 giugno 2022.

<sup>127</sup> In sintesi, la normativa prevede che il trasferimento può fondarsi su una decisione adottata dalla Commissione ai sensi dell’art. 45, con cui viene dichiarato che il paese terzo garantisce un livello di protezione adeguato, oppure, in assenza di una siffatta decisione di adeguatezza, sulla presenza, nell’ordinamento dello Stato di destinazione, di garanzie adeguate che spetta alle parti contrattuali, inclusi titolare o responsabile del trattamento, e del riconoscimento, a favore degli interessati, di diritti azionabili e mezzi di ricorso effettivi, come richiesto dall’art. 46, e ciò pur se nei rapporti contrattuali sia stato fatto riferimento alle clausole contrattuali tipo di protezione dei dati, nella specie contenute nella decisione 2010/87 (v. anche considerando 108 del RGPD). In merito, sia permesso rinviare a C. PERARO, *Protezione extraterritoriale dei diritti*, cit., spec. p. 677 ss.

<sup>128</sup> Decisione della Commissione 2000/520/CE, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull’adeguatezza della protezione offerta dai principi di approdo sicuro, annullata da Corte di giustizia (Grande Sezione), sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, EU:C:2015:650 (nota come *Schrems I*).

<sup>129</sup> Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull’adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, annullata da Corte di giustizia (Grande Sezione), sentenza del 16 luglio 2020, causa C-

Con il risultato che sono state avviate le negoziazioni, basate sul cd. *Transatlantic Data Privacy Framework*<sup>130</sup>, al fine di consentire il trasferimento legittimo dei dati dall'Unione agli Stati Uniti, che si sono concluse il 10 luglio 2023 con l'adozione della decisione di adeguatezza da parte della Commissione<sup>131</sup>.

La vicenda pone in rilievo gli aspetti problematici relativi ai *cross-border data flows* dall'UE agli USA, che hanno infatti riguardato, in particolare, i mezzi di tutela dei titolari dei dati personali, che si trovano nell'Unione europea, di fronte ad accessi indiscriminati e illegittimi che si verificano oltreoceano. Le criticità erano state affrontate, nello specifico, nella citata sentenza *Schrems II* della Corte di giustizia. In tale occasione, la Corte aveva valutato il livello di protezione predisposto dal paese terzo affermando che non dovesse essere necessariamente identico a quello garantito dall'Unione, ma, per poter essere considerato "adeguato", dovesse risultare «sostanzialmente equivalente a quello assicurato all'interno dell'Unione», ora contenuto nel RGPD, letto alla luce della Carta<sup>132</sup>. I diritti fondamentali devono infatti essere presi in considerazione per determinare il livello di protezione<sup>133</sup>, così come richiede lo stesso regolamento e, in particolare, come emerge dal suo considerando 10, che indica come obiettivo quello di protezione delle libertà e dei diritti fondamentali delle persone fisiche all'interno dell'Unione con riguardo al trattamento dei dati personali<sup>134</sup>. È in riferimento alla valutazione effettuata dai giudici di Lussemburgo che è possibile assistere all'estensione extraterritoriale degli standard europei di tutela, che diventano i criteri per accertare l'adeguatezza dell'ordinamento del paese di destinazione dei dati<sup>135</sup>. Ne consegue che

---

311/18, *Schrems II*, cit. In merito, per alcuni commenti, v. C. PERARO, *Protezione extraterritoriale dei diritti*, cit.; G. CAGGIANO, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza Schrems II della Corte di giustizia*, in *Studi sull'integrazione europea*, 2020, n. 3, pp. 563-585; G. FORMICI, *Schrems colpisce ancora? Il trasferimento dei dati personali dall'Unione europea a Stati terzi, le Conclusioni dell'Avvocato generale nel caso Data Protection Commissioner v. Facebook Ireland Limited e Maximilian Schrems e una storia che rischia di ripetersi*, in *Rivista di diritto dei media - MediaLaws*, 2020, n. 1, pp. 310-325; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, n. 3, pp. 733-759; I. OLDANI, *The future of data transfer rules in the aftermath of Schrems II*, in *SIDIBlog*, 23 ottobre 2020; F. ROSSI DAL POZZO, *L'Accordo Privacy Shield non è un vero scudo per la privacy: scenari passati e futuri in merito a trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Rivista di diritto internazionale*, 2020, n. 4, pp. 1112-1121.

<sup>130</sup> Cfr. il comunicato stampa reperibile al sito Internet [https://ec.europa.eu/commission/presscorner/detail/it/ip\\_22\\_2087](https://ec.europa.eu/commission/presscorner/detail/it/ip_22_2087).

<sup>131</sup> Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023) 4745 final (cfr. il comunicato stampa reperibile al sito Internet [https://ec.europa.eu/commission/presscorner/detail/it/ip\\_23\\_3721](https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3721)). Per alcune considerazioni, v. A. TITONE, *EU-U.S. Data Privacy Framework: è (finalmente) realtà!*, in *MediaLaws*, 17 luglio 2023.

<sup>132</sup> Sentenza *Schrems II*, cit., punto 94, e considerando 104 del RGPD. V. anche Avvocato generale Saugmandsgaard Øe, conclusioni del 19 dicembre 2019, *Schrems II*, cit., punto 248: «tale criterio non significa che il livello di protezione deve essere «identico» a quello richiesto nell'Unione. Pur se i mezzi ai quali ricorre un paese terzo per proteggere i diritti delle persone interessate possono differire da quelli prescritti dal RGPD, letto alla luce della Carta, «tali strumenti devono (...) rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione»».

<sup>133</sup> Sentenza *Schrems II*, cit., punto 99.

<sup>134</sup> *Ivi*, punto 101.

<sup>135</sup> A tal riguardo, è stato osservato che la Corte di giustizia, con tale passaggio, ha rivendicato «il ruolo di Corte costituzionale pan europea, andando a rimarcare la necessità di un check and balance tra il potere, squisitamente politico e discrezionale della Commissione, e la sofisticata tutela dei diritti fondamentali garantita dall'Unione»: A. CRISTOFANO, *La Sentenza Schrems II e il judicial activism della Corte di Giustizia dell'Unione Europea. Verso*

gli strumenti processuali dello Stato terzo, integrati nel sistema dell'Unione tramite la decisione di adeguatezza, devono anch'essi rispettare i principi di cui all'art. 47 della Carta. Ai paesi terzi viene così imposto, implicitamente, un obbligo di disporre di mezzi di tutela giurisdizionale effettiva per poter sviluppare interessi commerciali con l'Unione tramite la circolazione dei dati personali.

Nell'ambito dei negoziati per elaborare la nuova decisione di adeguatezza, la Commissione europea e gli Stati Uniti avevano pubblicato nel marzo 2022 un comunicato stampa congiunto annunciando un'intesa di principio su un accordo quadro, noto come *Trans-Atlantic Data Privacy Framework*<sup>136</sup>. Era stata annunciata la previsione di un sistema di ricorso a due livelli per l'esame e la risoluzione dei reclami degli individui che si trovano nell'UE, con l'istituzione di una autorità, la *Data Protection Review Court* (DPRC), soggetta a un monitoraggio periodico da parte della *Privacy and Civil Liberties Oversight Board* (PCLOB), nonché di un sistema di certificazione delle aziende statunitensi ad opera del Dipartimento del Commercio USA. L'assunzione ufficiale degli impegni da parte degli USA è avvenuta con l'Ordine Esecutivo (*Enhancing Safeguards for United States Signals Intelligence Activities*) n. 14086 emesso dal Presidente Biden il 7 ottobre 2022. La priorità per la Casa Bianca sarebbe quella di trovare un accordo che bilanci la necessità statunitense di garantire la sicurezza nazionale e la priorità europea di tutelare la privacy dei propri cittadini.

La bozza di decisione di adeguatezza, elaborata alla luce del nuovo accordo UE-USA, veniva poi adottata dalla Commissione europea il 13 dicembre 2022. Sul testo ha espresso parere negativo la commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo, il cui progetto di risoluzione del 14 febbraio 2023<sup>137</sup> è stato discusso e approvato nella sessione plenaria dell'11 maggio 2023<sup>138</sup>. In sintesi, le critiche riguardano la mancanza di pubblicità delle decisioni prese dalla *Court* e, più in generale, di trasparenza, indipendenza e imparzialità di questo nuovo organo, nonché la carenza di garanzie circa l'efficacia del meccanismo di ricorso proposto. In ogni caso, la risoluzione non è vincolante per la Commissione europea, che ha il solo obbligo di consultare il Parlamento ai fini dell'adozione della decisione definitiva.

Precedentemente, il 28 febbraio 2023, il Comitato europeo per la privacy aveva adottato il suo parere<sup>139</sup>, con cui aveva accolto con favore i miglioramenti sostanziali contenuti nella bozza di decisione, tra cui la previsione del nuovo meccanismo di ricorso. Tuttavia, anch'esso

---

*un GDPR a vocazione universale?*, in *MediaLaws*, 15 febbraio 2021. Il controllo giurisdizionale consiste in realtà in un esame indiretto dell'ordinamento statunitense, effettuato in via mediata poiché avente ad oggetto la legittimità di un atto dell'Unione, che lo richiama. Operando in tal modo, la Corte assicura in concreto, nel contesto dei rapporti internazionali, la protezione effettiva dei dati personali delle persone che si trovano nell'Unione. Sul punto, v. anche R. CAFARI PANICO, *Le imprese multinazionali*, cit., p. 22 ss.; nonché sia consentito rinviare a C. PERARO, *Protezione extraterritoriale dei diritti*, cit., p. 682 ss.

<sup>136</sup> V. il comunicato stampa reperibile al sito Internet [https://ec.europa.eu/commission/presscorner/detail/it/ip\\_22\\_2087](https://ec.europa.eu/commission/presscorner/detail/it/ip_22_2087).

<sup>137</sup> Progetto di proposta di risoluzione del 14 febbraio 2023, Risoluzione del Parlamento europeo sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati (2023/2501(RSP)).

<sup>138</sup> Risoluzione del Parlamento europeo dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati (2023/2501(RSP)).

<sup>139</sup> EDPB, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*; v. anche il comunicato stampa reperibile al sito Internet [https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain\\_en](https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en).

esprimeva preoccupazione in merito a quest'ultimo, facendo rilevare che le risposte fornite dalla *Court* potrebbero limitarsi a formule standard, nel senso che potrebbe notificare ai denunciati una semplice decisione dove dichiara che non sono state individuate violazioni oppure con cui informa che è stato richiesto un rimedio adeguato senza ulteriori specificazioni, e che tale provvedimento non può tuttavia essere impugnato.

La decisione di adeguatezza del 10 luglio 2023, in merito al meccanismo di *redress*<sup>140</sup>, conferma la possibilità, accessibile anche ai cittadini dell'Unione<sup>141</sup> gratuitamente, di presentare un reclamo (*complaint*), tramite l'autorità competente dello Stato UE interessato<sup>142</sup>, al *Civil Liberties Protection Officer of the Director of National Intelligence* (ODNI CLPO), il cui provvedimento potrà poi essere impugnato davanti alla *Data Protection Review Court*<sup>143</sup>. Le decisioni di tale tribunale saranno vincolanti e definitive, quindi non appellabili<sup>144</sup>, e verranno conservate in registri<sup>145</sup>. Inoltre, chiunque «irrespective of nationality or place of residence» può promuovere azioni legali davanti ai tribunali americani<sup>146</sup>. Ad avviso della Commissione, quindi, il sistema di tutela così previsto assicura un livello di protezione che è essenzialmente equivalente a quello predisposto dal RGPD<sup>147</sup>. Solo con la prassi si potrà valutare l'effettivo funzionamento di tale meccanismo, che sarà oggetto di costante monitoraggio e di una prima *review* a distanza di un anno dall'entrata in vigore della decisione di adeguatezza<sup>148</sup>.

In concreto, con riferimento alla circolazione dei dati personali verso le imprese statunitensi che partecipano al *EU-US Data Privacy Framework*, sulla base della nuova decisione di adeguatezza, tale trasferimento è considerato sicuro, quindi senza la necessità di ulteriori garanzie per la protezione dei dati. Diversamente, le garanzie predisposte dal paese di destinazione devono essere accertate e assicurate dai partner commerciali europei che intendono avvalersi di servizi oltreoceano<sup>149</sup>, potendo altrimenti essere le stesse parti contrattuali ad incorrere in violazioni del RGPD<sup>150</sup>.

---

<sup>140</sup> V. considerando 175 ss. della decisione di adeguatezza.

<sup>141</sup> *Ivi*, considerando 176, dove viene precisato che «This redress mechanism is available to individuals from countries or regional economic integration organisations that have been designated by the U.S. Attorney General as 'qualifying states'. On 30 June 2023, the European Union and the three European Free Trade Association countries that together constitute the European Economic Area have been designated by the Attorney General under Section 3(f) EO 14086 as a 'qualifying state'».

<sup>142</sup> Cfr. considerando 177 della decisione di adeguatezza.

<sup>143</sup> *Ivi*, considerando 184 ss.

<sup>144</sup> *Ivi*, considerando 191.

<sup>145</sup> *Ivi*, considerando 192.

<sup>146</sup> *Ivi*, considerando 195 ss.

<sup>147</sup> *Ivi*, considerando 201 e art. 1.

<sup>148</sup> *Ivi*, considerando 209 e 211 e art. 3.

<sup>149</sup> In merito, sono utili i provvedimenti dello EDPB, reperibili al sito Internet [https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices\\_it](https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_it), tra cui: Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti, adottate il 14 febbraio 2023; Linee guida 4/2021 sui codici di condotta come strumento per i trasferimenti; 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.

<sup>150</sup> In questo senso, v. Garante per la protezione dei dati personali, provvedimento n. 224 del 9 giugno 2022, *Caffeina Media Srl*, col quale ha chiarito che il sito web che utilizza il servizio Google Analytics viola la normativa sulla protezione dei dati perché trasferisce i dati degli utenti negli Stati Uniti, paese privo di un adeguato livello di protezione; nonché provvedimento n. 243 del 7 luglio 2022, *IlMeteo S.r.l.*

5. Per rafforzare la “diplomazia digitale” dal 1° settembre 2022 la Commissione europea ha aperto un ufficio a San Francisco nella Silicon Valley al fine di sviluppare relazioni più strette con i Big del mondo tech<sup>151</sup>. L’intento dovrebbe essere quello di coordinare gli ordinamenti europeo e statunitense e così diffondere la cultura europea in tema di tutela della privacy<sup>152</sup>. Una cultura che appare in realtà alquanto elaborata, formata da svariati testi legislativi, settoriali e trasversali, con obblighi, doveri, sanzioni, diritti, diversi ruoli, diverse autorità competenti e mezzi di protezione. Proprio l’*enforcement*, nell’Unione, così come in territori extra-UE, nei termini sopra esposti, rimane comunque una questione non totalmente europea, spettando ai singoli Stati membri adoperarsi per prevedere gli strumenti idonei a garantire i diritti derivanti dall’ordinamento UE.

Nell’analisi della normativa europea rilevante nel contesto digitale si sono potute constatare convergenze tra le discipline in tema di privacy e antitrust, accomunate dalla finalità di assicurare il funzionamento del mercato interno, pur sempre attente alla tutela dei diritti fondamentali delle persone. Tuttavia, tali discipline presentano criticità, soprattutto in ottica pratica. In primo luogo, le numerose regole potrebbero essere oggetto di miglioramento, o semplificazione, utile soprattutto per i beneficiari dei diritti, questi ultimi conferiti in via diretta o indiretta quali contropartita degli obblighi imposti dagli atti UE alle imprese; nonché, in secondo luogo, la cooperazione tra autorità potrebbe essere regolata, in termini operativi, a livello europeo, intervenendo su meccanismi già esistenti<sup>153</sup>, che potrebbero essere oggetto di valutazione in sede di riesame dell’applicazione delle discipline in parola.

Una migliore interazione tra autorità sarebbe *a fortiori* richiesta quando nel contesto di una fattispecie si toccano diversi profili di indagine, appunto privacy e antitrust, ma ora anche mercati digitali. Come è possibile notare in altri ambiti governati dal diritto UE, mancherebbe nei settori qui esaminati una armonizzazione nell’attuazione e nell’esecuzione delle norme europee nei contesti nazionali. Si tratta però di un aspetto su cui l’Unione non ha competenza ad intervenire. In tal senso si era espresso il Comitato europeo per la privacy con una *Wish List*<sup>154</sup>, ovvero una “lista dei desideri” che fa parte delle azioni chiave definite nella dichiarazione di Vienna del Comitato sulla cooperazione in materia di applicazione del Regolamento<sup>155</sup>, dove poneva l’attenzione sul coordinamento tra aspetti di diritto processuale

---

<sup>151</sup> Conclusioni del Consiglio sulla diplomazia digitale dell’UE del 18 luglio 2022; v. anche il comunicato stampa reperibile al sito Internet <https://www.consilium.europa.eu/it/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/>.

<sup>152</sup> *Ibidem*. Per alcune considerazioni in merito alla politica digitale di UE e Stati Uniti, v. G. MUSCOLO, *Biden’s antitrust: verso una nuova alleanza transatlantica? Cenni di comparazione tra Stati Uniti e Europa*, in *Politica di Concorrenza e Politica Industriale, Sinergia o Conflitto?*, in *Eurojus*, numero speciale, aprile 2023, pp. 108-128.

<sup>153</sup> Si fa riferimento al *Consumer Protection Cooperation Network*, istituito con Regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio, del 27 ottobre 2004, sulla cooperazione tra le autorità nazionali responsabili dell’esecuzione della normativa che tutela i consumatori, poi abrogato con Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, in *GUUE*, L 345 del 27 dicembre 2017, pp. 1-26; e al *European Competition Network*, istituito con Regolamento (CE) n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l’applicazione delle regole di concorrenza (su cui v. A.M. ROMITO, *Ruolo e funzioni dell’European Competition Network : dal regolamento (CE) n. 1/2003 alla direttiva ECN*, Bari, 2020).

<sup>154</sup> Si veda il comunicato stampa del 12 ottobre 2022, reperibile al sito [https://edpb.europa.eu/news/news/2022/edpb-adopts-wish-list-procedural-aspects-first-eu-data-protection-seal-and-statement\\_it](https://edpb.europa.eu/news/news/2022/edpb-adopts-wish-list-procedural-aspects-first-eu-data-protection-seal-and-statement_it).

<sup>155</sup> EDPB, *Statement on enforcement cooperation*, adottato il 28 aprile 2022, reperibile al sito Internet [https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-enforcement-cooperation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-enforcement-cooperation_en).

nazionale che potrebbero essere armonizzati a livello europeo per facilitare l'applicazione del RGPD. Tra gli ostacoli che il Comitato ha individuato, è stato fatto riferimento allo status e ai diritti delle parti nelle procedure amministrative, ai termini procedurali, ai requisiti per l'ammissibilità o il rigetto dei reclami, ai poteri investigativi delle autorità di protezione dei dati e all'attuazione pratica della procedura di cooperazione. In merito all'ultimo profilo, sono state suggerite dalla Commissione europea, con una proposta di regolamento pubblicata il 4 luglio 2023, alcune regole operative da applicare per l'attuazione dei meccanismi di cooperazione e coerenza<sup>156</sup>, basata, come quest'ultimo, sull'art. 16 TFUE<sup>157</sup>. Prevedendo garanzie a tutela dei diritti procedurali di difesa, oltre a termini e obblighi di informazione in capo alle autorità, nonché norme minime sul contenuto dei reclami, le nuove disposizioni per la trattazione concreta di casi transfrontalieri potrebbero rappresentare un primo passo verso una uniforme e migliore esecuzione del regolamento, sollecitando rapidità e trasparenza, per assicurare così il perseguimento concreto dei suoi obiettivi di protezione.

A quanto sopra osservato, si potrebbe aggiungere l'opportunità di una revisione dei poteri delle autorità, sempre al fine di allineare gli strumenti nazionali di *enforcement*, che potrebbero essere uniformati per superare le disparità dovute all'applicazione di regole interne differenti, per garantire così una protezione il più simile possibile in tutti i paesi UE<sup>158</sup>. Allo stesso scopo, dovrebbe essere valutata l'utilità di prevedere tra i poteri degli enti rappresentativi a tutela degli interessi collettivi, come osservato in ambito privacy, la loro legittimazione ad agire in assenza di danni effettivi e in mancanza di vittime identificate o identificabili.

In conclusione, ciò cui si assiste è una interconnessione tra esigenze di garantire il buon funzionamento del mercato interno, nelle sue varie dimensioni, compresa quella digitale, e i diritti degli interessati, in quanto consumatori e titolari dei dati, ma soprattutto il loro diritto alla protezione dei propri dati in ogni operazione che li riguardi. Ecco allora che la funzione della tutela pubblicistica sembrerebbe la via da seguire per assicurare un corretto bilanciamento delle suddette esigenze. Anche perché le azioni individuali o collettive rimangono in ogni caso "a carico" dei soggetti contrattualmente più vulnerabili, i titolari dei dati.

---

<sup>156</sup> Il riferimento è agli art. 60 ss. RGPD.

<sup>157</sup> Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679 (COM(2023)348 final del 4 luglio 2023).

<sup>158</sup> In questo senso, ma in un diverso ambito materiale, la Corte di giustizia, nella sentenza del 29 settembre 2022, causa C-597/20, *LOT (Indemnisation imposée par l'autorité administrative)*, EU:C:2022:735, ha confermato la possibilità per gli Stati membri di autorizzare l'organismo nazionale responsabile dell'applicazione del Regolamento (CE) n. 261/2004 in tema di tutela dei passeggeri aerei, a imporre a un vettore aereo la corresponsione della compensazione pecuniaria, ai sensi dell'art. 7 di detto regolamento, qualora tale organismo nazionale sia stato investito di un reclamo individuale di un passeggero, purché sussista per tale passeggero e per detto vettore aereo la possibilità di un ricorso giurisdizionale (punto 41). Infatti, una simile competenza consente, per le ragioni di semplicità, rapidità ed efficacia, di garantire un elevato livello di tutela dei passeggeri aerei, evitando al contempo la congestione dei tribunali tenuto conto del numero potenzialmente elevato di richieste di compensazione pecuniaria (punto 40). Nello stesso senso, la Corte di giustizia, con sentenza del 30 marzo 2023, *Green Network (Ordine di restituzione di somme addebitate)*, cit., ha stabilito che, alla luce della direttiva 2009/72/CE, uno Stato membro può prevedere nel proprio ordinamento che all'autorità di regolazione nazionale sia conferito il potere di ordinare alle società elettriche di restituire somme corrispondenti ai costi di gestione amministrativa riscosse «in applicazione di una clausola contrattuale considerata illegittima da tale autorità» (punto 25 ss.), «anche nel caso in cui l'ordine di restituzione in questione non sia fondato su ragioni attinenti alla qualità del servizio di cui trattasi fornito da dette società, bensì sulla violazione di obblighi di trasparenza tariffaria» (punto 27 ss.).

Alla luce delle svariate cause che riguardano la Meta Platforms, non solo nell'Unione europea ma anche negli Stati Uniti, accompagnate da ingenti sanzioni pecuniarie e dall'imposizione di misure correttive e riparative, non sarebbe così assurdo domandarsi cosa potrebbe accadere qualora il social network americano decidesse di interrompere i servizi, come Facebook, WhatsApp o Instagram. La risposta, forse, riguarderebbe solo le potenziali conseguenze sul mercato per le attività commerciali che da quei servizi ricavano quantità di *big data*, ormai essenziali per gestire le strategie aziendali. Viviamo quindi in un mercato digitale europeo governato in realtà da piattaforme e da Big Tech principalmente americane, con cui si devono confrontare non solo i sistemi normativi, il legislatore europeo, le autorità, le imprese, le persone, ma anche, in seconda battuta, i giudici, nonché la Corte di giustizia, quale garante europeo dei diritti fondamentali.