Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

OSSERVATORIO NUOVE TECNOLOGIE E DIRITTI FONDAMENTALI N. 1/2025

4. IL NUOVO LIVELLO DI PROTEZIONE DEI DATI PERSONALI TRAMITE LA DISCIPLINA DELLA CONCORRENZA SLEALE ALLA LUCE DELLA SENTENZA NELLA CAUSA C-21/23

1. *Introduzione*

La Corte di Giustizia, riunita in Grande Sezione, ha preso posizione su un tema da tempo dibattuto, concernente una "zona di tensione" che coinvolge il Regolamento (UE) 2016/679 (GDPR) sin dallo sviluppo dell'economia digitale.

Con le sentenze C-319/20 (causa C-319/20, del 28 aprile 2022, *Meta Platforms Ireland* EU:C:2022:322) e C-252/21 (causa C-252/21, del 4 luglio 2023, *Meta Platforms Ireland,* ECLI:EU:C:2023:537*)*, la Corte aveva consolidato l'orientamento secondo il quale la violazione di una norma relativa alla protezione dei dati personali possa simultaneamente comportare una violazione del diritto della concorrenza nonché una pratica commerciale sleale.

Con la pronuncia in esame (causa C-21/23, 4 ottobre 2024, *ND/DR*, ECLI:EU:C:2024:846), la Corte si è espressa sulla questione logicamente conseguente, affermando la possibilità che una violazione delle disposizioni del GDPR possa giustificare la proposizione, anche da parte di un concorrente, di un'azione inibitoria ai sensi della legge (tedesca) sulla concorrenza sleale, in assenza di una specifica previsione nel testo del Regolamento.

La pronuncia si inserisce, infatti, in un contesto normativo e giurisprudenziale sempre più orientato verso un approccio integrato (ed olistico) tra protezione dei dati personali e diritto della concorrenza. Tale evoluzione riflette la crescente consapevolezza del valore economico dei dati personali, che assumono una duplice natura. Da un lato, essi costituiscono informazioni personali e diritti fondamentali tutelati dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea e dal GDPR; dall'altro lato, rappresentano un *asset* competitivo di rilevante valore economico per le imprese digitali, utilizzato per finalità di profilazione, *marketing* comportamentale (L. PIGNA, *Schrems c. Meta. La Corte di Giustizia si pronuncia sui limiti al trattamento dei dati personali per fini di pubblicità mirata*, in Ordine Internazionale e Diritti Umani, 2024, pp. 1033-1039) e personalizzazione dei servizi.

In questo contesto, si rendeva necessaria l'introduzione di uno strumento di *enforcement* privato attivabile dai concorrenti, attribuendo al GDPR una funzione regolatrice della dialettica commerciale tra gli operatori economici. Tale impostazione, non solo permette il

mantenimento di una concorrenza equa e trasparente, bensì, rafforza contestualmente il livello di protezione dei diritti fondamentali nei mercati digitali europei.

Inoltre, nell'epoca della crescente condivisione dei dati personali a carattere sanitario, la Corte di Giustizia è stata chiamata a valutare se i dati relativi agli acquisti e agli ordini online di medicinali senza prescrizione medica possano essere considerati dati sanitari e, dunque, soggetti alla disciplina protettiva di cui all'articolo 9, paragrafo 2, del GDPR.

2. *Il contesto fattuale*

La domanda di pronuncia pregiudiziale nasce da una controversia intercorsa tra due persone fisiche ND e DR, titolari ciascuna di una farmacia, avente ad oggetto la commercializzazione *online* di medicinali non soggetti a prescrizione medica. La farmacia ND, operante con il nome commerciale "Lindenapotheke" ha posto in vendita a partire dal 2017, medicinali sulla piattaforma "*Amazon Marketplace*". In tale contesto, al momento dell'ordine dei farmaci *online*, veniva richiesto ai clienti di fornire dati personali quali il nome, l'indirizzo di consegna, nonché gli elementi necessari all'individuazione dei medicinali ordinati. Il concorrente, ND, ha adito il Tribunale del Land Dessau-Roßlau (Germania), chiedendo che fosse inibita alla "Lindenapotheke", a pena di ammenda, la commercializzazione sulla piattaforma *Amazon* dei medicinali fino a quando non fosse garantita la prestazione del consenso da parte dei clienti. In particolare, i dati personali inseriti al fine dell'inoltro dell'ordine venivano qualificati, dalla ricorrente, come dati relativi alla salute: da ciò discende la conseguenza che il loro trattamento è soggetto al consenso di cui all'art. 9, paragrafo 2, del Regolamento (UE) 679/2018, (GDPR).

Richiedendo tale azione inibitoria, il concorrente sostiene che la commercializzazione dei medicinali, specie di quelli la cui vendita era riservata alle farmacie, violasse la normativa sulla protezione dei dati personali (per l'omessa acquisizione di un consenso esplicito ai sensi del comma 2 dell'articolo 9 GDPR), costituendo simultaneamente atto di concorrenza sleale, vietato dall'articolo 3, paragrafo 1, della *Gesetz gegen den unlauteren Wettbewerb* (*Gesetz gegen den unlauteren Wettbewerb* UWG, legge contro la concorrenza sleale, del 3 luglio 2004, BGBl. 2004 I, pag. 1414). La legge tedesca contro la concorrenza sleale, ai sensi dell'articolo 3, vieta le pratiche commerciali sleali e, ai sensi dell'articolo 3a dell'UWG, dispone che commette pratica commerciale sleale «colui il quale violi una disposizione di legge che sia altresì destinata a disciplinare il comportamento sul mercato nell'interesse dei soggetti partecipanti al mercato stesso, nel caso in cui la violazione sia idonea a pregiudicare in maniera sensibile gli interessi dei consumatori, di altri soggetti partecipanti al mercato o dei concorrenti».

Siffatta violazione, consente a qualsiasi concorrente, in base all'articolo 8, paragrafo 3, punto 1, UWG, di agire davanti ai giudici civili per ottenere un provvedimento inibitorio.

La legittimazione ad agire da parte di un concorrente, tramite la legge sulla concorrenza sleale per la violazione del Regolamento GDPR e, la qualificazione dei dati summenzionati come dati relativi alla salute, non trovavano un chiaro fondamento normativo né risultavano corroborate da precedenti della Corte di Giustizia.

Il giudice di prima istanza, con sentenza del 28 marzo del 2018, accoglie il ricorso. Avverso tale pronuncia è stato proposto appello dinnanzi al Tribunale superiore del Land, Naumburg che, con decisione del 7 novembre 2019, ha respinto il gravame.

La soccombente ha quindi proposto ricorso per cassazione "*Revision*" dinanzi alla Corte federale di giustizia, la quale, ponendo il dubbio che le disposizioni del GDPR ammettano la

legittimazione di un concorrente, ha investito la Corte di Giustizia dell'Unione europea di una domanda di pronuncia pregiudiziale (BGH ZD 2023, 273).

3. *Il contesto normativo della prima domanda pregiudiziale: la lacuna nei mezzi di tutela previsti dal GDPR rispetto all'azione inibitoria da parte dei concorrenti*

Dinnanzi al Giudice del rinvio, si appalesava la necessità di stabilire se le disposizioni del capo VIII del GDPR, ostino a una normativa nazionale che conferisce ai concorrenti del presunto autore di una violazione della protezione dei dati personali la legittimazione ad agire contro quest'ultimo, mediante ricorso dinanzi ai giudici civili, per violazione di detto regolamento e sul fondamento del divieto delle pratiche commerciali sleali di cui all'articolo 8, paragrafi 3 e 3a, dell'UWG.

Effettivamente, alla luce del tenore letterale degli articoli da 77 a 79 del GDPR, la legittimazione a proporre reclami dinanzi all'autorità di protezione dei dati e ad avviare azioni giudiziarie contro i responsabili o i titolari del trattamento è attribuita, in via esclusiva, ai soggetti qualificabili come interessati dei dati ai sensi dell'articolo 4, par. 1, del GDPR, ossia alle persone fisiche o giuridiche cui tali dati si riferiscono.

Dalla lettera di tali disposizioni, pertanto, emerge un vuoto di tutela per i concorrenti, i quali non risultano legittimati dal GDPR a promuovere azioni inibitorie in sede civile per far valere eventuali violazioni del Regolamento. Nel caso di specie, gli interessati dei dati, i quali hanno la legittimazione ai sensi dell'articolo 79 del GDPR, sarebbero esclusivamente i clienti che inseriscono i propri dati personali sulla piattaforma.

Ciò su cui ci deve interrogare, in particolare, è relativo al se, dato l'impianto generale del Capo VIII del regolamento 2016/679, vi sia una armonizzazione completa ed esaustiva dei mezzi di ricorso, volta ad escludere ogni tentativo ampliamento dei mezzi di tutela, oppure se, viceversa, in virtù della clausola «fatto salvo ogni altro ricorso» menzionata negli articoli da 77 a 79, possa essere colmata tale "lacuna" riconoscendo la legittimazione attiva ai concorrenti per un'azione dinanzi all'autorità giurisdizionale civile (cfr. parr. 34 e 36).

Una volta risposto a tale quesito, si può poi riflettere sulla possibilità che tale legittimazione sia in contrasto con gli obiettivi di armonizzazione e di uniformazione dell'applicazione del GDPR. Difatti una "concorrenza" nell'applicazione del diritto in materia di protezione dei dati tra le autorità di controllo e i giudici civili, rischierebbe di invadere i poteri e le competenze delle stesse autorità di protezione dei dati, nonché di generare decisioni divergenti sulle medesime questioni all'interno dell'Unione europea (par. 37).

Tuttavia, la legittimazione dei concorrenti ad agire ai sensi del diritto della protezione dei dati personali non è esclusa dal tenore letterale delle norme. Al contrario, essa costituisce un'ulteriore modalità di controllo da parte degli interessati dei dati rispetto ai loro dati personali, ipotesi auspicabile in virtù del principio di efficacia (il cd. "*effetto utile*"), contribuendo a garantire il massimo livello di tutela possibile in materia di dati personali e a coadiuvare il raggiungimento degli obiettivi del GDPR.

Inoltre, tale attribuzione si spiegherebbe alla luce delle nuove dinamiche dell'economia digitale. I dati personali hanno assunto una duplice natura. Essi sono, infatti, divenuti un vero e proprio *asset* per le attività d'impresa, conferendo un vantaggio competitivo a coloro che ne dispongono (M. MAGGIOLINO, *I Big Data e il diritto antitrust*, Milano, 2018), oltre che diritti fondamentali garantiti dagli articoli 7 ed 8 della Carta dei diritti fondamentali.

È interessante, sotto questa prospettiva, valutare come il GDPR e le disposizioni concernenti il trattamento dei dati personali, riescano ad assumere, simultaneamente, una dimensione aggiuntiva rispetto a quella di strumento tutela dei diritti fondamentali.

Una violazione del GDPR, pertanto, oltre che determinare un indebito trattamento dei dati personali degli interessati dati (ai sensi dell'articolo 4 GDPR), può comportare ripercussioni negative sul corretto funzionamento delle dinamiche concorrenziali; tramite tale violazione, i concorrenti ottengono slealmente tale risorsa, collocandosi in una posizione di vantaggio competitivo rispetto alle imprese che, invero, osservano le prescrizioni di tale Regolamento.

È interessante notare come questa impostazione giuridica rappresenta un approccio innovativo nel panorama europeo, che rafforza la tutela dei dati personali mediante l'interconnessione tra normativa sulla protezione dei dati e diritto della concorrenza, esplicando i suoi effetti su un duplice versante (OECD, *The Intersection between Competition and Data Privacy*, in *OECD Roundtables on Competition Policy Papers*, No. 310, Paris, 2024).

Dal punto di vista del diritto della concorrenza, le cui questioni sono valutate in maniera strumentale nell'ambito di questa complessa questione, la soluzione del quesito comporta l'attribuzione della legittimazione ad agire in giudizio da parte delle imprese rivali, invocando la violazione del GDPR come pratica commerciale sleale, quando il concorrente ottenga (indebitamente) un vantaggio competitivo grazie a tale violazione. In tal modo, le disposizioni sulla protezione dei dati personali diventano regole di condotta vincolanti per tutte le imprese operanti sul mercato, configurandosi come *standard* di lealtà concorrenziale, garantendo un *level playing field*, per tutti gli operatori economici.

Difatti, l'eventualità che i concorrenti possano agire *ex lege* sulla base della disciplina contro la concorrenza sleale per la cessazione della violazione delle disposizioni del GDPR, permetterebbe di qualificare la violazione del GDPR quale regola destinata a disciplinare il comportamento delle imprese sul mercato. Sul punto, difatti, l'art. 3a della legge sulla concorrenza sleale tedesca, sancisce che «Commette un atto sleale colui il quale violi una disposizione di legge che sia altresì destinata a disciplinare il comportamento sul mercato nell'interesse dei soggetti partecipanti al mercato stesso».

Oltre ad avere implicazioni in materia di concorrenza, tale impostazione è funzionale ad introdurre ulteriori meccanismi di tutela per la protezione dei dati personali e della *privacy*.

La disciplina del GDPR, tradizionalmente circoscritta alla protezione delle informazioni personali, qualora assurga a criterio di correttezza sul piano dei rapporti concorrenziali, pone un ulteriore responsabilità comportamentale a carico degli operatori economici.

In questo ambito, l'attribuzione della legittimazione ad agire anche ai concorrenti, svolge una significativa funzione deterrente. Le imprese saranno dissuase dall'intraprendere condotte che concretizzino violazioni del GDPR, in quanto le stesse sarebbero consapevoli del rischio di attivazione non soltanto delle procedure previste dal Regolamento (Articolo 79 per azioni individuali da parte degli interessati dei dati, Articolo 80 per azioni rappresentative del GDPR), ma anche di ulteriori azioni, di natura privatistica, da parte dei concorrenti. Tale duplice possibilità di tutela comporta un rafforzamento della "pressione conformativa" nei confronti dei titolari del trattamento (gli operatori economici), fungendo così da efficace meccanismo dissuasivo.

Ulteriormente, l'introduzione di un meccanismo di tutela attivabile dai concorrenti, rappresenta un'innovazione rilevante che, ampliando i soggetti legittimati ad agire, consente a questi lo svolgimento di un'attività di monitoraggio della conformità al GDPR, superando

altresì i limiti che circondano la proposizione di azioni individuali degli interessati dei dati, in caso di violazione dei dati personali da parte di un operatore economico.

È cosa nota, difatti, che i concorrenti dispongono di mezzi più efficaci ed incisivi per individuare eventuali violazioni del GDPR da parte di altri soggetti, avendo accesso a maggiori informazioni e conoscenze tecniche, nonché essendo guidati da un rilevante interesse economico. Tali violazioni, infatti, potrebbero non essere note al singolo utente o potrebbero risultare di difficile individuazione per quest'ultimo. A differenza del singolo interessato, inoltre, il concorrente è generalmente dotato di maggiori risorse finanziarie e possiede le conoscenze tecniche necessarie per intraprendere azioni legali, contribuendo così a superare le difficoltà connesse agli elevati costi di giudizio e alla complessità delle azioni collettive in materia di protezione dei dati personali (cfr. Direttiva (UE) 2020/1828 del Parlamento Europeo e del Consiglio, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, 25 novembre 2020, in *GUUE*, L 409/1, 2020).

Pertanto, la risoluzione della questione posta a fondamento del rinvio pregiudiziale riveste un notevole interesse dal punto di vista sistematico, poiché l'assenza di una tutela adeguata influisce negativamente sia sulla correttezza delle dinamiche concorrenziali, sia sulla protezione dei dati personali degli interessati, privandoli di un ulteriore meccanismo (indiretto) di tutela, volto a salvaguardare la sfera privatissima delle proprie informazioni personali.

4. *La seconda domanda pregiudiziale, l'articolo 9 del GDPR ed il consenso al trattamento dei dati relativi alla salute.*

In secondo luogo, il giudice del rinvio pone una questione strettamente attinente alla protezione dei dati personali, la quale assume particolare rilievo nelle nuove dinamiche del commercio *online*, volta ad accordare un'estensione della tutela accordata ai dati personali.

Ci si chiede se l'articolo 8, par. 1, della direttiva 95/46 e l'articolo 9, par. 1, del GDPR debbano essere interpretati nel senso che, nel caso in cui il gestore di una farmacia commercializzi, tramite una piattaforma *online*, medicinali la cui vendita è riservata alle farmacie, le informazioni che i clienti inseriscono al momento dell'ordine, quali il loro nome, l'indirizzo di consegna e le informazioni necessarie all'individualizzazione dei medicinali, costituiscono dati relativi alla salute, ai sensi di tali disposizioni, anche qualora la vendita di tali medicinali non sia soggetta a prescrizione medica.

Difatti, nell'ipotesi di acquisto di medicinali non soggetti a prescrizione medica, la qualificazione dei dati inseriti dagli utenti al momento dell'ordine quali dati relativi alla salute non appare, viceversa, di immediata evidenza. Ciò in quanto tali prodotti potrebbero anche essere destinati a terzi non identificabili, anziché al medesimo cliente che procede all'ordine. Tale incertezza risulta comprensibile alla luce della definizione contenuta nell'articolo 4, punto 15, del GDPR, secondo cui per «dati relativi alla salute» si intendono quelli che «rivelano informazioni relative al suo stato di salute» di un individuo. In senso conforme, il considerando 35 fa riferimento ai dati personali relativi alla salute come a quelli «lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso».

L'articolo 9, par. 1, del GDPR impone il divieto del trattamento di categorie particolari di dati personali, tra i quali rientra la categoria suddetta. Difatti, a mente del considerando 51 di tale regolamento, tali dati meritano una specifica protezione in quanto, il contesto del loro

trattamento potrebbe creare rischi significativi sotto il profilo dei diritti e delle libertà fondamentali. La medesima disposizione, tuttavia, al secondo par., lettera *a*), stabilisce una deroga a tale divieto qualora l'interessato abbia dato il proprio consenso esplicito al trattamento. Consenso che, tuttavia, non risultava essere stato prestato.

La qualificazione dei dati suddetti, come dati rientranti in tale categoria, varrebbe ad estendere, per via interpretativa, il novero dei dati personali ritenuti sensibili prevista dal GDPR. A questo proposito, giova richiamare la pronuncia della Corte di Giustizia in *Vyriausioji tarnybinės etikos komisija* (Corte di Giustizia, C-184/20, del 10 agosto 2022, EU:C:2022:601), nella quale il Giudice europeo ha optato per una interpretazione estensiva della nozione di «categorie particolari di dati personali», di cui all'articolo 9, par. 1, del Regolamento, la quale appare giustificata sulla base dell'obiettivo di tale normativa, che è quello di garantire un elevato livello di tutela delle libertà e dei diritti fondamentali delle persone fisiche, in particolare della loro vita privata, in relazione al trattamento dei dati personali che le riguardano.

Qualora la Corte aderisse a un'interpretazione ampia di tale categoria, concludendo che le informazioni fornite dagli acquirenti dei medicinali, ancorché non sia certo, ma soltanto probabile, che essi siano effettivamente i destinatari finali dei prodotti, siano da annoverare tra i dati relativi alla salute, si determinerebbe un ampliamento del novero dei dati personali qualificabili in tal senso, introducendo un vincolo al loro trattamento, quale la necessità della prestazione del consenso.

5. *L'inquadramento della vicenda alla luce dell'orientamento della CGUE*

5.1. *CGUE, causa C-319/20, Meta Platforms*

Per comprendere la portata della questione in relazione all'approccio olistico tra diritto della concorrenza e protezione dei dati personali è utile inquadrare la questione alla luce di due precedenti storici, che hanno segnato una svolta in materia.

La prima questione pregiudiziale, si pone, in definitiva, nel solco tracciato dalla sentenza pregiudiziale emessa dalla Corte nella vicenda *Meta Platforms* C-319/20. Difatti, nel rinvio pregiudiziale, alla Corte era stato richiesto di pronunciarsi sul tema della legittimazione di una associazione di tutela dei consumatori in assenza di mandato ad agire degli interessati dei dati, a proporre un'azione inibitoria contro le pratiche commerciali sleali (articolo 3a della legge tedesca contro la concorrenza sleale), fondata sulla presunta violazione delle norme del GDPR. La Corte viene, pertanto, sollecitata a pronunciarsi in merito alla qualificazione della violazione del GDPR quale atto di concorrenza sleale, in un contesto privo di un orientamento giurisprudenziale consolidato.

Entrambe le questioni, come si vedrà, offrono spunti per la risoluzione della controversia in esame.

In primo luogo, si nota come la prima domanda pregiudiziale affrontata dalla sentenza C-23/21, si rendeva indispensabile poiché la Corte, nella sentenza C-319/20, aveva espressamente lasciato aperta la questione della legittimazione ad agire in un concorrente. Il Giudice del rinvio aveva infatti domandato alla Corte di Lussemburgo se le disposizioni del capo VIII del GDPR, e in particolare l'articolo 80, parr. 1 e 2 conferissero, non solo «ad associazioni, organismi ed organi camerali legittimati in base alla normativa nazionale il potere di agire, in caso di violazioni [dell'RGPD], contro l'autore della violazione, indipendentemente dalla lesione di diritti specifici di singoli interessati e in assenza di un

mandato dell'interessato, proponendo un ricorso dinanzi ai giudici civili fondato sul divieto di pratiche commerciali sleali (…)», ma anche la possibilità di estendere tale legittimazione anche "ai concorrenti" (causa C-319/20, punto 47).

Tuttavia, in quell'occasione, la Corte di Giustizia non si pronunciò espressamente sul punto, posto che la ricorrente era un'associazione di tutela dei diritti dei consumatori. In questo contesto, la Corte non ritenne necessario affrontare la questione relativa alla legittimazione dei concorrenti rilevante per la risoluzione della controversia dinnanzi al giudice *a quo* (causa C-319/20, punto 50).

Ciononostante, il ragionamento della Corte risulta rilevante per fondare la legittimazione delle associazioni di tutela degli interessi dei consumatori a proporre un'azione inibitoria.

La Corte afferma che l'articolo 80, rubricato «Rappresentanza degli interessati», al paragrafo 2, contenga una cd. "*clausola di apertura*", che consente agli Stati membri di emanare una normativa che preveda che le associazioni attive nel settore della protezione dei dati personali, possano, «indipendentemente dal mandato conferito dall'interessato», proporre le azioni previste ai sensi degli articoli 77, 78 e 79 del GDPR (causa C-319/20, punto 59).

La Corte di Giustizia sostiene che tale "*clausola di apertura*" non determini una armonizzazione completa sui mezzi di ricorso presenti, lasciando un margine di discrezionalità circa il modo in cui tali disposizioni possono essere attuate (causa C-319/20, punto 57).

Tuttavia, era necessario verificare se l'articolo 80, par. 2, del regolamento 2016/679 osti all'esercizio di un'azione rappresentativa indipendentemente da una violazione concreta di un diritto di un interessato e da un mandato conferito da quest'ultimo, nel caso in cui la violazione delle norme in materia di protezione dei dati sia stata fatta valere nell'ambito di un'azione intesa a controllare l'applicazione di altre norme giuridiche volte a garantire la tutela dei consumatori (causa C-391/20, cit., punto 77). Per attribuire la legittimazione ad associazioni di tutela dei consumatori e non degli interessi dei degli interessati dati personali, era necessario che la Corte si esprimesse sul raccordo tra la disciplina in materia di pratiche commerciali sleali e la disciplina dei dati personali, stabilendo che «la violazione delle norme aventi per scopo la tutela dei consumatori o la lotta contro le pratiche commerciali sleali può essere correlata, come nel caso di specie, alla violazione delle norme in materia di protezione dei dati personali di tali consumatori». Sostiene, difatti, la Corte che «la violazione di una norma relativa alla protezione dei dati personali può simultaneamente comportare la violazione di norme relative alla tutela dei consumatori o alle pratiche commerciali sleali» (causa C-391/20, punti 66 e 78).

Pertanto, l'articolo 80, par. 2, del regolamento non osta a che gli Stati membri esercitino la facoltà che essa offre loro nel senso che le associazioni di categoria (degli interessi dei consumatori) siano legittimate ad agire contro violazioni dei diritti previsti dal GDPR per il tramite, di norme aventi per finalità la tutela dei consumatori o la lotta contro le pratiche commerciali sleali, quali quelle previste dalla direttiva (UE) 2020/1828 (causa C-319/20, punto 79).

Inoltre, rispetto all'assenza del mandato la Corte ritiene che non sia necessaria «l'identificazione individuale della persona specificamente interessata da un trattamento di dati asseritamente contrario alle disposizioni dell'RGPD» (punto 68), né «*l'esistenza di una violazione concreta dei diritti di cui una persona beneficia sulla base delle norme in materia di protezione dei dati*» (causa C-391/20, punto 70).

Anzi, i Giudici sostengono che una siffatta interpretazione è «*conforme agli obblighi derivanti dall'articolo 16 TFUE e dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea*». Con tale pronuncia, pertanto, la Corte rende manifesto l'obiettivo di assicurare una tutela multilivello dei dati personali, assicurando un'efficace protezione dei diritti e delle libertà fondamentali delle persone fisiche, quali garantiti dall'articolo 16 del TFUE.

Al di là dei principi specifici enucleati da tale sentenza, la Corte di Giustizia ha affermato che la violazione di una norma del GDPR può simultaneamente costituire una violazione di norme relative alle «pratiche commerciali sleali» (causa C-391/20, punto 78), sancendo il collegamento tra le due discipline.

Appare così evidente la necessaria statuizione circa la legittimazione ad agire da parte dei concorrenti, direttamente lesi dalle pratiche commerciali sleali, in presenza di un vuoto normativo; se questi sono lesi da una tale pratica posta in essere da un'impresa nel mercato interno, il passo successivo, in termini logico-giuridici, richiede l'attribuzione dell'azione necessaria per la tutela dei loro diritti.

5.2 *CGUE, causa C-252/21, Meta Platforms*

La sentenza pregiudiziale in esame si colloca altresì in linea di contiguità con la sentenza della Corte *Meta Platforms* C-252/21 (P. MANZINI, *Antitrust e privacy: la strana coppia*, in Quaderni AISDUE, 2023, pp. 196-220). In tale sentenza, la Corte di Giustizia ha innanzitutto riconosciuto la competenza delle autorità *antitrust* che, in quanto tali, non rivestono il ruolo di autorità preposte alla protezione dei dati personali, a valutare se un'impresa in posizione dominante abbia posto in essere una violazione delle disposizioni del GDPR. In tal modo, la Corte ha altresì stabilito la rilevanza che tale violazione assume nel diritto antitrust, affermando che questa costituisce un'ipotesi di abuso di posizione dominante ai sensi dell'articolo 102 del TFUE.

In prima battuta, la Corte, ha stabilito che la competenza delle autorità di concorrenza non prevede espressamente la competenza ad esaminare la conformità di una condotta posta in essere da una impresa in posizione dominante, rispetto alle norme del GDPR (causa C-252/21, punto 49). Ciò in quanto, secondo la Corte, l'eventuale difformità di tale condotta alle disposizioni del GDPR può costituire «un importante indizio (…) per stabilire se (…) costituisca un ricorso a mezzi su cui s'impernia la concorrenza normale nonché per valutare le conseguenze di una determinata pratica sul mercato o per i consumatori» (causa C-252/21, punto 47).

A parere sia della Corte e sia della Commissione europea, tale collegamento, di ordine procedurale e sostanziale tra i due settori del diritto, risulta necessario poiché nei mercati digitali, «l'accesso ai dati personali e la possibilità di trattamento di tali dati sono diventati un parametro significativo della concorrenza fra imprese». Pertanto, una esclusione della valutazione delle norme in materia di protezione dei dati personali, anche nel contesto giuridico delle norme di concorrenza, come quella ai sensi dell'articolo 102 TFUE, «*ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione*» (causa C-252/21, punto 51; sul punto v. W. KERBER & K. K. ZOLNA, *The German Facebook case: the law and economics of the relationship between competition and data protection law*, in *European Journal of Law and Economics*, 2020, pp. 217-250). I principi enucleati in tale pronuncia risultano di particolare interesse per la prima questione pregiudiziale all'esame.

Al riguardo, la Corte afferma che la violazione delle disposizioni del GDPR sia in grado di incidere non soltanto sugli interessati dei dati quali beneficiano della tutela diretta prevista

dal Regolamento, ma anche sul mercato e, di conseguenza, sui concorrenti e sui consumatori, sottolineando l'efficacia trasversale delle disposizioni (causa C-252/21, punto 47). Questo è in linea rispetto a quanto già emerso nella causa C-391/20 in tema di concorrenza sleale (Conclusioni dell'avvocato generale Richard de la Tour nella causa *Meta Platforms Ireland* C-319/20, EU:C:2021:979).

In secondo luogo, sotto questa prospettiva, il GDPR viene implicitamente qualificato come una regola di condotta rilevante anche nel contesto del diritto *antitrust* europeo, ampliando i confini delle conseguenze giuridiche della sua violazione (causa C-252/21, cit., punto 48).

L'attribuzione di competenze alle autorità di concorrenza implica, pertanto, la possibilità per i concorrenti di un'impresa di proporre reclamo dinanzi a tali autorità al fine di far valere un abuso di posizione dominante ai sensi del 102 TFUE fondato sulla violazione del GDPR

Pertanto, la risposta della Corte in esame non potrebbe discostarsi da tali statuizioni, limitando la possibilità di tener conto in via incidentale della violazione delle disposizioni del RGPD esclusivamente nei procedimenti *antitrust* e non nei giudizi avverso pratiche di concorrenza sleale.

Resta tuttavia aperta la questione che la successiva giurisprudenza potrà eventualmente chiarire, dell'esercizio di un'azione di *private enforcement* da parte dei concorrenti in sede civile per violazioni dell'articolo 102 TFUE, sulla base di violazioni delle normative del GDPR, similmente a quanto è stato proposto con la prima domanda pregiudiziale in esame. Anche questo strumento, infatti, andrebbe a completare la tutela dei dati personali, stante la duplice natura di questo *asset* nel contesto dei mercati digitali, introducendo uno strumento processuale per tutelare i diritti fondamentali degli utenti in maniera più vigorosa.

Ulteriormente, la Corte di Giustizia ha espresso valutazioni rilevanti per la seconda questione pregiudiziale qui in esame, soffermandosi sulla natura dei dati generati dagli utenti in fase di consultazione di siti *internet* o in occasione dell'inserimento di informazioni personali, quali ad esempio, in sede di registrazione o di piazzamento di ordini *online*.

La Corte ha ritenuto che simili informazioni possano rientrare nella categoria dei «dati personali sensibili», ivi compresi quelli «*relativi alla salute*» ai sensi degli articoli 9, paragrafo 1, e 4, punto 15, del GDPR. E ciò anche «a prescindere dal fatto che tali informazioni riguardino un utente di tale social network o qualsiasi altra persona fisica», poiché in grado di «rivelare informazioni rientranti in una delle categorie menzionate da tale disposizione» (sentenza della Corte, causa C-252/21, cit., punto 68). In tal caso, permane il divieto di trattamento dei dati medesimi, a meno che non intervenga il consenso esplicito *ex* articolo 9, paragrafo 2, GDPR.

La Corte precisa, inoltre, che detto divieto opera indipendentemente «dalla questione se l'informazione rivelata dal trattamento di cui trattasi sia esatta o meno e se il titolare del trattamento agisca allo scopo di ottenere informazioni rientranti in una delle categorie particolari previste da tale disposizione» (punto 69). L'attenzione per i rischi potenziali connessi al trattamento di tali dati personali, in particolare per le libertà fondamentali e i diritti degli interessati, giustifica la natura assoluta del divieto di cui all'articolo 9, par. 1, GDPR (causa C-252/21, punto 70), che si applica quindi a prescindere dalla finalità dichiarata dal titolare del trattamento.

6. *La Corte di giustizia si esprime sulla legittimazione attiva da parte dei concorrenti introducendo un ulteriore meccanismo di tutela per l'efficacia del GDPR.*

Rispetto alla prima questione pregiudiziale, la Corte di Lussemburgo assume una decisione in linea con la giurisprudenza sopra menzionata. In questa nuova pronuncia, la Corte ha

offerto un vero e proprio esempio di dogmatica giuridica, il cui percorso argomentativo è basato sul tenore letterale, sull'impianto generale e, sugli obiettivi del GDPR, nonché sul principio dell'*effet utile*, spesso invocato in giurisprudenza (sul quale v. R. ORMAND, *L'interpre tation des Traite s europe ens selon leur "effet utile"*, Paris, 1975).

Nel dettaglio, sebbene il tenore letterale delle disposizioni contenute nel capo VIII del GDPR non contemplino espressamente la legittimazione alla proposizione di una azione inibitoria da parte dei concorrenti, la Corte chiarisce che tale "lacuna" non vada intesa come una scelta intenzionale del legislatore. La *ratio* è legata alla natura delle sue disposizioni, volte ad introdurre i principi per la protezione dei dati personali degli interessati (come previsto dagli articoli 5 e 6 del GDPR), che mirano ad assicurare il pieno rispetto del diritto fondamentale alla protezione dei dati personali degli interessati, garantito all'articolo 16, par. 1, TFUE e all'articolo 8 della Carta.

È pertanto pacifico che, in prima battuta, il GDPR si rivolga agli interessati, principali destinatari della protezione dei dati personali (causa C-21/23, punto 54).

Tuttavia, in conformità con quanto già deciso nella sentenza *Meta Platforms* (causa C-252/21, punti 50 e 51), la Corte ribadisce che l'accesso ai dati personali ed il loro sfruttamento rivestono un'importanza fondamentale nell'ambito dell'economia digitale, costituendo un parametro significativo della concorrenza tra imprese. Pertanto, per tener conto della realtà di questa evoluzione economica e garantire una concorrenza leale, risulta «*necessario tener conto delle norme in materia di protezione dei dati personali nell'ambito dell'applicazione (…) delle norme relative alle pratiche commerciali sleali*», riaffermando così il collegamento tra protezione dei dati personali e pratiche commerciali sleali già delineato in entrambe le decisioni *Meta Platforms* (rispettivamente: C-391/20, punto 66 e causa C-21/23, punto 56). In tal senso, le normative del GDPR costituiscono una regola di condotta per le imprese operanti nel mercato; di conseguenza, la loro violazione può costituire *anche* un atto di concorrenza sleale.

Tuttavia, l'attribuzione della legittimazione ai concorrenti per agire in giudizio, impone alla Corte di interpretare le disposizioni del GDPR superando un ostacolo letterale, giacché gli articoli da 77 a 79 del GDPR attribuiscono il diritto di presentare reclamo e di agire in giudizio agli «*interessati*» ai sensi l'articolo 4, par. 1, GDPR nozione che, non include i concorrenti.

Difatti, se è ben vero che la violazione delle disposizioni sostanziali volte alla protezione dei dati personali siano tali da pregiudicare in prima linea gli interessati dei dati, è altresì vero che queste possono arrecare pregiudizio ai terzi. Tale impostazione sembrerebbe essere corroborata dal tenore letterale dell'articolo 82, paragrafo 1 del GDPR il quale prevede un diritto al risarcimento per «chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento». Inoltre, non si può negare che dai termini degli articoli 77, 78 e 79 al loro paragrafo 1, si evince con chiarezza che il diritto di proporre reclamo a un'autorità di controllo, nonché il diritto a un ricorso giurisdizionale effettivo, si intendono «*fatt[i] salvi[ ]*» eventuali altri ricorsi amministrativi, giurisdizionali o extragiudiziali (causa C-21/23, punto 53).

A *fortiori*, la Corte afferma che sulla base di una interpretazione dell'impianto generale del GDPR, l'articolo 1, paragrafo 1 del GDPR, letto unitamente ai considerandi 9 e 13, si prevede una armonizzazione delle legislazioni nazionali in materia che è, in linea di principio completa, non lasciando margini di discrezionalità per ulteriori interventi in senso ampliativo del Regolamento; tuttavia, questa chiusura è da intendersi da un punto di vista sostanziale.

Pur mancando, nel caso di specie, una "*clausola di apertura*" analoga a quella di cui all'articolo 80, par. 2, GDPR, richiamata nella prima pronuncia *Meta Platforms* (causa C-

319/20, punto 57), la Corte chiarisce che «la completa armonizzazione del GDPR non si estende ai mezzi di ricorso» (causa C-21/23, punto 59). Ciò implica che il legislatore dell'Unione «non ha inteso, in particolare, escludere una siffatta possibilità per il concorrente di un'impresa di proporre un ricorso dinanzi ai giudici civili sulla base del divieto delle pratiche commerciali sleali per far cessare la violazione delle disposizioni sostanziali del RGPD» (causa C-21/23, punto 60).

La stessa Corte sostiene, pertanto, che siffatta possibilità sia anche corroborata dagli obiettivi del GDPR. Ne discende che la legittimazione ad agire di attori privati contribuisce agli obiettivi del GDPR, assicurando un'efficace protezione dei diritti e delle libertà fondamentali delle persone fisiche, nonché a garantire un elevato livello di protezione dei dati personali, come previsto dall'articolo 16, par. 1, TFUE e dall'articolo 8 della Carta. Tale legittimazione è funzionale a rafforzare il diritto degli interessati e degli obblighi di coloro che effettuano il trattamento dei dati, nonché ad assicurare poteri equivalenti negli Stati membri volti controllare il rispetto delle norme del GDPR (considerando 11 del GDPR). Inoltre, il riconoscimento della legittimazione ad agire ai terzi interessati è garanzia di maggiore trasparenza e di certezza del diritto per gli operatori economici (considerando 13 del GDPR). Pertanto, mirando al rafforzare i diritti degli interessati ad assicurare loro un elevato livello di protezione, questa è in linea con il principio di efficacia il c.d. "*effet utile*" del diritto dell'Unione europea (causa C-21/23, punto 62).

A livello procedurale, rispetto ad un possibile pregiudizio del sistema dei mezzi di ricorso previsti dal Capo VIII, la Corte stabilisce che tale legittimazione «si aggiunge ai mezzi di ricorso previsti agli articoli da 77 a 79 del RGPD, che sono pienamente preservati e possono sempre essere esercitati dagli interessati». Al fine di scongiurare il rischio di *ne bis in idem*, la Corte precisa che il ricorso attivabile ai sensi della legge sulla concorrenza sleale per la cessazione della violazione del GDPR, non persegue il fine di tutelare le libertà e dei diritti fondamentali degli interessati, ma mira ad assicurare una concorrenza leale tra le imprese, nell'interesse in particolare di tale concorrente.

Infine, come ha osservato il governo tedesco, l'applicazione e l'interpretazione uniforme del GDPR da parte dei giudici civili, rimane garantita dalla procedura preliminare ai sensi dell'articolo 267 TFUE (causa C-21/23, punti 65-67).

Alla luce di quanto sopra, la Corte di giustizia stabilisce la possibilità che i concorrenti agiscano in giudizio al fine di chiedere un'azione inibitoria, per violazione di detto Regolamento e sul fondamento del divieto delle pratiche commerciali sleali (causa C-21/23, punti 71-72).

La pronuncia in esame, pur muovendo da una lacuna del GDPR, approda pertanto ad un'interpretazione estensiva del testo normativo, la quale risulta tuttavia coerente con il principio dell'effetto utile del diritto dell'Unione, nonché giustificata dalla necessità adattare le norme ivi contenute alle dinamiche dell'economia digitale.

Attribuendo ai concorrenti danneggiati da tali pratiche commerciali sleali il diritto di poter agire in giudizio, la Corte garantisce un miglior controllo dell'applicazione delle norme del GDPR, nonché un'effettiva tutela del corretto comportamento delle imprese nella dialettica competitiva, a beneficio sia degli interessati dei dati e sia dei concorrenti.

La Corte di Giustizia dell'Unione Europea ha delineato i confini di questa nuova dimensione normativa, stabilendo se e in che misura il GDPR possa fungere da parametro di lealtà commerciale e se le azioni processuali attivabili dai concorrenti possano rafforzare indirettamente la tutela dei dati personali, creando un sistema integrato di *enforcement* che coniuga protezione della *privacy* e lealtà concorrenziale.

Questa pronuncia, pertanto, non solo chiarisce l'efficacia trasversale del GDPR, ma amplia significativamente la tutela dei dati personali nell'ecosistema digitale, rendendo la protezione dei dati una questione di conformità normativa e di correttezza concorrenziale.

7. *I dati relativi agli ordini online dei medicinali senza prescrizione come dati relativi alla salute ai sensi dell'articolo 9 del GDPR*

La seconda questione pregiudiziale è stata oggetto di visioni contrapposte da parte, rispettivamente, dell'Avvocato generale e della Corte. Da un lato, l'avvocato generale, (Conclusioni dell'Avvocato Generale M. Szpunar, presentate il 25 aprile 2024, per la causa C-21/23, ECLI:EU:C:2024:354) ritenendo che la decisione su questa fosse preliminare alla valutazione del merito della prima, ha modificato l'ordine delle domande proposte (par. 31 delle Conclusioni), rispondendo negativamente alla domanda in esame e soffermandosi solo in generale sulla questione relativa alla legittimazione.

Secondo l'opinione dell'AG, «i dati dei clienti di un farmacista che vengono trasmessi quando viene effettuato un ordine su una piattaforma di vendita online per farmaci solo in farmacia ma non soggetti a prescrizione medica non costituiscono "dati riguardanti la salute" ai sensi dell'articolo 4(15) e dell'articolo 9 del GDPR, nella misura in cui possono essere tratte solo conclusioni ipotetiche o imprecise sullo stato di salute della persona che effettua l'ordine online, che spetta al tribunale del rinvio verificare» (par. 54 delle conclusioni).

La Corte di Giustizia si è invece discostata da tale orientamento. Secondo la Corte, operare una distinzione tra dati personali soggetti a prescrizione medica, che pertanto consentono di tratte conclusioni sullo stato di salute dell'interessato ai sensi dell'articolo 4, par. 1 del GDPR, rispetto al caso in cui, invero, i medicinali non siano soggetti a prescrizione medica e, pertanto, possibilmente destinati non al soggetto acquirente, ma bensì a terzi, non risulterebbe conforme alla finalità di assicurare un elevato livello di protezione dei dati personali.

In questo contesto, la Corte sostiene che il divieto al trattamento dei dati personali in assenza del consenso esplicito sia «indipendente dal fatto che le informazioni rivelate dal trattamento in questione siano accurate o meno e che il gestore agisca allo scopo di ottenere informazioni rientranti in una delle categorie particolari menzionate all'articolo 8, paragrafo 1, della direttiva 95/46 e all'articolo 9, paragrafo 1, del RGPD». Difatti, valorizza, ritenendo prevalenti i «rischi significativi per le libertà fondamentali e i diritti fondamentali degli interessati, generati da qualsiasi trattamento di dati personali rientranti in tali categorie». Pertanto, richiamando il *dictum* della seconda sentenza *Meta Platforms* (C-252/21), «nel caso in cui un utente di una piattaforma online comunichi dati personali quando ordina medicinali la cui vendita è riservata alle farmacie senza essere soggetta a prescrizione medica, il trattamento di tali dati da parte del gestore di una farmacia che vende tali medicinali attraverso tale piattaforma online deve essere considerato un trattamento riguardante dati relativi alla salute, ai sensi dell'articolo 8, paragrafo 1, della direttiva 95/46 e dell'articolo 9, paragrafo 1, del RGPD, dato che tale trattamento di dati è idoneo a rivelare informazioni sullo stato di salute di una persona fisica, a prescindere dal fatto che tali informazioni riguardino tale utente o qualsiasi altra persona per la quale quest'ultimo effettua l'ordine» (causa C-21/23, punti 87-88,).

Come emerge dal considerando 51 del GDPR, infatti, i trattamenti di dati particolarmente sensibili comportano un'ingerenza di maggiore portata nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli

articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Di conseguenza, il regime previsto per i «dati relativi alla salute» non può essere attenuato o variato in ragione della circostanza che il medicinale sia o meno soggetto a prescrizione medica (causa C-21/23, punto 89).

Pertanto, tali dati costituiscono dati relativi alla salute e soggetti al consenso di cui all'articolo 9, par. 2, anche quando sia solo con una certa probabilità, e non con assoluta certezza che tali medicinali siano destinati a tali clienti (causa C-21/23, punto 90).

8. *Riflessioni conclusive*

Più che concentrarsi sulla seconda domanda pregiudiziale, che comunque si esprime nel senso di un ampliamento del novero dei dati personali ritenuti sensibili, il quale è stato più o meno soggetto a critica (M. VAN DEN POEL, *Case C-21/23 Lindenapotheke – Competitors can enforce GDPR-based unfair commercial practices, and a broadening concept of health and sensitive data*, in *European Law Blog*, 2024) è interessante approfondire la portata della decisione sulla prima domanda pregiudiziale.

La Corte, in assenza di un'esplicita indicazione normativa, ha stabilito che i concorrenti vantano la legittimazione ad agire in giudizio per violazione del GDPR, avvalendosi della disciplina in materia di concorrenza sleale. In tal modo, l'organo giudicante ha riconosciuto un ulteriore strumento di tutela, funzionale a salvaguardare gli interessi dei soggetti i cui dati siano stati trattati illecitamente, ma anche gli interessi economici dei concorrenti lesi da una condotta contraria alle regole di mercato.

Tale statuizione costituisce un precedente di rilievo poiché attribuisce al GDPR una funzione regolatrice della dialettica concorrenziale, configurandolo come parametro di lealtà commerciale. In questo modo, la Corte ha esteso la tutela dei dati personali introducendo un ulteriore strumento di *enforcement* privato, finalizzato non solo a salvaguardare i diritti degli interessati, ma anche a tutelare gli interessi economici dei concorrenti danneggiati da un trattamento illecito di dati personali che falsi le dinamiche di mercato.

La pronuncia ha un duplice effetto: da un lato, incentiva gli operatori economici a conformarsi al GDPR per evitare azioni legali anche da parte dei concorrenti; dall'altro, attribuendo ai concorrenti la legittimazione ad agire, amplia il perimetro di controllo sul rispetto delle norme in materia di protezione dei dati personali, contribuendo a superare le criticità legate all'inefficacia del GDPR nei mercati digitali.

Tale inefficacia sarebbe ascrivibile, da un lato, alla portata "restrittiva" dei suoi obiettivi, limitati alla protezione dei dati personali, come testimonia la nozione di "interessato" nella fattispecie e, dall'altro, all'impossibilità che il GDPR distingua tra titolari del trattamento dei dati personali di piccole dimensioni e di grandi dimensioni, in caso di violazione delle sue disposizioni. In questo secondo caso, la portata della violazione del GDPR, si riverbera su un numero di utenti superiore, con un significativo aumento della portata del danno (F.COSTA-CABRAL, O. LYNSKEY, *Family ties: The intersection between data protection and competition in EU law*, in *Common Market Law Review*, 2017, Issue 1, pp. 11-50).

Ne discende che la legittimazione ad agire in giudizio da parte delle imprese, si configura quale strumento "complementare" rispetto alle tutele già contemplabili singolarmente dalle varie normative di settore. La sentenza de qua si colloca, pertanto, in un contesto giuridico dinamico e di evoluzione interpretativa, accompagnato anche da un vivace confronto sviluppatosi in dottrina, il quale aveva già sottolineato il bisogno di un "*approccio più collaborativo*" tra le discipline di concorrenza e di protezione dei dati personali (W. KERBER,

Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law, in *The Antitrust Bulletin*, 2022, pp. 280-301).
Sul punto, si può altresì affermare come la decisione si ponga in un'ottica di incoraggiamento degli Stati membri a predisporre, nell'ambito dei rispettivi ordinamenti nazionali, ulteriori strumenti di tutela ispirati a un approccio olistico tra due discipline (R. VANDENDRIESSCHE, *Using Data Protection Law to Fight Data-Related Anticompetitive Conduct Expanding the "Meta Model"? Lindenapotheke (C-21/23),* in *Kluwer Competition Law Blog,* 2024).

Ad ogni modo, questa impostazione non è esente da criticità. Si potrebbe osservare che le implicazioni di tale sentenza, andrebbero ad aggiungersi ad una già complessa rete di procedure di applicazione del GDPR. In effetti, in forza di tale pronuncia, e in aggiunta alla competenza già riconosciuta alle autorità antitrust di valutare eventuali violazioni del GDPR (cfr. sentenza C-252/21), potrebbero sorgere interferenze fra l'*enforcement* di tipo amministrativo e quello giudiziario. Ciò potrebbe tradursi in procedimenti paralleli, radicati presso diversi organi giurisdizionali nazionali e presso le autorità di protezione dei dati, con il rischio di pronunce divergenti relativamente al medesimo trattamento di dati personali.

Tuttavia, la centralità del rinvio pregiudiziale, nonché i meccanismi di cooperazione tra le autorità, uniti alla scarsa probabilità di duplicazioni processuali o sentenze in contrasto, attenuano tali pericoli, escludono che possano giustificare la mancata estensione della legittimazione ad agire ai concorrenti ai sensi del GDPR (G. GENTILE, O. LYNSKEY, *Deficient By Design? The Transnational Enforcement Of The Gdpr,* in *International and Comparative Law Quarterly*, vol. 71, 2022).

Sul punto, va inoltre segnalata la recente Proposta della Commissione, finalizzata all'introduzione di ulteriori norme procedurali per l'applicazione del GDPR (*Proposal for a Regulation of the European Parliament and of the Council, laying down additional procedural rules relating to the enforcement of Regulation* (EU) 2016/679, Bruxelles, 4.7.2023, COM (2023) 348 *final*).

A ciò si aggiunga la seconda Relazione sull'applicazione del Regolamento generale sulla protezione dei dati (Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati, Bruxelles, 25.7.2024, COM(2024) 357 *final*), che pone l'enfasi sulla «governance delle nuove norme sul digitale», sottolineando come lo sviluppo della legislazione in tale settore comporti «la necessità di una stretta cooperazione in tutti i settori normativi». Nel medesimo documento si legge che «tale cooperazione è tanto più necessaria in quanto le questioni relative alla protezione dei dati si intersecano sempre più con le questioni relative, ad esempio, al diritto della concorrenza, al diritto dei consumatori, alle norme sui mercati digitali, alla regolamentazione delle comunicazioni elettroniche e alla cibersicurezza»; di qui l'esigenza di consolidare la «rete di cooperazione per la tutela dei consumatori», istituendo, tra l'altro, «*task force*» specifiche per l'interazione tra protezione dei dati, concorrenza e tutela dei consumatori.

La necessità di tale interconnessione emerge con ancor più evidenza quando si tratta di garantire un mercato digitale più equo e contenibile, ad esempio con il Regolamento (UE) 2022/1925, *Digital Markets Act* (Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio, relativo a mercati equi e contendibili nel settore digitale, Digital Markets Act - DMA, 14 settembre 2022, in *GUUE*, L 265/1; si veda G. CONTALDI, *Il DMA (Digital Markets Act) può contribuire alla protezione dei dati degli utenti online?,* in *DUDI*, pp. 77-94).

Il DMA riserva alla Commissione europea la competenza esclusiva per la propria applicazione (articolo 37 DMA), ma al contempo prevede un raccordo con le disposizioni del GDPR e con le autorità deputate alla sua tutela attraverso l'istituzione di un organismo di cooperazione, il Gruppo di Alto Livello (articolo 40 DMA). Tale Gruppo, composto anche

dal Comitato Europeo per la Protezione dei Dati e dal Garante Europeo per la protezione dei Dati, è incaricato di fornire consulenza e interpretazioni del DMA ogniqualvolta la Commissione si trovi a deliberare su ambiti inerenti alle competenze di tali organi. Questa impostazione testimonia la crescente integrazione fra i diversi settori regolatori nell'economia digitale.

Tale decisione rappresenta, dunque, l'ulteriore tassello di un mosaico giurisprudenziale europeo, che delinea una convergenza normativa tra protezione dei dati personali e concorrenza leale, istituendo una tutela multilivello dei diritti fondamentali nell'innovativo e rischioso ecosistema digitale. Conferisce al GDPR una funzione regolatrice della dialettica tra operatori economici, non solo a garanzia dell'equità e della competitività dei mercati digitali, bensì anche una funzione a beneficio di un sistema più incisivo e coordinato nell'applicazione delle regole in materia di protezione dei dati.

Si delinea progressivamente un'interconnessione tra discipline apparentemente distinte, ma destinate a convergere ogniqualvolta si manifestino comportamenti lesivi del mercato, dei concorrenti e, simultaneamente, della protezione dei dati personali all'interno dell'ordinamento dell'Unione europea.

BEATRICE LUPACCHINI