Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 - Fascicolo n. 1/2024

BlogDUE

L'obbligo di leale cooperazione tra autorità nazionali garanti della concorrenza e autorità di controllo istituite dal RGPD nella sentenza *Meta Platforms e a.*

Martina Previatello (Assegnista di ricerca presso l'Università degli Studi di Trieste) – 10 febbraio 2024

SOMMARIO: 1. Introduzione. – 2. Il caso *Meta Platforms e a.*: i fatti di causa e i quesiti pregiudiziali relativi ai rapporti tra le autorità nazionali garanti della concorrenza e le autorità di controllo istituite dal regolamento generale sulla protezione dei dati. – 3. La sentenza della Corte: l'obbligo di cooperazione tra autorità. – 4. Le modalità della collaborazione: una valutazione d'insieme. – 5. Conclusioni.

1. Nel caso *Meta Platforms e a.*, del 4 luglio 2023, la Corte di giustizia ha chiarito se e a quali condizioni un'autorità nazionale garante della concorrenza può – nell'ambito di un procedimento che potrebbe condurre all'accertamento e alla sanzione di un abuso di posizione dominante – constatare che un trattamento di dati personali è stato effettuato senza rispettare quanto prescritto dal regolamento generale sulla protezione dei dati (in seguito anche: "RGPD" o "reg. 2016/679"; v. sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms e a.*, su cui v. in dottrina P. MANZINI, *Antitrust e privacy: la strana coppia*, in *Quaderni AISDUE*, n. 10, 15 settembre 2023, p. 196 ss.; I. GRAEF, *The European Court of Justice in Meta Platforms leaves competition and data protection authorities with an assignment*, in *European Law Blog*, n. 30, 19 July 2023; I. GRAEF, Meta platforms: *How the CJEU leaves competition and data protection authorities with an assignment*, in *Maastricht Journal of European and Comparative Law*, 2023, p. 325 ss.; P. G. PICHT, *CJEU on Facebook: GDPR Processing Justifications and Application Competence*, in *Gewerblicher Rechtsschutz und Urheberrecht*, n. 16, 2023, p. 1169 ss.).

Si tratta di una pronuncia innovativa, che affronta questo tema per la prima volta. La giurisprudenza precedente si era, infatti, occupata del sistema di cooperazione tra le autorità istituite dal RGPD (v. sentenza della Corte del 15 giugno 2021, causa C-645/19, *Facebook Ireland e a.*), ma non aveva preso in considerazione i rapporti tra quest'ultime e le autorità nazionali antitrust. In

assenza di una disciplina specifica nei rilevanti atti di diritto derivato, la Corte ha desunto taluni obblighi di collaborazione e di coordinamento direttamente dal principio di leale collaborazione, previsto dall'art. 4, par. 3, TUE. Autorità amministrative, che hanno compiti distinti e perseguono obiettivi diversi, devono cooperare tra loro al fine di garantire, da un lato, l'effettiva applicazione del diritto della concorrenza dell'Unione e, dall'altro, la coerenza del sistema di protezione dei dati personali istituito dal RGPD (sul principio di leale cooperazione tra gli Stati membri v. P. DE PASQUALE, *Commento all'art. 4 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, spec. p. 28 ss.; M. KLAMERT, *Article 4 TEU*, in M. KELLERBAUER ET AL. (eds.), *The EU Treaties and the Charter of Fundamental Rights — A Commentary*, Oxford, 2019, p. 35 ss.; F. CASOLARI, *La leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020, p. 73 ss.).

Si tratta, inoltre, di una pronuncia particolarmente rilevante, che riguarda un contesto economico dominato dalle grandi piattaforme digitali. Queste raccolgono un'enorme quantità di dati degli utenti, che poi utilizzano per la loro attività commerciale.

Il presente contributo si propone di sottolineare le innovazioni introdotte dalla sentenza in commento rispetto al diritto vigente, nel quale manca una regolamentazione dei rapporti tra autorità privacy e autorità garanti della concorrenza. Inoltre, esso intende chiarire in che modo il principio di leale collaborazione incide sui rapporti tra queste autorità.

Per raggiungere tali obiettivi, il lavoro è strutturato come segue. Dopo la presente introduzione, si ricorderanno brevemente i fatti all'origine della controversia e i quesiti pregiudiziali posti dal giudice del rinvio, che riguardano i poteri delle autorità nazionali garanti della concorrenza in materia di protezione dei dati personali (par. 2). Seguirà un'analisi della sentenza, limitatamente a detti quesiti (par. 3), con un focus sulle modalità di cooperazione tra le diverse autorità coinvolte (par. 4). Saranno infine tratte le dovute conclusioni (par. 5).

2. La sentenza in commento trae origine da un rinvio pregiudiziale effettuato dal Tribunale di Düsseldorf, nell'ambito di una controversia che vedeva opposti Meta Platforms, Meta Platforms Ireland e Facebook Deutschland (in seguito: Meta/Facebook) all'autorità tedesca garante della concorrenza (in seguito anche: "Bundeskartellamt").

Il caso riguardava il trattamento, da parte di Meta/Facebook, dei c.d. dati *off* Facebook, vale a dire di quei dati relativi ad attività condotte dagli utenti fuori dal social network. Può trattarsi, da un lato, di dati che riguardano la consultazione di pagine Internet e di applicazioni di terzi, che sono collegate a Facebook attraverso interfacce di programmazione e, dall'altro, di dati riguardanti l'utilizzo degli altri servizi online offerti dal gruppo Meta, di cui anche Facebook fa parte, tra i quali ad esempio Instagram o WhatsApp.

Tali dati *off* Facebook – insieme a quelli raccolti all'interno del social network e a quelli forniti all'atto dell'iscrizione al servizio – sono messi in

relazione con l'account dell'utente per crearne un profilo dettagliato a fini commerciali. Com'è noto, infatti, Facebook nasce come un servizio offerto gratuitamente, che si finanzia tramite la pubblicità online. Questa è tanto più efficace e mirata quanto più è possibile conoscere nel dettaglio i comportamenti e gli interessi dell'utente-consumatore.

L'autorità tedesca garante della concorrenza ha considerato le condizioni generali concernenti il trattamento dei dati *off* Facebook contrarie al RGPD, in particolare, agli artt. 6, par. 1, lett. a), e 9, par. 2, lett. a), i quali richiedono il consenso dell'interessato al trattamento dei suoi dati personali per una o più finalità specifiche (sul punto v. S. DIENST, *Lawful processing of personal data in companies under the General Data Protection Regulation*, in T. KUGLER, D. RÜCKER (eds.), *New European General Data Protection Regulation: A Practitioner's Guide*, Baden-Baden, 2018, p. 49 ss.; W. KOTSCHY, *Article 6. Lawfulness of processing*, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020, p. 321 ss.; B. QUINN, *Data Protection Implementation Guide: A Legal, Risk and Technology Framework for GDPR*, Alphen aan den Rijn, 2021, p. 59 ss.; G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, p. 63 ss.; C. DE TERWANGNE, K. ROSIER, *Le réglement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Bruxelles, 2018, p. 118 ss.). Il trattamento operato da Facebook è stato considerato illecito, in quanto le condizioni generali imposte agli utenti, da un lato, subordinavano l'uso del social network alla possibilità di trattamento di questi dati e, dall'altro, consentivano il trattamento in questione anche in mancanza di un valido e specifico consenso degli interessati. È importante sottolineare che, secondo il Bundeskartellamt, proprio l'illecito trattamento dei dati personali degli utenti iscritti al social network rappresentava un comportamento abusivo, ai sensi dell'art. 102 TFUE, e comportava quindi un abuso di posizione dominante vietato da questa disposizione (v. punto 31 della sentenza).

Contro la decisione dell'autorità tedesca garante della concorrenza, Meta/Facebook ha proposto ricorso davanti al Tribunale di Düsseldorf.

Quest'ultimo ha, tra le altre cose, considerato che la competenza a vigilare sull'osservanza del RGPD è attribuita ad autorità di controllo specificamente istituite.

Infatti, gli artt. 51 ss. del reg. 2016/679 disciplinano l'istituzione di autorità di controllo indipendenti in ogni Stato membro e affidano a queste autorità il compito di controllare che il RGPD sia correttamente applicato su tutto il territorio dell'Unione, dotandole di appositi poteri di indagine, correttivi e sanzionatori (v. art. 58, reg. 2016/679).

Di norma, ogni autorità di controllo è competente a sorvegliare la corretta attuazione del RGPD sul territorio del rispettivo Stato membro (v. art. 55, par. 1, del reg. 2016/679). Tuttavia, in caso di trattamento transfrontaliero di dati personali l'art. 56, par. 1, precisa che è competente l'autorità di controllo capofila, ossia l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento (ai sensi dell'art. 4, punto 23,

del reg. 2016/679, un trattamento transfrontaliero può avere luogo qualora il titolare del trattamento sia stabilito in più Stati membri oppure qualora, pur essendo il titolare del trattamento stabilito in un solo Stato membro, esso svolga un trattamento di dati che incide in modo sostanziale su interessati in più di uno Stato membro; su questi aspetti v. P. VOIGT, A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham, 2017, p. 189 ss.; M. MACCHIA, C. FIGLIOLA, *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, in *Giornale di diritto amministrativo*, n. 4, 2018, p. 423 ss.).

In considerazione delle specifiche competenze attribuite alle autorità istituite dal RGPD, il Tribunale di Düsseldorf si è, tra le altre cose, interrogato sulla sussistenza del potere di un'autorità nazionale garante della concorrenza di constatare una violazione del reg. 2016/679 nell'ambito di un procedimento antitrust, nonché sulla permanenza di detto potere nel caso in cui un'indagine sulla stessa condotta sia in corso innanzi all'autorità di controllo capofila nello Stato membro in cui si trova lo stabilimento principale del titolare del trattamento dei dati. Nel contesto di un rinvio pregiudiziale più ampio, tali quesiti sono stati sottoposti alla Corte giustizia, ai sensi dell'art. 267 TFUE (v. primo e settimo quesito e punto 36 della sentenza).

3. La sentenza, nella parte che qui interessa, mette subito in chiaro che il giudice del rinvio ha chiesto, in sostanza, di colmare, in via giurisprudenziale, una lacuna normativa, in quanto il diritto derivato dell'Unione non disciplina in alcun modo la cooperazione tra le autorità nazionali garanti della concorrenza e le autorità di controllo istituite dal RGPD (v. punto 43 della sentenza).

Infatti, la regolamentazione vigente riguarda soltanto i rapporti tra le diverse autorità istituite dal reg. 2016/679. In particolare, risulta disciplinata la cooperazione tra le autorità nazionali di controllo interessate e l'autorità di controllo capofila nonché, se del caso, la cooperazione di tali autorità con il comitato europeo per la protezione dei dati e la Commissione. La giurisprudenza precedente si è limitata a chiarire l'interpretazione delle disposizioni relative a queste forme di collaborazione espressamente previste, ma non disciplinate in modo dettagliato dal RGPD (v. sentenza *Facebook Ireland e a.*, cit.).

Svolta questa premessa, la Corte ha riconosciuto la competenza delle autorità nazionali antitrust a interpretare le disposizioni del RGPD al fine di constatare una violazione del diritto della concorrenza e, nella specie, un abuso di posizione dominante.

Anzitutto, la Corte ha sottolineato che nel reg. 2016/679 non vi è alcuna disposizione che escluda espressamente detta competenza (v. punto 43 della sentenza).

Inoltre, la Corte ha ricordato che le autorità di controllo istituite dal RGPD e le autorità antitrust esercitano compiti e perseguono obiettivi diversi (v. punto 44 ss. della sentenza). Da un lato, infatti, il RGPD assegna alle autorità di controllo il compito di vigilare sul rispetto di tale regolamento e di garantire

che esso sia coerentemente applicato sul territorio dell'Unione, "al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali nonché di agevolare la libera circolazione di tali dati all'interno dell'Unione" (v. punto 45 della sentenza e art. 51, par. 1, del reg. 2016/679, cit.). Dall'altro, le autorità antitrust hanno il compito di assicurare che la concorrenza nel mercato interno non sia falsata da comportamenti anticoncorrenziali posti in essere dalle imprese; in particolare, le autorità nazionali garanti della concorrenza possono adottare, sulla base dell'art. 5 del reg. 1/2003, decisioni che constatano e sanzionano un abuso di posizione dominante, ai sensi dell'art. 102 TFUE.

La Corte ha precisato che l'indagine che conduce l'autorità antitrust ad adottare una simile decisione deve tenere in considerazione tutti gli elementi rilevanti per valutare "sulla base di tutte le circostanze del caso di specie, se il comportamento dell'impresa in posizione dominante abbia l'effetto di ostacolare, ricorrendo a mezzi diversi da quelli su cui si impernia la concorrenza normale tra prodotti o servizi, la conservazione del grado di concorrenza esistente sul mercato o lo sviluppo di detta concorrenza". Nei casi come quello in esame, ha precisato la Corte, va presa in considerazione anche l'esistenza di un comportamento contrario al RGPD da parte di una società operante sul mercato dei servizi digitali. Infatti, la violazione di questo regolamento può costituire un "importante indizio" per stabilire se la condotta di un'impresa che detiene una posizione dominante sul mercato "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" (v. punto 47 della sentenza).

La Corte ha sottolineato che, in un mercato peculiare qual è quello digitale, la potenza commerciale delle imprese si esprime soprattutto attraverso l'accesso ai dati personali degli utenti e il loro trattamento. In effetti, come la Corte ha chiarito, l'accesso ai dati personali nonché il loro sfruttamento rivestono un'importanza fondamentale nell'ambito dell'economia digitale e sono diventati un parametro significativo della concorrenza fra imprese. Ciò vale in particolare nel caso delle società che gestiscono i social network, le quali traggono finanziamento e profitto dalla profilazione degli utenti allo scopo di proporre loro forme di pubblicità mirata a fini commerciali. Escludere in un caso del genere la competenza dell'autorità nazionale garante della concorrenza a valutare – nell'ambito di un'indagine volta a constatare un abuso di posizione dominante – la conformità di un trattamento dei dati al RGPD significherebbe pregiudicare l'effettiva applicazione del diritto antitrust sul territorio dell'Unione (v. punti 50-51 della sentenza).

La Corte di giustizia ha aggiunto che il riconoscimento di questo potere alle autorità nazionali garanti della concorrenza non comporta alcuna sostituzione di quest'ultime nelle competenze delle autorità di controllo istituite dal RGPD, in quanto le une e le altre agiscono, nell'ambito delle rispettive competenze, per raggiungere obiettivi distinti, che sono stabiliti, da un lato, dall'art. 102 TFUE e, dall'altro, dal RGPD (v. punto 49 della sentenza).

Ciò posto, la Corte di giustizia ha chiarito quali sono le modalità di esercizio e i limiti di questa competenza riconosciuta alle autorità antitrust (v. punto 52 ss. della sentenza).

La Corte ha stabilito che "nel caso in cui un'autorità nazionale garante della concorrenza ritenga necessario pronunciarsi, nell'ambito di una decisione relativa ad un abuso di posizione dominante, sulla conformità o sulla non conformità al RGPD di un trattamento di dati personali effettuato dall'impresa in questione, tale autorità e l'autorità di controllo interessata o, se del caso, l'autorità di controllo capofila competente ai sensi di tale regolamento devono cooperare tra loro" (v. punto 52 della sentenza).

Seguendo le indicazioni dell'Avvocato generale (v. punto 28 ss. delle conclusioni), la Corte ha sostenuto che autorità antitrust e autorità privacy devono collaborare tra loro, sottolineando che detto obbligo di cooperazione discende direttamente dal diritto primario e, in particolare, dal principio di leale cooperazione, di cui all'art. 4, par. 3, TUE, che include anche l'obbligo di leale cooperazione tra le autorità amministrative degli Stati membri (v. punto 53 della sentenza).

La Corte di giustizia ha desunto dal principio in questione obblighi piuttosto stringenti, soprattutto in capo alle autorità nazionali antitrust, ma anche, seppur in misura minore, a carico delle autorità di controllo istituite dal reg. 2016/679.

Per quanto riguarda le autorità nazionali garanti della concorrenza, la Corte ha stabilito che queste devono innanzitutto verificare se l'autorità nazionale di controllo competente, l'autorità di controllo capofila o la Corte di giustizia abbiano già pronunciato una decisione in merito al comportamento oggetto di indagine (o ad un comportamento simile).

In un'ipotesi del genere, l'autorità nazionale antitrust è tenuta ad attenersi a tale decisione, salva la possibilità di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto antitrust. Qualora essa "nutra dubbi sulla portata della valutazione effettuata dall'autorità nazionale di controllo competente o dall'autorità di controllo capofila […] deve consultare tali autorità e chiederne la cooperazione, al fine di fugare i propri dubbi […]" (v. punto 57 della sentenza).

Nel caso in cui, invece, non vi siano decisioni delle autorità privacy – perché un'indagine non è stata avviata o è ancora in corso – l'autorità antitrust è tenuta ad attivare la cooperazione con l'autorità nazionale di controllo competente o con l'autorità di controllo capofila, allo scopo di "determinare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione" (v. punto 57 della sentenza).

Con riguardo poi alle autorità privacy, la Corte ha precisato che queste sono tenute, in forza dell'art. 4, par. 3, TUE, a rispondere alle richieste di informazioni e di cooperazione provenienti da autorità nazionali garanti della concorrenza. In particolare, nel caso in cui l'autorità antitrust nutra dubbi riguardo una decisione già emanata, l'autorità di controllo dovrà comunicare alla prima "le informazioni di cui dispone che possano consentire di fugare

[tali] dubbi". In caso di assenza di decisione, l'autorità di controllo deve informare l'autorità antitrust della volontà o meno di avviare un procedimento (v. punto 58 della sentenza).

Qualora l'autorità di controllo consultata dall'autorità nazionale antitrust non risponda entro un termine ragionevole, quest'ultima può proseguire la propria indagine. Lo stesso vale nel caso in cui l'autorità di controllo consultata non sollevi obiezioni "a che si prosegua tale indagine senza attendere l'adozione di una [sua] decisione" (v. punto 59 della sentenza).

4. La sentenza *Meta Platforms* ha riconosciuto alle autorità nazionali garanti della concorrenza il potere di accertare violazioni del RGPD nell'ambito di un'indagine volta a constatare un abuso di posizione dominante. Al tempo stesso, però, la pronuncia in esame ha sottolineato la centralità del ruolo delle autorità di controllo istituite dal reg. 2016/679.

In effetti, la sentenza in commento sottolinea la necessità di rispettare le decisioni adottate dalle autorità privacy. Nel caso in cui vi siano decisioni preesistenti rese da quest'ultime, le autorità nazionali antitrust sono tenute a conformarvisi. Qualora nutrano dubbi in merito a dette decisioni, devono interpellare l'autorità privacy, non potendo decidere autonomamente in maniera difforme.

Inoltre, il ruolo centrale dell'autorità privacy è preservato anche in assenza di una decisione. In tal caso, l'autorità antitrust deve comunque interpellare l'autorità di controllo, la quale può in tal modo valutare l'opportunità di avviare una propria indagine. A tal riguardo, è interessante sottolineare che questo adempimento imposto dalla Corte alle autorità nazionali garanti della concorrenza è coerente con quanto disposto dall'art. 57, par. 1, lett. h), del reg. 2016/679, il quale prevede che le autorità di controllo possono svolgere "indagini sull'applicazione" di detto regolamento "anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica". L'obbligo delle autorità antitrust di interpellare preventivamente le autorità privacy pone quest'ultime in condizione di attivarsi per dare avvio a un procedimento ai sensi del RGPD.

La sentenza *Meta Platforms* ha chiarito che l'autorità nazionale garante della concorrenza può valutare autonomamente la conformità di un determinato trattamento dei dati con il reg. 2016/679 soltanto in due ipotesi: i) nel "caso in cui l'autorità nazionale di controllo competente e l'autorità di controllo capofila", previamente consultate, "non sollevino obiezioni a che si prosegua tale indagine senza attendere l'adozione di una loro decisione"; e ii) in "assenza di risposta da parte dell'autorità di controllo interpellata entro un termine ragionevole" (v. punto 59 della sentenza).

Una lettura d'insieme delle indicazioni della Corte consente di affermare la priorità dell'intervento delle autorità appositamente istituite dal reg. 2016/679: le decisioni di queste autorità devono essere rispettate dalle autorità garanti della concorrenza; quest'ultime devono previamente rivolgersi alle prime, se intendono pronunciarsi, ai fini dell'applicazione dell'art. 102 TFUE, sulla compatibilità di un trattamento dei dati con il regolamento citato;

l'intervento autonomo delle autorità antitrust è riservato ai casi di assenza di obiezioni espresse o di mancata risposta entro un termine ragionevole.

L'esatta configurazione dei rapporti tra le autorità coinvolte richiede di sciogliere alcune questioni rilevanti, che la sentenza non ha affrontato.

Anzitutto, essa non specifica che cosa si debba intendere per "termine ragionevole" ai fini sopra indicati. Invero, non si tratta di una questione di poco conto, nella misura in cui la scadenza del termine comporta l'insorgere di un autonomo potere di valutazione in capo all'autorità antitrust.

Non è escluso che in futuro sia richiesto alla Corte di pronunciarsi su questo specifico aspetto. Fino ad allora, limitandosi ad un ragionamento per analogia, si potrebbe fare riferimento ai termini previsti dal RGPD per la cooperazione dell'autorità di controllo capofila con le altre autorità di controllo interessate. L'art. 56, par. 3, del reg. 2016/679 indica un termine di tre settimane entro cui l'autorità capofila deve comunicare, all'autorità di controllo interessata, se intende o meno trattare il caso secondo la procedura di cooperazione, di cui agli artt. 60 ss. Il termine di tre settimane potrebbe essere considerato ragionevole ed applicato anche nel contesto della collaborazione con le autorità nazionali garanti della concorrenza.

Inoltre, la pronuncia non considera l'ipotesi in cui l'autorità di controllo interpellata ritenga, all'esito di un sommario esame, di non aprire un'indagine, non ravvisando i presupposti per procedere in tal senso. Ci si potrebbe chiedere se, in un caso del genere, l'autorità antitrust possa valutare autonomamente la conformità del comportamento oggetto di indagine con il RGPD.

Una risposta affermativa potrebbe essere fornita argomentando che, in una simile ipotesi, non vi sarebbe una vera e propria decisione, resa dall'autorità privacy in esito ad un'indagine formale, in grado di vincolare l'autorità antitrust.

Tuttavia, la centralità del ruolo delle autorità privacy e il rilievo riconosciuto nella pronuncia in esame al principio di leale collaborazione conducono ad essere più cauti. In altre parole, l'esclusione, da parte dell'autorità di controllo istituita dal reg. 2016/679, dei presupposti necessari per iniziare un procedimento di accertamento dovrebbe vincolare l'autorità antitrust, la quale – in applicazione del principio di leale collaborazione – dovrebbe conformare la propria analisi a dette indicazioni, per quanto preliminari.

Tale interpretazione sembra garantire meglio l'uniforme applicazione del reg. 2016/679, escludendo "il rischio di divergenze" tra le diverse autorità in merito all'interpretazione del RGPD (in tal senso cfr. punto 55 della sentenza).

Inoltre, questa conclusione sembra confermata dalla considerazione, desumibile dalla sentenza (v. punti 38 e 45), per cui la competenza in materia di interpretazione e applicazione del reg. 2016/679 spetta, come regola generale, alle autorità di controllo istituite dal RGPD e soltanto in via d'eccezione alle autorità nazionali antitrust. Infatti, è la sentenza stessa che, come detto poc'anzi, si preoccupa di precisare che l'autorità nazionale garante della concorrenza gode del potere di valutare autonomamente la conformità di

un determinato trattamento dei dati con il RGPD unicamente nel caso in cui le autorità privacy non sollevino obiezioni e in caso di mancata risposta entro un termine ragionevole.

Se ne potrebbe dedurre, in linea con la regola secondo cui le eccezioni vanno interpretate restrittivamente, che in tutti gli altri casi non espressamente menzionati dalla Corte, l'autorità antitrust non possa decidere autonomamente sulla compatibilità o meno di un certo trattamento dei dati con il RGPD, dovendo invece attenersi a qualsiasi indicazione di merito dell'autorità privacy, sia essa resa in esito ad una vera e propria indagine, tramite una decisione, o al termine di un esame preliminare.

Ciò detto, è interessante notare che una simile ricostruzione dei rapporti tra le diverse autorità non rileva soltanto sul piano procedurale, ma presenta altresì implicazioni di carattere sostanziale (sul punto v. P. MANZINI, *op. cit.*, spec. p. 204 ss.; C. PERARO, *Quando la violazione della privacy costituisce un illecito antitrust: quali rimedi nell'ordinamento UE?*, in *rivista.eurojus.it*, n. 3, 2023, p. 50 ss.). La sentenza valorizza infatti il legame tra violazioni della privacy e sussistenza di un abuso di posizione dominante. In particolare, la Corte ha precisato che "la conformità o non conformità [di un comportamento dell'impresa in posizione dominante] alle disposizioni del RGPD può costituire, se del caso, un importante indizio fra le circostanze rilevanti del caso di specie per stabilire se siffatto comportamento 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" (v. punto 47 della sentenza, nonché punto 23 delle conclusioni).

Ne consegue che un'eventuale decisione dell'autorità privacy che constatasse la difformità di un comportamento tenuto da un'impresa in posizione dominante rispetto a quanto prescritto dal RGPD influenzerebbe in misura significativa le valutazioni svolte dall'autorità antitrust nell'ambito dell'indagine di sua competenza.

Ad ogni modo, il carattere vincolante della decisione dell'autorità privacy non predetermina l'esito del procedimento avviato per applicare l'art. 102 TFUE. La sentenza in commento precisa infatti che tale decisione, pur essendo vincolante per l'autorità antitrust, non impedisce a quest'ultima di trarne "le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza" (v. punto 56 della sentenza). Da questo passaggio sembra potersi dedurre che, in alcuni casi, potrebbe anche non sussistere un rapporto tra violazioni del RGPD e violazioni del diritto della concorrenza. In altri termini, un determinato comportamento potrebbe essere al contempo illecito sotto il profilo del RGPD, ma non costituire una violazione del diritto della concorrenza, e viceversa (in tal senso v. anche punto 23 e nota 18 delle conclusioni).

5. Nella sentenza esaminata, la Corte di giustizia riconosce in capo alle autorità nazionali garanti della concorrenza il potere di constatare, nell'ambito dell'esame di un abuso di posizione dominante, la non conformità con il RGPD delle condizioni generali d'uso di un'impresa relative al trattamento

dei dati personali, qualora tale constatazione sia funzionale all'accertamento dell'abuso.

Tuttavia, si tratta di un potere che subisce dei limiti rilevanti, in quanto esso dev'essere esercitato dalle autorità antitrust conformemente al principio di leale cooperazione, nel rispetto delle prerogative riconosciute alle autorità di controllo istituite dal reg. 2016/679.

In conclusione, è possibile affermare che la sentenza *Meta Platforms* riconosce a quest'ultime un ruolo centrale, in quanto autorità specificamente preposte a controllare l'applicazione del RGPD e ad assicurarne il rispetto. Le autorità antitrust sono vincolate dalle decisioni emesse da questi organi in relazione all'interpretazione del RGPD e, nel caso in cui questi non si siano ancora espressi, devono interrogarli prima di decidere circa una violazione dell'art. 102 TFUE connessa a un illecito trattamento dei dati personali.

Le valutazioni delle autorità privacy costituiscono un indizio significativo dell'esistenza di un abuso di posizione dominante, ma devono essere considerate alla luce di tutte le circostanze del caso di specie e non comprimono, quindi, del tutto l'autonomia decisionale delle autorità nazionali garanti della concorrenza.

ABSTRACT (ITA)

Nella sentenza *Meta Platforms e a*., del 4 luglio 2023, la Corte di giustizia riconosce in capo alle autorità nazionali garanti della concorrenza il potere di constatare, nell'ambito dell'esame di un abuso di posizione dominante, la non conformità con il RGPD delle condizioni generali d'uso di un'impresa relative al trattamento dei dati personali, qualora tale constatazione sia funzionale all'accertamento dell'abuso. In assenza di una disciplina specifica nei rilevanti atti di diritto derivato, la Corte ha desunto taluni obblighi di collaborazione e di coordinamento direttamente dal principio di leale collaborazione, previsto dall'art. 4, par. 3, TUE. Autorità amministrative, che hanno compiti distinti e perseguono obiettivi diversi, devono cooperare tra loro al fine di garantire, da un lato, l'effettiva applicazione del diritto della concorrenza dell'Unione e, dall'altro, la coerenza del sistema di protezione dei dati personali istituito dal RGPD. Il contributo si propone di sottolineare le innovazioni introdotte dalla sentenza in commento rispetto al diritto vigente. Inoltre, esso intende chiarire in che modo il principio di leale collaborazione incide sui rapporti tra queste autorità, riservando un ruolo centrale alle autorità di controllo istituite dal reg. 2016/679, in quanto autorità specificamente preposte a controllarne l'applicazione e ad assicurarne il rispetto. Come si dirà, una simile ricostruzione non rileva soltanto sul piano procedurale, ma presenta altresì implicazioni di carattere sostanziale.

ABSTRACT (ENG)

In the judgment *Meta Platforms e a*., delivered on 4 July 2023, the Court of Justice of the European Union stated that national competition authorities can find, in the context of the examination of an abuse of a dominant position by an undertaking, that the latter's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with the GDPR, where that finding is necessary to establish the existence of such an abuse. In absence of EU legislation concerning the issue, the Court clarified that the duty of cooperation between authorities stems directly from the duty of sincere cooperation, enshrined in Art. 4, para 3, TEU. It follows from the foregoing that administrative authorities, endowed with different tasks and pursuing different objectives, must cooperate to ensure the effective application of EU competition law and, at the same time, the coherence of EU data protection legislation. The contribution aims at highlighting the novelties introduced by the judgment, against the existing legal framework. Besides that, it purports to shed light on the way how the duty of sincere cooperation shapes the relationship between national authorities, emphasizing the central role played by national data protection supervisory authorities, charged with the control of the effective application of the GDPR. As will be explained, such a solution not only involves procedural aspects, but also has substantive implications.