Trattamento dei dati personali. La Corte di Giustizia si pronuncia sull'abuso di posizione dominante relativo al trattamento di dati personali degli utenti previsto dalle condizioni generali d'uso di un *social network online*

07/07/2023

DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, CONTENZIOSO

Marco Stillo

In data 4 luglio 2023, la Corte di Giustizia dell'Unione Europea si è pronunciata nella Causa C-252/21, *Meta Platforms e a. contro Bundeskartellamt*, sull'interpretazione dell'articolo 4, paragrafo 3, del Trattato sull'Unione Europea (TUE) nonché dell'articolo 6, paragrafo 1, dell'articolo 9, paragrafi 1 e 2, dell'articolo 51, paragrafo 1, e dell'articolo 56, paragrafo 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 (*General Data Protection Regulation*, GDPR)[1]. Tale domanda era stata presentata nell'ambito di una controversia tra, da un lato, la *Meta Platforms Inc.*, la *Meta Platforms Ireland Ltd* e la *Facebook Deutschland GmbH* (congiuntamente

[1] GUUE L 119 del 04.05.2016.

"Meta") e, dall'altro, il *Bundeskartellamt* (autorità federale tedesca garante della concorrenza) in merito alla decisione con cui quest'ultimo aveva a tali società di procedere al trattamento di taluni dati personali previsto dalle condizioni generali di utilizzo del *social network* Facebook.

Questi i fatti.

La Meta gestisce diversi servizi in linea, tra i quali Facebook, attraverso un modello economico che consiste, da un lato, nell'offrire servizi di rete sociale gratuiti per gli utenti privati e, dall'altro, nel vendere pubblicità in linea, personalizzata per il singolo utente della rete sociale e finalizzata a mostrargli i prodotti e i servizi che potrebbero interessargli in base, in particolare, al suo personale comportamento di consumo, ai suoi interessi, al suo potere d'acquisto e alle sue condizioni di vita. Al fini della raccolta e del trattamento dei dati degli utenti, la Meta si basa sul contratto di licenza d'uso concluso con i propri utenti tramite l'attivazione da parte di questi ultimi del pulsante "Iscriviti", con la quale essi accettano le condizioni d'uso di Facebook, presupposto essenziale per l'utilizzo della rete sociale[2].

Ritenendo che il trattamento dei dati costituisse uno sfruttamento abusivo della posizione dominante della Meta sul mercato delle reti sociali per gli utenti privati in Germania, il *Bundeskartellamt* aveva avviato un procedimento nei confronti di quest'ultima vietandole il trattamento stesso nonché l'attuazione delle condizioni d'uso di Facebook. Di conseguenza, la Meta aveva proposto ricorso dinnanzi all'*Oberlandesgericht Düsseldorf* (Tribunale superiore del Land di Düsseldorf; il "giudice del rinvio") che, alla luce della necessità di interpretare la normativa europea rilevante in materia, aveva deciso di sospendere il procedimento e di sottoporre alla Corte di Giustizia sette questioni pregiudiziali.

Con la prima e la settima questione, il giudice del rinvio chiedeva se gli articoli 51[3] e seguenti del GDPR debbano essere interpretati nel senso che un'autorità garante della concorrenza di uno Stato Membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 del Trattato sul Funzionamento dell'Unione Europea (TFUE), che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi al GDPR e, in caso affermativo, se l'articolo 4,

[2] L'elemento centrale della controversia riguarda la prassi consistente i) 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, ii) nel collegamento di tali dati con l'*account* Facebook dell'utente interessato, e iii) nell'utilizzo di detti dati.

[3] L'articolo 51 GDPR, intitolato "Autorità di controllo", dispone: "*... Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).*
Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII.
Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.
Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica...".

paragrafo 3[4], TUE debba essere interpretato nel senso che una simile constatazione, di natura incidentale, da parte di tale autorità è possibile anche nel caso in cui tali condizioni siano sottoposte, al contempo, ad una procedura d'esame da parte dell'autorità di controllo capofila competente ai sensi dell'articolo 56, paragrafo 1[5], del GDPR.

La Corte ha preliminarmente ricordato che le norme di cooperazione previste nel GDPR non si rivolgono alle autorità nazionali garanti della concorrenza (ANC), e bensì disciplinano la cooperazione tra le autorità nazionali di controllo interessate e la capofila nonché, se del caso, la cooperazione di tali autorità con il Comitato europeo per la protezione dei dati e la Commissione. Nè il GDPR né altri strumenti del diritto dell'Unione, infatti, stabiliscono norme specifiche sulla cooperazione tra un'ANC e le autorità nazionali di controllo interessate o la capofila. Nessuna disposizione del GDPR, inoltre, vieta alle ANC di constatare, nell'ambito dell'esercizio delle loro funzioni, la non conformità a tale regolamento di un trattamento di dati effettuato da un'impresa in posizione dominante e tale da costituire un abuso.

Le autorità di controllo e le ANC esercitano funzioni diverse e perseguono obiettivi e compiti ad esse propri. Più particolarmente, nell'adottare una decisione che constata un abuso di posizione dominante da parte di un'impresa ai sensi dell'articolo 102 TFUE, un'autorità garante della concorrenza deve valutare, sulla base di tutte le circostanze del caso di specie, se il comportamento dell'impresa in questione 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 il suo sviluppo[6]. A tale riguardo, la conformità o meno di tale comportamento alle disposizioni del GDPR può costituire, se del caso, un importante indizio fra le circostanze rilevanti del caso concreto per valutare le conseguenze di una determinata pratica sul mercato o per i consumatori. Di conseguenza, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa su un dato mercato, può risultare necessario che l'ANC dello Stato Membro interessato esamini anche la conformità del comportamento di tale impresa a norme diverse da quelle rientranti nel diritto della concorrenza, quali quelle in materia di protezione dei dati personali previste dal GDPR. Tenuto conto dei diversi obiettivi perseguiti dalle norme in materia di concorrenza, in particolare dall'articolo 102 TFUE, e da quelle previste in materia di protezione dei dati personali in forza del GDPR, pertanto, quando un'ANC rileva una violazione di quest'ultimo nell'ambito della constatazione di un abuso di posizione dominante, essa non si sostituisce alle autorità di controllo. Nello specifico, l'ANC non controlla l'applicazione né assicura il rispetto di tale regolamento per le finalità di cui all'articolo 51, paragrafo 1, di quest'ultimo, né esercita alcuno dei compiti ivi previsti o fa uso dei poteri riservati all'autorità di controllo.

Nel caso in cui ritenga necessario pronunciarsi, nell'ambito di una decisione relativa ad un abuso di posizione

[4] L'articolo 4 TUE al paragrafo 3 dispone: "*... In virtù del principio di leale cooperazione, l'Unione e gli Stati membri si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dai trattati.*
Gli Stati membri adottano ogni misura di carattere generale o particolare atta ad assicurare l'esecuzione degli obblighi derivanti dai trattati o conseguenti agli atti delle istituzioni dell'Unione.
Gli Stati membri facilitano all'Unione l'adempimento dei suoi compiti e si astengono da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione...".
[5] L'articolo 56 GDPR, intitolato "Competenza dell'autorità di controllo capofila", al paragrafo 1 dispone: "*... Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60...*".
[6] CGUE 25.03.2021, Causa C-152/19 P, *Deutsche Telekom/Commissione*, punti 41-42.

dominante, sulla conformità o meno di un trattamento di dati personali effettuato dall'impresa in questione al GDPR, tuttavia, un'ANC e l'autorità di controllo interessata o, se del caso, la capofila competente ai sensi di tale regolamento devono cooperare tra loro al fine di garantirne un'applicazione coerente. Sebbene, infatti, né il GDPR né alcun altro strumento del diritto dell'Unione prevedano norme specifiche a tal riguardo, ciò non toglie che le diverse autorità nazionali coinvolte siano tutte vincolate dal principio di leale cooperazione, in forza del quale, nelle materie rientranti nel diritto dell'Unione, gli Stati Membri devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati, adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti agli atti delle istituzioni dell'Unione nonché astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione[7]. Di conseguenza, qualora, nell'ambito dell'esame diretto a constatare un abuso di posizione dominante ai sensi dell'articolo 102 TFUE, un'ANC ritenga necessario esaminare la conformità di un comportamento dell'impresa in questione alle disposizioni del GDPR, essa deve verificare se tale comportamento, o un comportamento simile, sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o della capofila. Del pari, quando riceve una richiesta di informazioni o di cooperazione da parte di un'ANC, l'autorità di controllo deve rispondere entro un termine ragionevole, comunicandole le informazioni di cui dispone che possano consentirle di fugare i suoi dubbi o, se del caso, informandola se intende avviare il procedimento di cooperazione con le altre autorità di controllo interessate o con la capofila, al fine di giungere a una decisione volta a constatare la conformità o meno della condotta in questione al GDPR.

Tutto ciò premesso, pertanto, l'ANC non può discostarsi da una decisione dell'autorità nazionale di controllo o della capofila competente riguardante le condizioni generali d'uso di un'impresa relative al trattamento dei dati personali o condizioni generali analoghe. Laddove nutra dubbi sulla portata di tale decisione, o laddove tali condizioni siano, al contempo, oggetto di esame da parte di tali autorità o, ancora, laddove, in assenza di una loro indagine o decisione, ritenga che le condizioni in questione non siano conformi al GDPR, l'ANC deve consultare tali autorità e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una loro decisione prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, invece, l'ANC può proseguire la propria indagine.

Con la seconda questione, lettera a), il giudice del rinvio chiedeva se l'articolo 9, paragrafo 1[8], del GDPR debba essere interpretato nel senso che, nel caso in cui un utente di un *social network online* consulti siti *internet* o applicazioni attinenti ad una o più delle categorie indicate in tale disposizione e, se del caso, vi inserisca dati iscrivendosi o effettuando ordini *online*, il trattamento di dati personali da parte dell'operatore di tale *social network*, consistente nel raccogliere, tramite interfacce integrate, *cookie* o simili tecnologie di registrazione, i dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché i dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del *social network* di quest'ultimo e nell'utilizzare detti dati, deve essere

[7] CGUE 01.09.2022, Cause riunite C-14/21 e C-15/21, *Sea Watch*, punto 156; CGUE 07.11.2013, Causa C-518/11, *UPC Nederland*, punto 59.

[8] L'articolo 9 GDPR, intitolato "Trattamento di categorie particolari di dati personali", al paragrafo 1 dispone: "*... È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona...*".

considerato un “trattamento di categorie particolari di dati personali” ai sensi di detta disposizione, il quale è vietato in linea di principio, fatte salve le deroghe previste dal paragrafo 2 di tale articolo 9.

Nel caso concreto, il trattamento effettuato dalla consiste i) nel raccogliere dati personali degli utenti di Facebook quando essi consultano siti *internet* o applicazioni, ivi inclusi quelli che possano rivelare informazioni rientranti in una o più delle categorie di cui all’articolo 9, paragrafo 1, del GDPR, e, se del caso, vi inseriscono informazioni iscrivendosi o effettuando ordini *online*, ii) nel mettere in relazione tali dati con l’*account* del *social network* di tali utenti, e iii) nell’utilizzare tali dati. Secondo la Corte, pertanto, spetta al giudice del rinvio stabilire se i dati in tal modo raccolti, di per sé oppure mediante la loro messa in relazione con gli *account* Facebook degli utenti interessati, consentano effettivamente di rivelare informazioni di questo tipo, a prescindere dal fatto che esse riguardino un utente di tale *social network* oppure qualsiasi altra persona fisica. Fatte salve le verifiche che tale giudice è tenuto ad effettuare, tuttavia, pare che il trattamento dei dati relativi alla consultazione dei siti *internet* o delle applicazioni in questione possa, in determinati casi, rivelare tali informazioni, senza che sia necessario che gli utenti si iscrivano o effettuino ordini *online*.

Con la seconda questione, lettera b), invece, il giudice del rinvio chiedeva se l’articolo 9, paragrafo 2, lettera e)[9], del GDPR debba essere interpretato nel senso che, qualora un utente di un *social network online* consulti siti *internet* o applicazioni collegate alle categorie indicate all’articolo 9, paragrafo 1, del GDPR, inserisca dati su tali siti o applicazioni, o attivi pulsanti di selezione integrati in questi ultimi, quali i pulsanti “Mi piace” o “Condividi” o quelli che consentono all’utente di identificarsi su tali siti o tali applicazioni utilizzando gli identificativi di connessione legati al suo account di utente del *social network online*, il suo numero di telefono o il suo indirizzo di posta elettronica, si ritiene che egli abbia manifestamente reso pubblici i dati raccolti in tale occasione dall’operatore di tale *social network* mediante *cookie* o simili tecnologie di registrazione.

Prevedendo un’eccezione al principio del divieto di trattamento di categorie particolari di dati personali, l’articolo 9, paragrafo 2, del GDPR deve essere interpretato restrittivamente[10], di talché è necessario verificare se l’interessato abbia inteso, in modo esplicito e con un atto positivo chiaro, rendere accessibili al pubblico i dati personali in questione. A tale riguardo, con la consultazione di siti *internet* o di applicazioni correlati ad una o più delle categorie di cui all’articolo 9, paragrafo 1, del GDPR, l’utente interessato non intende in alcun modo rendere pubblico il fatto di aver consultato tali siti o tali applicazioni e i dati relativi che possono essere ricollegati alla sua persona. Tale utente, infatti, può tutt’al più attendersi che il gestore del sito o dell’applicazione abbia accesso a tali dati e che li condivida, se del caso e fermo restando il suo consenso esplicito, con taluni terzi e non con il pubblico. Di conseguenza, dalla mera consultazione di tali siti *internet* o applicazioni da parte di un utente non si può dedurre che tali dati personali siano stati da lui manifestamente resi pubblici ai sensi dell’articolo 9, paragrafo 2, lettera e), del GDPR.

Le attività consistenti nell’inserire dati in tali siti *internet* o applicazioni nonché nell’attivare i pulsanti di selezione in essi integrati o quelli che consentono all’utente di identificarsi utilizzando gli identificativi di connessione collegati al suo account utente Facebook, il suo numero di telefono o il suo indirizzo di

[9] L’articolo 9 GDPR al paragrafo 2 lettera e) dispone: “*… Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:*
(...)
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato...”.
[10] CGUE 06.06.2019, Causa C-361/18, *Weil*, punto 43; CGUE 17.09.2014, Causa C-3/13, *Baltic Agro*, punto 24.

posta elettronica, invece, comportano un'interazione fra tale utente e il sito *internet* o l'applicazione in questione e, se del caso, quello del *social network online*, le cui forme di pubblicità possono variare in quanto possono essere oggetto di una impostazione individuale di parametri da parte dell'utente. Di conseguenza, qualora abbiano la possibilità di decidere, sulla base di un'impostazione di parametri effettuata con piena cognizione di causa, di rendere i dati inseriti nei siti *internet* o nelle applicazioni in questione, nonché quelli risultanti dall'attivazione dei pulsanti di selezione in essi integrati, accessibili ad un numero illimitato di persone, gli utenti interessati rendono manifestamente pubblici i dati che li riguardano ai sensi dell'articolo 9, paragrafo 2, lettera e), del GDPR. Per contro, nel caso in cui non venga proposta un'impostazione individuale di parametri di questo tipo, per poter ritenere che gli utenti abbiano manifestamente reso pubblici dati allorché li inseriscono volontariamente in un sito *internet* oppure in un'applicazione o attivano pulsanti di selezione in questi ultimi essi devono aver esplicitamente acconsentito, sulla base di un'informazione espressa fornita dal sito o dall'applicazione prima di tale inserimento o attivazione, a che i suddetti dati possano essere visualizzati da chiunque vi abbia accesso.

Con la terza e la quarta questione, il giudice del rinvio chiedeva se, e a quali condizioni, l'articolo 6, paragrafo 1, primo comma, lettere b) e f)[11], del GDPR debba essere interpretato nel senso che il trattamento di dati personali effettuato da un operatore di un *social network online* consistente nel raccogliere dati dei relativi utenti provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte degli utenti in questione, di siti *internet* o di applicazioni di terzi, nel mettere in relazione tali dati con l'*account* del *social network* di questi ultimi e nell'utilizzare tali dati può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti, ai sensi della lettera b), oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi della lettera f).

La Corte ha preliminarmente ricordato che se il contratto in questione consiste in più servizi o in più elementi distinti di uno stesso servizio che possono essere prestati indipendentemente gli uni dagli altri, l'applicabilità dell'articolo 6, paragrafo 1, primo comma, lettera b), del GDPR deve essere valutata separatamente nel contesto di ciascuno di tali servizi. Nel caso concreto, sebbene sia utile per l'utente, in quanto gli consente in particolare di visualizzare un contenuto in larga misura corrispondente ai suoi interessi, la personalizzazione dei contenuti non appare necessaria per offrirgli i servizi del *social network online*, che possono eventualmente essergli forniti sotto forma

[11] L'articolo 6 GDPR, intitolato "Liceità del trattamento", al paragrafo 1 dispone: "*... Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:*
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti...".

di un'alternativa equivalente che non implichi tale personalizzazione, che non è dunque oggettivamente indispensabile per una finalità che faccia parte integrante degli stessi. Una persona, inoltre, non è tenuta a sottoscrivere i diversi servizi proposti dalla Meta per poter creare un *account* utente su Facebook, in quanto i diversi prodotti e servizi proposti possono essere utilizzati indipendentemente gli uni dagli altri, e l'utilizzo di ciascuno di essi si basa sulla sottoscrizione di un contratto d'uso distinto. Di conseguenza, un trattamento di dati personali provenienti da servizi diversi da quello del *social network online*, proposti dalla Meta, non sembra essere necessario per consentire la fornitura di quest'ultimo servizio.

Per quanto riguarda, invece, l'articolo 6, paragrafo 1, primo comma, lettera f), del GDPR, tale disposizione prevede tre condizioni cumulative affinché i trattamenti di dati personali da essa considerati siano leciti, ossia i) il perseguimento di un legittimo interesse del titolare del trattamento o di terzi, ii) la necessità del trattamento dei dati personali per la realizzazione del legittimo interesse perseguito, e iii) il fatto che gli interessi o i diritti e le libertà fondamentali dell'interessato dalla tutela dei dati non prevalgano sul legittimo interesse del responsabile del trattamento o di terzi[12]. Nello specifico, spetta al titolare del trattamento, all'atto della raccolta presso l'interessato di dati che lo riguardano, indicargli i legittimi interessi perseguiti, qualora tale trattamento si basi sull'articolo 6, paragrafo 1, primo comma, lettera f), del GDPR[13]. La condizione relativa alla necessità del trattamento dei dati personali per la realizzazione del legittimo interesse perseguito, inoltre, impone al giudice del rinvio di verificare che quest'ultimo non possa ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per quelli al rispetto della vita privata e alla protezione dei dati personali[14]. Il fatto che gli interessi o i diritti e le libertà fondamentali dell'interessato non debbano prevalere sul legittimo interesse del responsabile del trattamento o di terzi, infine, implica una ponderazione dei diritti e degli interessi contrapposti che dipende, in linea di principio, dalle circostanze del caso concreto e che, di conseguenza, spetta al giudice del rinvio effettuare[15].

Nel caso concreto, malgrado la gratuità dei servizi di un *social network online* come Facebook, l'utente di quest'ultimo non può ragionevolmente attendersi che, senza il suo consenso, il relativo operatore tratti i suoi dati personali a fini di personalizzazione della pubblicità. In tali circostanze, pertanto, i diritti fondamentali e gli interessi dell'utente prevalgono su quello dell'operatore a tale personalizzazione, mediante la quale egli finanzia la sua attività, di talché il trattamento da quest'ultimo effettuato a tali fini non può rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del GDPR. Il trattamento in questione, inoltre, è particolarmente esteso, in quanto verte su dati potenzialmente illimitati ed ha un notevole impatto sull'utente, di cui la Meta controlla gran parte, se non la quasi totalità, delle attività *online*, ciò che può suscitare in quest'ultimo la sensazione di una continua sorveglianza della sua vita privata. In merito alla necessità di questo trattamento per la realizzazione del legittimo interesse a

[12] CGUE 17.06.2021, Causa C-597/19, *M.I.C.M.*, punto 106.
[13] L'articolo 13 del GDPR, intitolato "Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato", al paragrafo 1 lettera d) dispone: "*... In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:*
(...)
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi...".
[14] CGUE 22.06.2021, Causa C-439/19, *Latvijas Republikas Saeima (Punti di penalità)*, punto 110.
[15] CGUE 17.06.2021, Causa C-597/19, *M.I.C.M.*, punto 111.

garantire la sicurezza del *network*, infine, il giudice del rinvio dovrà verificare se e in quale misura il trattamento di dati personali raccolti a partire da fonti esterne a Facebook risulti effettivamente necessario per garantire che non sia compromessa la sicurezza interna di tale *network*.

Con la quinta questione, il giudice del rinvio chiedeva se l'articolo 6, paragrafo 1, primo comma, lettere da c) a e), del GDPR debba essere interpretato nel senso che un simile trattamento di dati personali può essere considerato necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, ai sensi della lettera c), per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, ai sensi della lettera d), o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ai sensi della lettera e), qualora il trattamento sia effettuato, rispettivamente, per rispondere a una legittima richiesta di determinati dati, per contrastare comportamenti dannosi e promuovere la sicurezza e per ricerche a beneficio della società e per promuovere protezione, integrità e sicurezza.

Per quanto riguarda le ipotesi di liceità del trattamento di cui all'articolo 6, paragrafo 1, primo comma, lettere c) ed e), del GDPR, il giudice del rinvio non ha fornito alla Corte elementi che le consentano di pronunciarsi concretamente al riguardo, di talché egli sarà tenuto a verificare se il trattamento in questione possa essere considerato giustificato dalle finalità addotte. Più particolarmente, il giudice del rinvio dovrà verificare se la Meta, da un lato, sia soggetta ad un obbligo legale di raccolta e di conservazione di dati personali in modo preventivo al fine di poter rispondere a qualsiasi richiesta di un'autorità nazionale diretta ad ottenere taluni dati relativi ai suoi utenti e se, dall'altro, sia investita di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, in particolare al fine di assicurare ricerche a beneficio della società nonché di promuovere protezione, integrità e sicurezza, restando inteso che, data la natura e il carattere essenzialmente economico e commerciale della sua attività, appare poco probabile che tale operatore privato sia investito di un simile compito. Per quanto riguarda, invece, l'ipotesi di liceità del trattamento di cui all'articolo 6, paragrafo 1, primo comma, lettera d), del GDPR, secondo la Corte l'operatore di un *social network online*, la cui attività riveste un carattere essenzialmente economico e commerciale, non può addurre la protezione di un interesse essenziale alla vita dei suoi utenti o di un'altra persona per giustificare, in assoluto e in modo puramente astratto e preventivo, la liceità di un trattamento di dati come quello del caso concreto.

Di conseguenza, il trattamento di dati personali effettuato da un operatore di un *social network online* consistente nel raccogliere dati dei relativi utenti provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte degli utenti in questione, di siti *internet* o di applicazioni di terzi, nel mettere in relazione tali dati con l'*account* del *social network* di questi ultimi e nell'utilizzare tali dati non può essere considerato necessario alla salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica né all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Con la sesta questione, infine, il giudice del rinvio chiedeva se l'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a)[16], del GDPR debbano essere interpretati nel senso che si può ritenere che un

[16] L'articolo 9 GDPR al paragrafo 2 lettera a) dispone: "*… Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:*
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1...".

consenso prestato dall'utente di un *social network online* al suo operatore soddisfi le condizioni di validità previste all'articolo 4, punto 11[17], di tale regolamento, in particolare quella secondo cui tale consenso deve essere prestato liberamente, qualora tale operatore occupi una posizione dominante sul mercato dei *social network online*.

La circostanza che l'operatore di un *social network online*, in quanto titolare del trattamento, occupi una posizione dominante sul mercato dei *social network* non osta, di per sé, a che i relativi utenti possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, del GDPR, al trattamento dei loro dati personali effettuato da tale operatore. Una circostanza del genere deve, tuttavia, essere presa in considerazione nella valutazione della validità e, in particolare, della libertà del consenso prestato dall'utente di tale *social network*, in quanto essa può incidere sulla sua libertà di scelta, potendo egli non essere in grado di rifiutare o di revocare il suo consenso senza subire pregiudizio. L'esistenza di una posizione dominante, inoltre, è tale da creare uno squilibrio evidente tra l'interessato e il titolare del trattamento, che favorisce l'imposizione di condizioni non strettamente necessarie all'esecuzione del contratto, ciò che deve essere del pari preso in considerazione.

Nel caso concreto, poiché non risulta che il trattamento in questione sia strettamente necessario all'esecuzione del contratto tra la Meta e gli utenti di Facebook, questi ultimi devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dall'operatore del *social network online*, dovendo pertanto esser loro proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati. Tenuto conto della portata del trattamento dei dati in questione e del suo notevole impatto sugli utenti di tale *network*, nonché della circostanza che essi non possono ragionevolmente attendersi che dati diversi da quelli relativi al loro comportamento all'interno del *social network* siano trattati dall'operatore di quest'ultimo, inoltre, è opportuno che possa essere prestato un consenso separato per il trattamento di questi ultimi dati, da un lato, e dei dati *off* Facebook, dall'altro.

[17] L'articolo 4 GDPR, intitolato "Definizioni", al paragrafo 11 dispone: "*... Ai fini del presente regolamento s'intende per:*
(...)
11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento...".

Marco Stillo

ASSOCIATE

m.stillo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Sadovaya-Chernogryazskaya 8, build. 8 · 107078, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com