# La Grande Sezione interviene sul principio di leale cooperazione tra autorità garanti e sul principio di liceità dei trattamenti di dati personali attuato da Facebook

*di Gianluca Bellomo*

**Title:** The Grand Chamber intervenes on the principle of sincere cooperation between Authorities and lawfulness of processing of personal data implemented by Facebook.

**Keywords:** Regulation (EU) 2016/679; Principle of sincere cooperation; Lawfulness of processing.

1. – Il tema della tutela dei dati personali sempre più si impone nella vita di tutti i giorni e sempre più la società civile si dimostra sensibile ai rischi per possibili lesioni di diritti collegati al trattamento di tali dati, che attengono alle presone fisiche, e che proprio ai diritti e alle libertà personali di queste possono arrecare pregiudizio in caso di trattamenti inadeguati.



Il Regolamento (UE) 2016/679, *Regolamento Generale sulla Protezione dei Dati personali* (in prosieguo RGPD), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, pienamente entrato in vigore il 25 maggio 2018 (su cui cfr., tra gli altri, almeno R. D'orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Milano; ma anche G. Finocchiaro, *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; L. Bolognino, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, t. II, 2016; G.M. Riccio, G. Scorza, E. Belisario, (cur.), *GDPR e normativa Privacy. Commentario*, II ed., Milano, 2022), ha decisamente innalzato e standardizzato a livello eurounitario le tutele ordinamentali per le persone fisiche alle quali si riferiscono i dati (c.d. interessati al trattamento) e, per converso, ha fissato importanti principi e paletti nelle azioni che si possono porre in essere sui dati personali da parte di soggetti pubblici e privati. Tra questi gli operatori di piattaforme informatiche, e dei *social network* in particolare, sono tra i principali soggetti destinatari, da parte del regolatore europeo, della normativa in materia e dei connessi limiti da rispettare nel trattamento quotidiano di una mole enorme di dati personali riferiti ai propri utenti. Tali tipologie di trattamento di detti dati, di fatto, per lungo tempo è stata sostanzialmente lasciata alle libere scelte degli operatori economici che, attraverso sofisticati algoritmi di profilazione dei propri utenti, hanno potuto porre in essere modelli economici con profitti enormi in sostanziale assenza di ogni forma di regolamentazione, almeno con riguardo al trattamento dei dati personali. Proprio

tra le tutele previste dal RGPD, tra le pietre angolari della normativa, oltre ai principi sanciti all'articolo 5 (su cui cfr. almeno C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 21 novembre 2018) da dover rispettare nel trattamento dei dati, si possono rivenire le c.d. *basi giuridiche del trattamento*, rinvenibili agli artt. 6 e 9 del Regolamento (sulle quali sia consentito rinviare, con specifico riferimento ai partiti politici a G. Bellomo, *Metodo democratico, partiti politici, nuove tecnologie e basi giuridiche per il trattamento dei dati personali: alcuni spunti di riflessione*, in questa *Rivista*, n. 1/2021). Infatti l'impostazione scelta dal legislatore europeo prende le mosse dal principio di divieto generalizzato del trattamento di dati personali, salvo l'esistenza di una norma che consenta di superare tale divieto. Così ogni trattamento, per poter essere posto in essere da parte di soggetti terzi rispetto alla persona fisica alla quale si riferiscono (c.d. *interessato* dal trattamento), deve preliminarmente e necessariamente fondarsi su una delle basi giuridiche di liceità elencate dal RGPD, a seconda della tipologia di dato coinvolto nel trattamento. Per i *dati personali comuni*, quindi, le basi giuridiche sono elencate appunto all'art. 6 e per le *particolari categorie di dati personali* (una volta individuati come c.d. *dati sensibili* dalla normativa), e cioè quei dati che potenzialmente presentano maggiori livelli di rischiosità per i diritti e le libertà fondamentali dei soggetti ai quali si riferiscono ove non trattati correttamente (es. dati sanitari, orientamento religioso, politico, sessuale, dati genetici, dati biometrici ecc). Le basi giuridiche per il trattamento di quest'ultima categoria di dati sono rinvenibili invece all'art. 9 del RGPD.

Proprio sulle basi giuridiche di liceità dei trattamenti di dati personali e sull'interpretazione di queste date dai soggetti che sono chiamati a farlo, e tra questi *in primis* troviamo proprio le autorità di controllo dei differenti Paesi membri, si gioca la legittimità o meno dei trattamenti posti in essere in UE e i possibili effetti distorsivi che si possono avere del Mercato unico.



La sentenza qui in commento, che ha richiesto l'intervento della Grande Sezione della Corte di Giustizia, si concentra sostanzialmente su due temi differenti, ma entrambi rilevanti: il primo, attinente al rapporto tra autorità garanti con differenti competenze, e ai limiti di intervento di queste in ambiti non direttamente rientranti nei compiti loro affidati dal legislatore nazionale; il secondo, invece, relativo alla corretta interpretazione e applicazione delle c.d. basi giuridiche del trattamento e all'uso improprio che possa essere fatto da un operatore privato per fondare il trattamento dei dati all'interno di un *social network* quale Meta Platform Inc. (più comunemente noto come Facebook).

2. – La questione pregiudiziale, che ha condotto alla pronuncia la Grande Sezione della Corte di Lussemburgo sulle tematiche sopra accennate, nasce tra la Meta Platforms Inc (già Facebook Inc), Meta Platforms Ireland Ltd (già Facebook Ireland Ltd) e Facebook Deutschland GmbH, gestori della nota piattaforma *social* a differenti livelli territoriali, contro la decisione emessa dal *Bundeskartellamt* (autorità federale garante della concorrenza, Germania) di vietare a tali società di procedere al trattamento di taluni dati personali dei propri utenti privati così come previsto nelle condizioni generali di utilizzo del *social network*.

Proprio l'Autorità federale garante della concorrenza tedesca, infatti, con decisione del 6 febbraio 2019 vietava a Meta Platforms Inc, Meta Platforms Ireland Ltd e Facebook Deutschland GmbH, in base alla normativa tedesca (art. 19, par. 1 e art. 32 del *Gesetz gegen Wettbewerbsbeschränkungen* - legge contro le restrizioni della concorrenza), di subordinare, così come previsto nelle condizioni generali d'uso, la fruizione del *Social network* da parte degli utenti privati residenti in Germania all'accettazione, da parte di questi ultimi, al trattamento dei dati

*DPCE online*
ISSN: 2037-6677

personali raccolti al di fuori di Facebook (c.d. dati «*off* Facebook») senza il consenso dei singoli utenti. Ciò sia con riferimento ai dati personali provenienti da soggetti terzi, ma comunque riferibili al singolo utente; sia a quelli, comunque esterni al *Social network*, raccolti da altre società del gruppo Meta (quali ad es. Instagram, WhatsApp, Oculus e fino al 13 marzo 2020 Masquerade). In tale provvedimento il Garante della concorrenza tedesco ordinava alle società gestrici del *Social network* di adeguare le condizioni generali così che da queste risultasse chiaramente che tali dati non sarebbero stati né raccolti, né messi in relazione con gli *account* dei singoli utenti del *Social network*, né utilizzati senza il consenso dell'utente interessato. Ed inoltre ha chiarito che tale consenso non è valido qualora costituisca una condizione per l'utilizzo del *Social network*.

La motivazione alla base del provvedimento era che, per l'autorità emanante, proprio il trattamento dei dati personali degli utenti del *Social network*, così come previsto nelle condizioni generali e attuato da Meta Platforms Ireland, rappresentava uno sfruttamento abusivo di una posizione dominante della Società nel panorama dei *social network online* per gli utenti privati tedeschi secondo la citata normativa nazionale. Più esattamente i profili di illiceità erano riconducibili al fatto che il trattamento dei dati c.d. «*off* Facebook» previsto nelle condizioni generali sarebbe stato lesivo dei principi del RGPD ed in particolare degli artt. 6 e 9 del Regolamento relativi alle basi giuridiche del trattamento dei dati personali degli utenti.

La Meta Platforms, la Meta Platforms Ireland e Facebook Deutschland l'11 febbraio 2019 presentavano un ricorso avverso la decisione dell'Autorità federale garante della concorrenza dinanzi all'*Oberlandesgericht Düsseldorf* (Tribunale superiore del Land, Düsseldorf, Germania).

Successivamente, il 31 luglio 2019, la Meta Platforms Ireland ha sia introdotto nuove condizioni generali, nelle quali è stato espressamente previsto che il singolo utente, invece di pagare per l'uso dei prodotti Facebook, dichiara di acconsentire alle inserzioni pubblicitarie; sia, a partire dal 28 gennaio 2020, la Meta Platforms offre in tutto il mondo, l'«*Off-Facebook-Activity*», che dà la possibilità agli utenti del *Social network* di avere contezza, attraverso la visualizzazione di un riepilogo delle informazioni che li riguardano, dei dati personali che le società del gruppo Meta ottengono in relazione alle loro attività su altri siti Internet e applicazioni, e di scollegare, se i singoli utenti lo desiderano, tali dati dal loro *account* Facebook.com sia per il passato che per il futuro.



Proprio nell'analisi del ricorso presentato il Giudice amministrativo tedesco, investito dalla richiesta, pone ben sette questioni pregiudiziali alla Corte, alcune delle quali contenenti ulteriori sub-questioni.

Più dettagliatamente viene sostanzialmente chiesto al giudice di Lussemburgo:

1) Con la prima e la settima questione se nell'ambito dell'esercizio di un controllo posto in essere da una autorità nazionale in materia di abusi di posizione dominante, ai sensi del diritto della concorrenza, secondo quanto previsto dagli artt. 51 e seguenti del RGPD, questa possa rilevare, in modo incidentale, che le condizioni contrattuali operate dalla filiale principale di una impresa violano il trattamento dei dati personali, secondo quanto previsto da detta normativa e la sua applicazione, e ne possa disporre l'interruzione. Inoltre, ove ciò sia possibile, se tale attività sia compatibile con il principio di «leale cooperazione» sancito dall'art. 4, par. 3 del TUE, nel caso in cui contemporaneamente a tale attività dell'autorità per la concorrenza tedesca, l'autorità di controllo capofila dello Stato membro nel quale si trova la filiale principale (Irlanda in questo caso) sottoponga ad un procedimento di indagine le condizioni contrattuali relative al trattamento dei dati personali operate da quest'ultima *ex* art. 56, par. 1 del RGPD.

2) Ove la risposta della Corte alla prima questione fosse affermativa si chiede, inoltre, sia se il fatto di collegare ai dati dell'account Facebook.com dell'utente dati c.d. «*off* Facebook» classificabili, ai sensi dell'art. 9 del RGPD, come *particolari categorie di dati* (quali ad es. l'orientamento sessuale, politico, religioso o i dati sanitari), o il fatto che la società che gestisce il *Social* li utilizzi, raccolga e/o lo stesso fatto di collegarli configurino o meno un trattamento di dati "sensibili" ai sensi di detto articolo; sia, in caso di risposta affermativa, se, ai sensi dell'art. 9, par. 2, lett. e) del RGPD, il fatto che il singolo utente ponga in essere una serie di azioni (es. accesso a siti e app di terzi, l'inserimento di dati e/o l'attivazione di pulsanti - quali ad es. "Mi piace" o "Condividi", ecc -) rappresentino una possibile modalità di rendere tali categorie di dati manifestamente pubblici.

3) Con la terza questione si chiede se le basi giuridiche rappresentate dall'art. 6, par. 1 lett. b) ed f), con riferimento a normali categorie di dati personali, e cioè rispettivamente la necessità del trattamento di detti dati per *l'esecuzione di un contratto* o per *la tutela di legittimi interessi* del titolare, sia idonea ai fini del trattamento di dati raccolti e utilizzati attraverso un collegamento all'account Facebook.com di dati c.d. «*off* Facebook».

4) Con riferimento alla possibilità di trattare tali dati c.d. «*off* Facebook» collegandoli all'account Facebook.com dell'utente e di utilizzarli fondandosi ai fini di tali trattamenti sulla base giuridica del legittimo interesse, *ex* art. 6, par.1, lett. f), se tale base possa essere utilizzata correttamente considerando legittimi interessi del titolare anche una serie di casi quali: « – la minore età dell'utente, ai fini della personalizzazione dei contenuti e della pubblicità, del miglioramento dei prodotti, della sicurezza del network e delle comunicazioni non commerciali destinate all'utente, – la fornitura di misurazioni, dati statistici e altri servizi per le aziende a inserzionisti, sviluppatori e altri partner, affinché questi possano valutare e migliorare le proprie prestazioni, – l'offerta di comunicazioni di marketing destinate all'utente affinché l'impresa possa migliorare i suoi prodotti e condurre marketing diretto, – ricerca e innovazione per il bene della società per far progredire lo stato dell'arte o la comprensione scientifica relativamente a importanti temi sociali e per avere un impatto positivo sulla società e sul mondo, – informazioni alle autorità preposte all'applicazione e all'esecuzione della legge e la risposta a richieste legali, al fine di prevenire, di individuare e di perseguire illeciti penali, usi non autorizzati, violazioni delle condizioni d'uso e delle regole aziendali ed altri comportamenti dannosi».



5) Con la quinta questione il Giudice tedesco specifica ulteriormente, chiedendo se il trattamento sempre dei c.d. dati «*off* Facebook», nelle modalità già descritte, possa fondarsi anche sulle basi giuridiche previste nel medesimo art. 6, par. 1 del RGPD, ma questa volta alle lettere c), d) ed e) rispettivamente, ad esempio «per rispondere ad una legittima richiesta di dati specifici [lettera c)], per contrastare comportamenti dannosi e promuovere la sicurezza [lettera d)], per ricerche a beneficio della società e per promuovere protezione, integrità e sicurezza [lettera e)]».

6) Infine con la sesta ed ultima questione si chiede, invece, se sia possibile ritenere validamente espresso il consenso fornito dagli utenti di Facebook sulla base degli artt. 6, par. 1, lettera a), e 9, par. 2, lettera a), ed in particolare se tale consenso possa essere ritenuto liberamente fornito ai sensi dell'art. 4, punto 11 del RGPD che prevede appunto i caratteri del consenso affinché sia tale.

3. – La prima e la settima questione poste dal giudice amministrativo tedesco attengono al rapporto tra autorità garanti dei Paesi membri, operanti in ambiti differenti, e agli obblighi di leale cooperazione ai quali le autorità nazionali dei

*DPCE online*
ISSN: 2037-6677

Paesi membri devono sottostare. Più in dettaglio il giudice del rinvio si chiede se nel caso di specie l'autorità garante per la concorrenza tedesco nel corso dello svolgimento delle sue funzioni proprie (accertamento di un abuso di posizione dominante) fosse legittimata a rilevare la violazione di norme relative al corretto trattamento di dati personali, materia di competenza delle autorità garanti per la tutela dei dati personali dei differenti Paesi membri coinvolti; e se tali rilevazioni fossero possibili anche se contemporaneamente tali comportamenti in violazione del RGPD fossero oggetto di valutazione anche da parte di un'autorità di controllo capofila nell'ambito di quanto previsto dall'art. 56, par. 1 del RGPD.

La questione viene affrontata dalla Corte rilevando preliminarmente che se da una parte il RGPD all'art. 55, paragrafo 1, stabilisce il potere posto dalla norma in capo ad ogni autorità di controllo di esercitare i poteri di vigilanza affidati all'interno del territorio nazionale di competenza (sentenza del 15 giugno 2021, *Facebook Ireland* e *a.*, C-645/19, EU:C:2021:483, punto 47 e giurisprudenza ivi citata), anche cooperando tra di loro, d'altra parte tali norme si rivolgono esclusivamente alle autorità di controllo affidatarie della tutela dei dati personali e non a tutte le autorità garanti indistintamente. Né tanto meno il RGPD o altri strumenti dell'Unione prevedono norme specifiche di cooperazione tra autorità garante per la concorrenza e autorità nazionali di controllo per la corretta applicazione del Regolamento; né, d'altra parte però va notato, esistono norme che vietano ad una autorità garante per la concorrenza di rilevare, nell'ambito dell'esercizio delle proprie funzioni ovviamente, la mancata conformità di un trattamento di dati personali effettuato da una impresa che potrebbe star abusando della propria posizione dominante (punto 43 della Sentenza).

A riguardo va notato peraltro, a parere di chi scrive, che alla luce del fatto che le autorità garanti sono esse stesse dei pubblici poteri, che peraltro nel caso delle autorità di controllo preposte alla tutela dei dati personali sono le uniche autorità che trovano legittimazione direttamente nei trattati (*ex* art. 8, terzo comma, della Carte dei diritti fondamentali dell'Unione europea) assumendo una rilevanza, almeno materialmente, costituzionale, e chi opera per loro conto nell'esercizio dell'attività istituzionale assume la veste di pubblico ufficiale, sarebbe difficile per questi nell'esercizio delle legittime funzioni proprie l'omissione di un intervento che sia volto all'interruzione di una eventuale violazione in corso. Altra cosa sarebbe, invece, se l'autorità garante per la concorrenza iniziasse a porre in essere interventi in una materia non di sua competenza, quale la tutela dei dati personali, pertanto in assenza di alcuna connessione con le funzioni che le sono proprie. In quest'ultima eventualità, infatti, vi sarebbe una palese ed ingiustificata invasione delle competenze affidate dall'ordinamento ad altre autorità. Nel caso di specie, però, la connessione tra la violazione delle norme in materia di tutela dei dati personali, rilevata nelle norme generali stabilite da Facebook, ben può rappresentare un importante indizio di un comportamento spregiudicato posto in essere da parte dell'azienda, con conseguenze distorsive sul mercato e sui consumatori (punto 47 della Sentenza).

La Corte, così, afferma che se è vero che un'autorità per la concorrenza di un Paese membro nell'esercizio delle proprie funzioni può rilevare la violazione, anche in via incidentale, di norme che non rientrerebbero sotto la propria competenza, ma ciò solo in quanto la norma coinvolta sia in stretta connessione con lo svolgimento delle proprie funzioni, è altrettanto vero che questa non si sostituisce alle autorità specificamente preposte a tale funzione. Tuttavia, va notato, che in capo a tutte le autorità resta l'obbligo, *ex* art. 4, paragrafo 3 del TUE, di leale cooperazione tra di loro per la coerente applicazione del Regolamento, che persegua il raggiungimento degli obiettivi dello stesso e preservi il loro effetto utile (punti 52-54). Da ciò consegue che detta autorità garante per la concorrenza, se è vero che può verificare, all'interno dei limiti

indicati, anche il rispetto del RGPD, è però altrettanto vero che prima di esprimersi a riguardo dovrà verificare se «tale comportamento o un comportamento simile sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila o, ancora, della Corte. Se così fosse, l'autorità nazionale garante della concorrenza non potrebbe discostarsene, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza» (punto 56 della Sentenza). Inoltre in caso di dubbi da parte dell'autorità garante per la concorrenza se vi siano già in corso interventi da parte di autorità di controllo nazionali o da parte di autorità di controllo capofila di altri Paesi membri o altri dubbi interpretativi nella materia non di sua stretta competenza, vi sarà un obbligo di consultazione di dette autorità prima di ogni eventuale constatazione di conformità o di difformità circa l'applicazione del RGPD. Tale azione potrà proseguire comunque anche in presenza o di una mancata risposta in tempi ragionevoli alle richieste di delucidazioni da parte dell'autorità garante per la concorrenza, o di una mancata opposizione alla prosecuzione delle indagini anche in assenza di adozione di decisioni ufficiali da parte loro.

Nel caso di specie la Corte rileva che l'autorità garante per la concorrenza ha provveduto nei mesi di ottobre e novembre 2018, attraverso una serie di comunicazioni indirizzate agli organi competenti nazionali a coinvolgere le altre autorità competenti per materia, assolvendo così di fatto ai citati obblighi di leale cooperazione imposti dal TUE.

La Corte, pertanto, ribadisce che l'autorità garante per la concorrenza tedesco, proprio in base a tale obbligo di leale cooperazione, non può discostarsi da una decisione dell'autorità nazionale di controllo o da un'autorità capofila competente con riguardo alle condizioni generali previste da Facebook. Nel caso in cui dovesse però nutrire dubbi sulla portata di tale decisione, allorché tali condizioni siano contemporaneamente oggetto di esame da parte di dette autorità, o, ancora, se ritenga che le condizioni in questione non siano conformi al RGPD, «l'autorità nazionale garante della concorrenza deve consultare dette autorità di controllo e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte di tali autorità prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine» (punto 63 della Sentenza).



Così la Corte se da una parte non vieta l'intervento da parte di autorità indipendenti in settori non strettamente di propria competenza, nell'esercizio delle funzioni che sono loro proprie, dall'altra fissa dei paletti reciproci all'azione di tali pubblici poteri e alla leale collaborazione che deve esserci tra questi così da ridurre gli ampi margini di discrezionalità in capo a tali autorità nell'esercizio delle loro funzioni nei Paesi membri.

4. – Una volta chiariti dalla Corte gli aspetti relativi ai limiti reciproci nei rapporti tra autorità garanti, questa passa ad analizzare le questioni più prettamente attinenti alle basi giuridiche del trattamento dei dati personali.

Più in dettaglio, per quanto attiene alla seconda questione, il giudice del rinvio chiede alla Corte se il porre in essere una serie di comportamenti da parte di un utente di un *social network online* che comporti, ad esempio, il consultare siti internet, o usare applicazioni attinenti a particolari categorie di dati, anche con ulteriori azioni quali inserire dati, iscriversi o effettuare ordini online, e il conseguente trattamento dei dati risultanti dalla consultazione di tali siti o di tali applicazioni, nonché il mettere in relazione detti dati con l'account dell'utente del *social network* e nell'utilizzarli, debba essere considerato esso stesso un trattamento

*DPCE online*
ISSN: 2037-6677

rientrante in un «trattamento di categorie particolari di dati» così come disciplinato dall'art. 9 del RGPD e quindi in linea di principio vietato. Inoltre viene chiesto, in caso di risposta affermativa, se tali azioni poste in essere dall'utente, anche con ulteriori comportamenti quali attivare pulsanti «Mi piace» o «Condividi» sul *social network* possono costituire una valida base giuridica *ex* art. 9, paragrafo 2, lettera e) del RGPD e cioè possano essere trattati da Facebook, in assenza di consenso da parte dell'utente, poiché questo li avrebbe resi manifestamente pubblici ai sensi di tale disposizione.

La prima parte della seconda questione viene agevolmente risolta dalla Corte in senso affermativo rilevando preliminarmente che il RGPD accorda una maggiore tutela alle particolari categorie di dati personali proprio alla luce della maggiore potenziale rischiosità di questi di poter incidere sui diritti e le libertà dei soggetti ai quali si riferiscono e proprio per questo l'art. 9 del RGPD sancisce in astratto un principio di divieto generale di trattamento, con le relative eccezioni previste nello stesso, che però andranno necessariamente interpretate in senso restrittivo, proprio in quanto eccezioni.

La Corte, così, richiamando, da una parte, quanto rilevato dall'avvocato generale nelle sue conclusioni, fa presente che per il RGPD il divieto posto all'art. 9 «è indipendente 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 della Sentenza); dall'altra, la Corte rileva che il divieto di trattamento prescinde sia dalla finalità dichiarata, sia dal fatto che tali dati riguardino un utente del *social network* o qualsiasi altra persona fisica e, pertanto, affinché tali attività rientrino in detta categoria di dati è sufficiente che questi siano in grado di fornire informazioni relative alle citate categorie di dati indipendentemente dai fattori richiamati.



Per quanto riguarda la seconda parte del secondo quesito, invece, va rilevato che, come già rappresentato, l'interpretazione delle eccezioni al divieto generale di trattamento previste dall'art. 9 del RGPD, proprio in quanto eccezioni, vanno applicate in senso restrittivo (su cui la Corte si era già espressa con la sentenza del 17 settembre 2014, *Baltic Agro*, C-3/13, EU:C:2014:2227, punto 24 e giurisprudenza ivi citata, nonché il 6 giugno 2019, *Weil*, C-361/18, EU:C:2019:473, punto 43 e giurisprudenza ivi citata). Da tale principio generale non è esclusa l'eccezione legata al fatto che un interessato, e solo lui, possa decidere di rendere manifestamente pubblici alcuni dati rientranti tra le particolari categorie di dati personali.

Alla luce di quanto sopra la questione va risolta valutando la volontà dell'interessato di rendere o meno manifestamente pubblici tali dati. Si dovrà verificare, pertanto, se l'interessato abbia inteso, in modo esplicito e con un atto positivo chiaro, rendere accessibili al pubblico i dati personali in questione.

Venendo alla questione specifica, quindi, si dovrà valutare se il fatto che un utente navighi su siti internet o attivi pulsanti quali «Mi piace» o «Condividi» soddisfi il requisito di voler rendere pubblici tali dati. A riguardo la Corte rileva, risolvendo anche questa seconda parte della questione, che il semplice navigare non possa di per sé costituire un atto positivo chiaro ed esplicito che esterni tale volontà e che tale volontà non è nemmeno desumibile dall'uso generico di applicazioni, salvo che non vi sia la possibilità per i singoli utenti di attivare un'impostazione individuale di parametri effettuata dallo stesso con piena cognizione di causa, e tali utenti abbiano chiaramente espresso la loro scelta che tali particolari categorie di dati personali siano resi accessibili a un numero illimitato di persone.

5. – Passando alle questioni dalla terza alla quinta, l'analisi si sposta sulle basi giuridiche del trattamento previste per le ordinarie categorie di dati personali, così come elencate all'art. 6 del RGPD ed in particolare a quelle previste nel paragrafo 1 lettere b) ed f), per la terza e quarta questione, e c), d) ed e) con specifico riferimento a tre specifiche ipotesi esplicitate dal giudice amministrativo tedesco.

La Corte, preliminarmente, fa rilevare che, da una parte, ove non sia possibile distinguere in maniera netta il trattamento delle *normali* categorie di dati personali da quelle «particolari» di cui all'art. 9, tali dati necessariamente dovranno rispondere ai requisiti più stringenti dell'art. 9 e non dell'art. 6 e quindi il primo diventerà assorbente nei confronti del secondo (tale principio risponde alla necessità di non abbassare i livelli di sicurezza nel trattamento delle particolari categorie di dati); dall'altra, che l'elenco delle basi di liceità per il trattamento dei dati previsto all'art. 6 (ma anche all'art. 9) rappresenta un elenco esaustivo e tassativo [sentenza del 22 giugno 2021, *Latvijas Republikas Saeima* (Punti di penalità), C-439/19, EU:C:2021:504, punto 99 e giurisprudenza ivi citata].

Inoltre nell'ipotesi in cui l'interessato, in base a quanto previsto dall'art. 6, paragrafo 1, primo comma, lettera a) del Regolamento, e cioè non abbia acconsentito per una o più finalità specifiche, e tale consenso non sia stato espresso in modo libero, specifico, informato e inequivocabile, *ex* art. 4, punto 11 del RGPD, sarà necessario che: il trattamento in questione si fondi su almeno una delle altre basi giuridiche previste nello stesso articolo 6, paragrafo 1, primo comma, lettere dalla b) alla f) del RGPD; che, come già sopra ricordato, tali ulteriori basi giuridiche vadano interpretate in senso restrittivo; e che sia onere del titolare del trattamento dimostrare, *ex* art. 5 del RGPD, che tali dati personali sono segnatamente raccolti per finalità *determinate*, *esplicite* e *legittime* e che essi sono trattati in modo *lecito*, *corretto* e *trasparente* nei confronti dell'interessato.



Alla luce di quanto sopra, quindi, la Corte passa a dettagliare l'analisi delle differenti basi giuridiche sostitutive del consenso dell'interessato, partendo da quella prevista alla lettera b) del citato art. 6 che prevede che un trattamento è lecito quando è «necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso».

Con riferimento a questa ipotesi, benché la valutazione concreta vada fatta dal giudice nazionale del rinvio, la Corte non si sottrae dal chiarire che, affinché si possa ricorrere a tale base giuridica, è indispensabile che il singolo trattamento sia «oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato» (punto 98 della Sentenza) e quindi che non esistano soluzioni alternative meno invasive. Inoltre il responsabile del trattamento dovrà essere in grado di dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento di cui è causa. La semplice menzione nel contratto o la semplice utilità del trattamento non sono sufficienti per il ricorso a tale base giuridica e la legittimità del ricorso a tale esimente del consenso dell'interessato dovrà essere valutato separatamente nel contesto di ogni singolo servizio. Così, nel caso di specie, per la Corte non sembra sostenibile che la personalizzazione di contenuti, né l'utilizzo omogeneo e fluido dei servizi del gruppo Meta siano necessari per consentire di fruire dei servizi del *Social network online*.

La successiva base giuridica presa in esame, e prevista alla lettera f) dell'art. 6 del RGPD, è quella relativa al trattamento di dati per la realizzazione del *legittimo interesse* perseguito dal titolare, affrontato dalla Corte nella quarta questione, che impone al giudice del rinvio di verificare che il legittimo interesse al trattamento dei dati perseguito non possa ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti

*DPCE online*
ISSN: 2037-6677

fondamentali degli interessati così come già sancito dalla Corte nei casi già sopra ricordati.

Nella concreta valutazione della sussistenza di un legittimo interesse, pertanto, si dovrà tenere presente sia il c.d. principio di «minimizzazione dei dati», *ex* art. 5 del RGPD, che prevede che i dati debbano essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»; sia che un siffatto trattamento sia necessario per la realizzazione di tale interesse e che gli interessi o le libertà e i diritti fondamentali della persona interessata non prevalgano su di esso. Ciò ovviamente implica necessariamente una ponderazione dei diritti e degli interessi contrapposti che spetterà valutare al giudice del rinvio secondo le circostanze specifiche (si pensi ad esempio anche ai differenti possibili risultati nel bilanciamento dei diritti nel caso in cui vegano trattati dati personali di minorenni). Pertanto in tale azione «si deve segnatamente tener conto … delle ragionevoli aspettative dell'interessato, nonché della portata del trattamento in questione e dell'impatto di quest'ultimo su tale persona» (punto 116 della Sentenza). Quindi nella valutazione delle singole questioni poste a possibile fondamento dell'impiego della base giuridica del «legittimo interesse» il giudice nazionale dovrà valutare sia se sussiste la possibilità di raggiungere il legittimo interesse al trattamento in modo ragionevolmente altrettanto efficace mediante altri mezzi meno pregiudizievoli per le libertà e i diritti fondamentali degli interessati, sia nel rispetto del citato principio di c.d. «minimizzazione».

6. – Con la quinta questione la Corte passa ad esaminare, sempre nell'ambito di quanto previsto dall'art. 6, paragrafo 1, del RGPD, le ulteriori basi giuridiche del trattamento previste rispettivamente: alle lettere c), ossia quando il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; alla lettera d), quando il trattamento di dati personali è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e alla lettera e), quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento.



Con specifico riferimento a quanto previsto dalle lettere c) ed e), viene ricordato dalla Corte che il trattamento per poter essere lecito in questi due casi «deve essere basato sul diritto dell'Unione o sul diritto dello Stato membro cui è soggetto il titolare del trattamento, e che tale base giuridica deve rispondere a un obiettivo di interesse pubblico ed essere proporzionata al legittimo obiettivo perseguito» (punto 128 della Sentenza).

In particolare nel caso sottoposto qui alla Corte si chiede se un trattamento di dati personali, come quello in causa nel procedimento principale, possa essere considerato giustificato alla luce dell'articolo 6, paragrafo 1, primo comma, lettera c), del RGPD, qualora miri a «rispondere ad una legittima richiesta di dati specifici», e, alla luce dell'articolo 6, paragrafo 1, primo comma, lettera e), di tale regolamento, quando abbia ad oggetto «ricerche a beneficio della società» e sia volto a «promuovere protezione, integrità e sicurezza» (punto 129 della Sentenza). Con specifico riguardo a questo quinto punto la Corte rimette di fatto la questione al giudice del rinvio sia in quanto questo non ha fornito sufficienti elementi che le consentano di esprimere la sussistenza o meno di detti requisiti; sia perché spetta proprio al giudice nazionale, alla luce del contesto applicativo della norma, la valutazione della sussistenza o meno delle condizioni qui sopra indicate, sia se il trattamento di dati personali fondato su tali due basi giuridiche possa essere giustificato dalle finalità rappresentate. Pertanto sarà proprio il giudice nazionale che dovrà valutare se: alla luce della lettera c), del citato art. 3, paragrafo 1 del RGPD, Meta Platforms Ireland sia soggetta a 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, alla luce della lettera e) del medesimo articolo, se 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. Inoltre dovrà anche valutare se, tenuto conto della portata del trattamento di dati effettuato da Meta Platforms Ireland e del suo notevole impatto per gli utenti del *social network* Facebook, detto trattamento sia effettuato nei limiti dello stretto necessario.

L'ultima base giuridica che resta da valutare alla Corte è quella prevista alla citata lettera d) dell'art. 6, paragrafo 1, e cioè quando il trattamento di dati personali è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

Anche in questo caso la Corte rinvia al giudice nazionale tale valutazione, non nascondendo però le propri perplessità nel ricorso a tale base giuridica da parte della Società gestrice del *social network*, in quanto tale base è stata pensata più per situazioni relative a fini umanitari, quali il controllo dell'evoluzione delle epidemie e della loro diffusione, nonché le situazioni di emergenza umanitaria, come i casi di catastrofi di origine naturale e umana. Nel caso di specie, invece, i trattamenti sono stati posti in essere da parte di una società la cui attività riveste un carattere essenzialmente economico e commerciale (punti 136 e 137 della Sentenza).

7. – Con l'ultima questione rimasta in sospeso, la sesta, l'attenzione del giudice del rinvio si sposta sulla prima base giuridica prevista dal RGPD, sia all'art. 6, paragrafo 1, primo comma, lettera a), sia all'art. 9, paragrafo 2, lettera a), e cioè il «consenso» dell'interessato al trattamento dei dati personali che lo riguardano (su cui per approfondimenti cfr. almeno G. Resta-V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, n. 2/2018). Più nello specifico il giudice amministrativo tedesco, chiede alla Corte se «un consenso prestato dall'utente di un *social network online* all'operatore di tale *social network* soddisfi le condizioni di validità previste all'articolo 4, punto 11, 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*».



A riguardo la Corte, partendo dalla definizione di «consenso» prevista all'art. 4, punto 11 del Regolamento che individua il consenso come «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», prosegue con una serie di considerazioni relative al ricorso a tale base giuridica. Così rileva che: 1) «il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio» (considerando 42 RGPD, ultima parte); 2) il considerando 43 del Regolamento enuncia che, per garantire che il consenso sia prestato liberamente, è opportuno che quest'ultimo non costituisca un valido fondamento giuridico per il trattamento dei dati personali, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento; il medesimo considerando prosegue precisando che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso; 3) l'articolo 7, paragrafo 4, del RGPD prevede che, «nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio,

*DPCE online*
ISSN: 2037-6677

sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto»; 4) infine, che l'art. 7, paragrafo 1, del RGPD, prevede che, qualora il trattamento sia basato sul consenso, spetterà al titolare del trattamento l'onere di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali che lo riguardano.

Nel caso specifico, pertanto e alla luce di quanto rammentato dalla Corte, questa constata che, certamente, il fatto che l'operatore di un *social network online*, in qualità di titolare del trattamento occupi una posizione dominante sul mercato dei *social network* non osta, di per sé, a che gli utenti di tale *social network* possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, del RGPD, al trattamento dei loro dati personali posto in essere da tale operatore. Tuttavia, rileva che una circostanza del genere deve essere presa in considerazione da parte di una autorità garante nella valutazione della validità e, in particolare, della libertà del consenso prestato dall'utente di detto *social network*, in quanto essa può incidere sulla libertà di scelta di tale utente, il quale potrebbe non essere in grado di rifiutare o di revocare il suo consenso senza subire pregiudizio (punti 147 e 148 della Sentenza). Peraltro proprio l'eventuale sussistenza di una posizione dominante è astrattamente idonea a creare uno squilibrio evidente, come previsto dal citto considerando 43 del RGPD, tra interessato e titolare del trattamento. Proprio tale squilibrio rischia di favorire l'imposizione di condizioni non strettamente necessarie all'esecuzione del contratto con la conseguente violazione della normativa citata.

Da quanto appena rappresentato discende, quindi, che gli utenti del *social network* dovranno disporre della libertà di rifiutare di prestare il proprio consenso al trattamento di dati personali (in particolare quelli c.d. «*off* Facebook», non necessari all'esecuzione del contratto, senza che venga chiesto agli utenti di rinunciare all'integrale fruizione del servizio offerto. Ciò comporta che agli utenti coinvolti debba essere proposta la possibilità, anche con il pagamento di un *adeguato corrispettivo*, di fruire di una alternativa equivalente che non comporti operazioni di trattamento di dati c.d. «*off* Facebook» non strettamente necessari. Ulteriore conseguenza di quanto previsto sarà rappresentata dalla necessità che l'operatore del *social network* debba prevedere, sempre ai sensi del citato considerando 43, un consenso differenziato tra i dati «off Facebook» e gli altri dati trattati, in assenza del quale si potrà presumere che il consenso non sia stato prestato liberamente, così come invece previsto dalla normativa citata.



Proprio alla luce dei citati criteri, nel caso di specie, conclude la Corte, spetterà al giudice nazionale tedesco, in base allo specifico contesto e a tutti gli elementi in suo possesso, valutare se gli utenti di Facebook abbiano espresso un consenso valido (in quanto conforme con i requisiti richiesti dal RGPD e, in particolare, che questo sia stato liberamente espresso alla luce delle considerazioni appena svolte); ma, come ricordato, spetterà all'operatore del *social network* dimostrare che tale consenso sia stato dato dall'interessato nelle forme e nei modi previsti.

8. – Dopo la necessaria disamina della sentenza qui in commento, sia qui consentita, infine, qualche breve considerazione finale sui vari temi sopra affrontati.

La pronuncia della Corte qui in commento rappresenta un ulteriore importante tassello nella definizione di un complesso quadro applicativo della normativa in materia di tutela dei dati personali che, sempre più, sta cercando di andare, almeno a livello eurounitario, nella direzione del perseguimento di maggiori livelli di effettività nell'applicazione del modello di tutela dei dati personali delle persone fisiche (su cui cfr. E. Cremona, *I poteri privati nell'era*

*digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023; F. Ruggeri, *Poteri privati e mercati digitali. Modalità di esercizio e strumenti di controllo*, Roma, 2023, scaricabile dal sito dell'editore). Va rilevato, infatti, che la formale legittimazione, sancita dalla Corte, di intervento da parte anche di autorità terze, sempre nel rispetto del principio di leale cooperazione, rispetto a quelle individuate dal Trattato per il controllo dell'applicazione del RGPD, estende ulteriormente i livelli di controllo sugli operatori privati sortendo l'effetto di moltiplicare i soggetti pubblici che nello spazio europeo possono rendersi parte attiva nella vigilanza e attuazione della normativa vigente in materia.

La rassegna e l'attenta disamina effettuata dalla Corte relativamente al corretto ricorso alle basi giuridiche del trattamento da parte dei *social network* nella gestione dei dati personali degli utenti, ma anche dei soggetti terzi coinvolti, innalza i livelli di chiarezza sui limiti entro i quali i trattamenti possono essere considerati leciti o meno e quindi aumenta anche la certezza per gli operatori pubblici e privati, ma soprattutto delimita meglio i confini di tutela per gli interessati e sostanzialmente sancisce la definitiva necessità per gli operatori dei *social network* del ricorso al «consenso» per il trattamento dei dati «*off* Facebook» ed in particolare per le *particolari categorie di dati personali*. Con tale effetto, sostanzialmente, si cerca di dare maggiore centralità agli utenti rispetto allo strapotere delle società gestrici delle piattaforme *social* in posizione dominante sul mercato.

Inoltre, con questa pronuncia la Corte, da una parte, prova a limitare ulteriormente la discrezionalità delle piattaforme social nell'uso spregiudicato dei dati personali dei propri iscritti. Così fissando dei più chiari criteri nell'uso delle particolari categorie di dati e nella qualificazione degli stessi quali *manifestamente resi pubblici dall'interessato* o meno; chiarendo quando un trattamento può essere considerato «necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso»; ma anche definendo meglio i limiti al ricorso all'uso del legittimo interesse quale base giuridica del trattamento; o del ricorso all'art. 6 lettera b), c) e d) come base di liceità del trattamento; ma anche, infine, con riguardo al ricorso anche alla lettera a) sempre dell'art. 6, e cioè rispetto al *consenso*. Dall'altra, chiarendo meglio i confini ermeneutici della normativa in materia di tutela dei dati personali, la Corte incide positivamente sui livelli di uniformità applicativa della normativa in materia all'interno dell'Unione, sulla quale le singole autorità di controllo in materia di tutela dei dati personali saranno chiamate a vigilare non potendo, peraltro, uscire da detti margini interpretativi a pena di divenire esse stesse fonte di distorsione nell'interpretazione della normativa in materia di tutela dei dati personali tra i differenti Paesi membri.



Infine, sia consentito fare un focus sul primo effetto che tale decisione della Corte ha già prodotto sul colosso dei *social network*, infatti dai primi di novembre 2023 per poter utilizzare Facebook, ma anche Instagram, gli utenti europei sono stati messi di fronte ad una scelta, e cioè se accettare di continuare a vedere pubblicità, e quindi essere di fatto profilati per finalità di marketing, con tutto ciò che questo comporta in termini di trattamento delle differenti tipologie di dati personali, oppure sottoscrivere un abbonamento a pagamento con un costo mensile che va dai 10 ai 13 euro circa per poter continuare ad usufruire della piattaforma senza pubblicità, impedendo, almeno in teoria, a Facebook il pieno trattamento dei dati personali per finalità di profilazione (su cui per maggiori dettagli sull'operazione posta in essere cfr. G. Adonopoulos, *Facebook e Instagram a pagamento: conviene abbonarsi? Cosa cambia*, reperibile in www.forbes.com/advisor/it/internet-mobile/facebook-instagram-a-pagamento-costo-conviene/; ma anche in ottica generale sulla tematica V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del*

*DPCE online*
ISSN: 2037-6677

*fenomeno*, e A. De Franceschi, *Il "pagamento" mediante dati personali*, entrambi in V. Cuffaro-R. D'Orazio-V. Ricciuto (cur.), *I dati personali nel diritto europeo*, Torino, 2019, 23).

Proprio con riguardo al tema del rapporto tra piattaforme digitali *social* e interessati, sia qui consentito, a chiusura del presente lavoro, di proporre alcune ulteriori brevi considerazioni conclusive.

La prima è che l'entità dell'importo richiesto da parte di Facebook per poter non profilare il singolo utente non è ininfluente nella scelta che sono obbligati a fare i fruitori della piattaforma (che, va ricordato, ha una posizione dominante sul mercato!) nell'acconsentire o meno da parte degli utenti alla propria profilazione per finalità di marketing, infatti, sarebbe interessante conoscere, sul numero totale di utenti europei della piattaforma *social*, la percentuale di utenti che ha deciso di sopportare un esborso economico, ad oggi di circa 150 euro annuali, per non vedere pubblicità e quindi per non consentire il pieno trattamento dei propri dati personali per fini di profilazione. Ciò darebbe un'evidenza empirica sull'effettivo potere di forza delle piattaforme rispetto ai propri utenti e all'irrinunciabilità dei servizi da queste erogati da parte degli utenti stessi. Ma anche al valore che oggi viene dato alla cessione dei propri dati personali da parte degli interessati al trattamento, utenti dei *social*.

La seconda è che con questa operazione si ha una quantificazione economica esatta, posta in essere dallo stesso operatore economico, sul valore che Meta dà alla profilazione di ogni utente. Sarebbe interessante comprendere se effettivamente sia questo il reale valore per Meta della profilazione di ogni singolo utente o se vi sia stata una scelta consapevole da parte della stessa di gonfiare tale valore per cercare di dissuadere la stragrande maggioranza degli utenti dal non farsi profilare per finalità di marketing. Quest'ultima ipotesi sarebbe un chiaro segnale dell'irrinunciabilità da parte di Meta nella profilazione della gran parte degli utenti, senza la quale il proprio modello di business subirebbe probabilmente un colpo mortale.



La terza, che si collega strettamente alla seconda, è che ormai è acclarato che la rischiosità nel trattamento dei dati da parte degli operatori non è data dalla somma delle rischiosità dei singoli trattamenti, bensì detta rischiosità aumenta in modo esponenziale al collegarsi tra di loro delle differenti banche dati, poiché l'incrocio dei dati consente di trarre informazioni che probabilmente sarebbe impensabile estrarre da parte degli algoritmi che avessero accesso ad una sola banca dati. E a riguardo va ricordato che Meta gestisce sia i dati di Facebook, ma anche di WhatsApp e di Instagram ad oggi, tutti applicativi con milioni di utenti.

La quarta, che tale meccanismo alternativo tra il pagamento di una somma di denaro (e chissà se la Corte quando ha previsto nella Sentenza, come ricordato sopra, «se del caso» il pagamento di un eventuale «adeguato corrispettivo», se per «adeguato» intendesse l'ordine di grandezza della cifra fissata oggi da Facebook) e il diritto di trattare anche le *particolari categorie* di dati personali da parte di un soggetto in posizione di forza, pone il problema della effettività della tutela del diritto fondamentale alla protezione dei dati personali nei Paesi membri. Infatti il problema nella tutela dei diritti e delle libertà fondamentali dei singoli utenti non è tanto legato al fastidio della pubblicità che gli stessi ricevono navigando sui *social network*, bensì alla propria profilazione e al livello di estremo dettaglio che questa può raggiungere. Infatti, con l'elaborazione da parte dei sofisticati algoritmi dell'incrocio dei dati raccolti dalle varie piattaforme i cui dati sono collegati, si può arrivare a sapere di una persona fisica anche di più di quanto questa consapevolmente sappia su se stessa. Non a caso il RGPD proprio alla profilazione pone particolare attenzione e tutele dedicate in quanto il legislatore europeo è ben consapevole degli elevati rischi per i diritti e le libertà fondamentali ai quali possono andare incontro le persone fisiche in caso di un non attento

trattamento di tali dati ed in particolare di quelli comunemente noti come *sensibili*. Si prospetta quindi il rischio che tali modelli di business evolvano verso una impostazione elitaria della tutela dei diritti fondamentali nella quale chi potrà permetterselo, ammesso che poi la promessa venga mantenuta dall'operatore economico, potrà decidere di non farsi profilare, invece la massa degli altri utenti, alla luce della "pistola alla tempia" rappresentata dalla posizione dominante dell'operatore, sarà costretta a "cedere" il diritto alla maggiore invasività rappresentata dall'essere profilato, rispetto al mero trattamento dei propri dati personali, in cambio dell'uso della piattaforma social o dell'applicativo di turno.

Infine va rilevato che alla sentenza qui in commento va riconosciuto il merito che, almeno per il tempo di un *click* sul pulsante «accetto», ha prodotto l'effetto di costringere milioni di utenti europei ha realizzare il livello di dipendenza da tali applicativi, infatti se prima la piattaforma sceglieva direttamente per gli utenti a chi inviare i dati degli stessi non dovendo richiedere alcun consenso al trattamento dei dati, oggi questi hanno avuto la possibilità (almeno teorica) di "scegliere" se finanziare direttamente la società che gestisce il *social network* con un costoso abbonamento, o se farlo, in via indiretta, attraverso le società che pagano i servizi pubblicitari al *Social*, accettando *ob torto collo* il trattamento incrociato per fini di profilazione dei dati prodotti anche «off Facebook». In pochi, infatti, visti i livelli di dipendenza che tali applicativi riescono a produrre in chi li usa, avranno anche solo per un attimo preso in considerazione la c.d. "*opzione zero*" e cioè l'abbandono della piattaforma con la contestuale rinuncia alla fruizione della stessa.

Gianluca Bellomo
Dipartimento di Scienze Giuridiche e Sociali,
Università degli Studi "G. d'Annunzio" – Chieti/Pescara
gianluca.bellomo@unich.it