Il caso Facebook e la tutela dei dati personali: una partita ancora aperta

di Alessandro Giovanni Masotti

Title: The Facebook case and the protection of personal data: still an open game

Keywords: GDPR, Competition authority of a Member State, Payment via personal data.

1. – Con la sentenza resa a Grande Sezione il 4 luglio 2023, in riferimento alla causa C-252/21 che contrappone varie società del gruppo *Meta* (d'ora in poi *Meta Platforms*) e l'autorità federale garante della concorrenza in Germania, la Corte di giustizia dell'Unione europea (CGUE) si è pronunciata sul tema della protezione delle persone fisiche con riguardo al trattamento dei dati personali, disciplinato dal Regolamento (UE) 2016/679, allorquando venga in rilievo un possibile abuso di posizione dominante praticato da un *social network online*.

La tematica in esame è di grande interesse sia dal punto di vista dei diritti dei consumatori, come dimostra l'intervento in causa della *Verbraucherzentrale Bundesverband eV* (l'associazione federale tedesca delle organizzazioni dei consumatori), che da quello dei margini di azione per i *social network online*.

L'attualità della questione è inoltre testimoniata dalla notevole attenzione riservata dalle Istituzioni europee alla profilazione degli utenti senza il loro consenso, in passato attraverso il Regolamento generale sulla protezione dei dati (GDPR) del 2016 e oggi, in aggiunta a quest'ultimo, con l'introduzione del *Digital Services Act package* composto dal *Digital Markets Act*, il Regolamento (UE) 2022/1925, e dal *Digital Services Act*, il Regolamento (UE) 2022/2065.

Ad ulteriore conferma dell'odierno interesse all'argomento, si considerino anche le numerose decisioni adottate dell'*European Data Protection Board* (EDPB). Da ultimo, quella vincolante e urgente, datata 27 ottobre 2023, nei confronti di *Meta Platforms Ireland Ltd*, sul trattamento dei dati personali per la pubblicità comportamentale offerta dalla piattaforma. Mediante questa decisione si è indicato, alle *Data Protection Authorities* interessate, di imporre un divieto a *Meta Platforms* di trattare i dati personali, raccolti per scopi pubblicitari, sulla base delle condizioni di contratto allora vigenti o dell'interesse legittimo perseguito dal titolare del trattamento. Secondo l'EDPB, il divieto si è reso necessario per evitare che le attività *online* dei soggetti interessati venissero costantemente monitorate e profilate da *Meta Platforms*. Infatti, il trattamento operato dal *social* è stato tale da determinare una lesione dei diritti fondamentali degli utenti, attraverso effetti negativi sulla libertà di informazione e di partecipazione alla vita politica, ai quali faceva seguito un rafforzamento degli stereotipi esistenti e una conseguente discriminazione per i clienti del *social* (v. *Urgent Binding Decision 01/2023 requested by the Norwegian SA for*

the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR), in https://www.edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf).

Si può osservare che la sentenza in commento inerisce perfettamente al tema della protezione dei dati personali ribadendo, seppur con riferimenti al solo GDPR, i valori e gli obbiettivi che le Istituzioni europee avevano già normato nel 2022 mediante il *Digital Services Act* (entrato in vigore il 17 febbraio 2024) e il *Digital Markets Act* (entrato in vigore il 7 marzo 2024).

Al fine di cogliere pienamente il bilanciamento svolto dalla CGUE, tra la tutela dei diritti fondamentali del soggetto interessato e le esigenze commerciali di un *social*, è vantaggioso inquadrare i diritti fondamentali coinvolti e l'impatto che il trattamento dei dati personali, finalizzato a scopi pubblicitari, ha avuto e continuerebbe ad avere sugli stessi diritti se la Corte non fosse intervenuta. Ad esempio, il principio sancito dall'art. 8 CDFUE (Carta dei diritti fondamentali dell'Unione europea) e dall'art. 16 TFUE (Trattato sul funzionamento dell'Unione europea) per cui "ogni persona ha diritto alla protezione dei dati personali che la riguardano" (v. M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati* personali, in V. Cuffaro, R. D'Orazio, V. Ricciuto (cur.), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 184). Ulteriormente coinvolti sono il diritto al rispetto della vita privata e della vita familiare, previsto all'art. 7 CDFUE, e ancora i diritti fondamentali come la tutela del domicilio e delle comunicazioni, la libertà di pensiero, di coscienza e di religione, la libertà d'informazione e la diversità culturale, linguistica e sessuale di ogni persona. L'impatto del trattamento compiuto dal *social* ha creato rischi significativi per questi diritti e libertà fondamentali dal momento che le attività degli utenti (soggetti interessati dal trattamento) compiute *online* sono state costantemente, intrusivamente e opacamente monitorate e profilate dal responsabile del trattamento.

Secondo la Corte, quest'ultimo, fornendo prova del rispetto delle previsioni normative in materia di consenso al trattamento dei dati, ha compiuto una serie di operazioni con gli stessi, che comunque dovevano essere note all'interessato e conformi a quanto previsto dal GDPR. Qui già si anticipa che la Corte, pur lasciando qualche spiraglio di apertura a favore dell'operatore di un *social network online*, ha privilegiato la tutela dei diritti e dei dati personali delle persone fisiche, lasciando al giudice del rinvio il compito di verificare se nel caso concreto si possa rientrare in detti spiragli.

2. - Per un'adeguata comprensione delle riflessioni svolte dalla Corte è utile partire da una premessa generale ed esporre poi, seppur succintamente, i fatti di causa. *Meta Platforms* gestisce l'offerta del *social network* Facebook nell'Unione Europea. Il modello imprenditoriale del *social*, fino a novembre 2023, si basava unicamente su un finanziamento tramite la pubblicità *online* creata su misura per il singolo utente. In particolare, venivano impiegati dati relativi al comportamento di consumo, agli interessi, al potere d'acquisto e alla situazione personale, ottenuti dagli utenti al momento dell'iscrizione ai servizi o raccolti all'interno e all'esterno del suddetto *social*. I dati relativi alle attività fuori dal *social* (dati *off* Facebook) sono, da un lato, concernenti la consultazione di pagine Internet e di applicazioni di terzi collegate a Facebook attraverso interfacce di programmazione (così detti Strumenti *business* di Facebook) e, dall'altro, riguardanti l'utilizzo degli altri servizi *online* appartenenti al gruppo *Meta*, tra i quali Instagram, WhatsApp, Oculus e Masquerade. Tutti questi dati vengono messi in relazione e il quadro generale che ne emerge consente di trarre conclusioni dettagliate sulle preferenze e sugli interessi degli utenti.

Con decisione del 6 febbraio 2019, fondata sull'art. 19, § 1, e sull'art. 32 del GWB (la legge tedesca contro le restrizioni della concorrenza), l'autorità federale garante della concorrenza in Germania ha vietato a *Meta Platforms* di subordinare,

DPCE online
ISSN: 2037-6677

nelle condizioni generali, l'uso di Facebook da parte di utenti privati residenti in Germania al trattamento dei loro dati *off* Facebook e di procedere, senza il loro consenso, al trattamento di tali dati come previsto dalle condizioni generali allora vigenti. Con la stessa misura ha ordinato di adeguare dette condizioni generali, in modo che da esse risultasse chiaramente che tali dati non sarebbero stati né raccolti, né messi in relazione con gli *account* degli utenti Facebook, né utilizzati senza il consenso dell'utente interessato e che tale consenso non sarebbe stato valido qualora avesse costituito una condizione per l'utilizzo del *social network*.

L'autorità federale garante della concorrenza ha giustificato il suo intervento in una materia, quella della protezione dei dati personali, disciplinata dal Regolamento 2016/679 e non appartenente, a prima vista, alla materia della concorrenza, con l'argomentazione che il trattamento dei dati *off* Facebook degli utenti interessati avrebbe costituito uno sfruttamento di posizione dominante di tale società sul mercato dei *social network online* in Germania e che lo stesso non sarebbe stato conforme ai valori sottesi al GDPR.

L'11 febbraio 2019 *Meta Platforms* ha presentato un ricorso avverso la decisione dinnanzi all'*Oberlandesgericht Düsseldorf* (Tribunale superiore del Land, Düsseldorf, Germania).

Dal 31 luglio 2019, *Meta Platforms* ha introdotto nuove condizioni generali in cui si indica che l'utente, invece di pagare una quota per l'uso dei prodotti Facebook, dichiara di acconsentire alle inserzioni pubblicitarie. Inoltre, dal 28 gennaio 2020, *Meta Platforms* offre in tutto il mondo la possibilità, attraverso apposita funzione, di visualizzare un riepilogo delle informazioni che riguardano il singolo utente e che le società del gruppo ottengono in relazione alla sua attività su altri siti Internet e applicazioni, e di scollegare, se l'utente lo desidera, tali dati dal suo account Facebook sia per il passato quanto per il futuro.

Il Tribunale, nutrendo numerosi dubbi sul tema, ha deciso di sospendere il procedimento sottoponendo alla Corte di giustizia sette articolate questioni pregiudiziali e ha ritenuto che la soluzione della controversia dipendesse dalla risposta alle stesse.

In particolare, un dubbio ha riguardato la possibilità per un'autorità nazionale garante della concorrenza di controllare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, la conformità di un trattamento dei dati personali alle condizioni stabilite dal GDPR. Ulteriormente, è stato domandato se questa autorità potesse procedere al controllo in contemporanea con una procedura avviata dall'autorità di controllo capofila competente ai sensi dell'articolo 56, § 1, del GDPR (quest'ultima corrisponde all'autorità dello Stato in cui ha sede lo stabilimento principale o unico nell'Ue del titolare o responsabile del trattamento ed è anche l'unica interlocutrice con lo stesso, alla quale viene trasferita la competenza da tutte le altre autorità di controllo definite, in questo caso, "autorità interessate" per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile).

Un secondo dubbio ha interessato la possibilità, per un operatore di un *social network online*, di trattare particolari categorie di dati sensibili della persona interessata che necessitano di una maggiore tutela, ai sensi dell'art. 9, § 1 e 2, del GDPR.

Un terzo dubbio ha riguardato la liceità, ai sensi dell'art. 6, § 1, del GDPR, del trattamento dei dati personali dell'utente interessato per le finalità asserite dal *social*.

Da ultimo il Tribunale ha domandato se, alla luce dell'art. 6, § 1, lett. a) e dell'art. 9, § 2, lett. a), del Regolamento, possa essere ritenuto valido il consenso prestato dall'utente, ai fini di un simile trattamento, a un'impresa che detiene una posizione dominante sul mercato nazionale dei *social network online*.

3. - Anzitutto, tratterò le questioni, prima e settima, attinenti la competenza dell'autorità garante della concorrenza di uno Stato membro e successivamente la sesta questione per avere chiara la regola generale elaborata dalla Corte in materia di consenso. Poi affronterò la seconda questione relativa alle particolari categorie di dati personali e da ultime la terza, quarta e quinta questione tutte attinenti ai casi in cui il trattamento dei dati possa essere considerato necessario a prescindere dal consenso.

La prima e la settima questione sono state affrontate congiuntamente dalla Corte, la quale ha da un lato precisato che le autorità di controllo e quelle garanti della concorrenza esercitano funzioni, compiti e perseguono obbiettivi diversi, dall'altro ha detto che l'autorità garante della concorrenza nel suo Stato membro potrebbe, quando esamina un abuso di posizione dominante di un'impresa, riferirsi a norme diverse da quelle sulla concorrenza, come ad esempio le norme del GDPR.

La Corte ha messo in luce come l'accesso ai dati personali e il loro sfruttamento rivestano un'importanza fondamentale nell'ambito dell'economia digitale. Pertanto, escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione, in sede di esame di abuso di posizione dominante, trascurerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione.

Per evitare poi divergenze tra le due autorità, la Corte ha affermato che esse devono confrontarsi e cooperare lealmente (principio di leale cooperazione) così da rispettare poteri e competenze altrui e, allo stesso tempo, osservare gli obblighi e obiettivi fissati dal GDPR. Secondo la Corte, nel caso sia già stata resa una decisione da parte dell'autorità di controllo, anche quella adottata a sua volta dall'autorità in materia di concorrenza non potrà discostarsene, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza.

Laddove l'autorità garante della concorrenza dovesse nutrire dubbi sulla valutazione operata dall'autorità di controllo interessata, la prima dovrà consultare la seconda per fugare i propri dubbi o per decidere di attendere che l'autorità di controllo capofila prenda una decisione prima di iniziare la sua attività di valutazione. L'autorità interpellata dovrà, entro un termine ragionevole, rispondere comunicando all'autorità garante della concorrenza le informazioni di cui dispone; trascorso tale termine quest'ultima potrà procedere ugualmente.

Nel caso di specie, la Corte ha rilevato che, ferme restando le verifiche che spettano al giudice del rinvio, l'autorità federale garante della concorrenza in Germania sembra aver ottemperato ai suoi obblighi di leale cooperazione con le autorità di controllo nazionali interessate nonché con l'autorità di controllo capofila.

4. - Rispondendo alla sesta questione pregiudiziale, la Grande Sezione, anzitutto, ha fornito la regola generale in tema di consenso, ripresa dall'art. 4, punto 11 del GDPR, che è quella di un consenso espresso in modo libero, specifico, informato e inequivocabile tranne nei casi in cui vengono in rilievo particolari dati per i quali la tutela è più intensa o nei quali in cui il consenso può non essere necessario.

Poi ha stabilito che gli utenti di un *social network* possano validamente acconsentire al trattamento dei loro dati personali anche nel caso in cui l'operatore online occupi una posizione dominante sul mercato dei *social network*. Tuttavia, lo squilibrio tra utente e *social* potrebbe permettere a quest'ultimo di imporre operazioni di trattamento non necessarie, come quelle relative ai dati esterni a Facebook. In tali casi, la Corte ha preteso che agli utenti venga lasciata la possibilità di rifiutarle senza rinunciare ad alcun servizio offerto dal *social network*. Quest'ultima eventualità implicherebbe che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non corredata da simili operazioni di trattamento.

DPCE online
ISSN: 2037-6677

5. - La seconda questione ha affrontato il tema della liceità o illiceità del trattamento quando un utente consulti una pagina *web* o applicazioni correlate e/o inserisca in esse dati o effettui ordini *online* e vengano coinvolte particolari categorie di dati personali, previste all'art. 9, § 1, del GDPR. Quest'articolo prevede che «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».

La Corte ha ritenuto che il trattamento operato da *Meta Platforms* possa rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose nonché i dati legati alla salute o alla vita sessuale e all'orientamento sessuale di una persona fisica. L'art. 9, § 2, del GDPR prevede delle eccezioni al divieto di trattamento dei dati rientranti nella categoria di cui al § 1. Ad esempio, la necessità di tutelare un interesse pubblico, l'ipotesi in cui i dati siano stati resi manifestamente pubblici dall'interessato e ancora il caso in cui il medesimo abbia dato il suo consenso esplicito al trattamento per finalità specifiche. I giudici hanno poi escluso che le attività di inserimento di dati su un sito Internet o all'interno di applicazioni, così come l'attivazione dei pulsanti "Mi piace" o "Condividi" da parte dall'interessato, possano far intendere che l'utente abbia voluto rendere manifestamente pubblici i suoi dati, ai sensi dell'eccezione presente al § 2.

6. - La terza, la quarta e la quinta questione possono essere affrontate assieme poiché la Corte, in esse, ha valutato la possibilità di considerare necessario il trattamento operato da *Meta Platforms* ai sensi dell'art. 6, § 1 del GDPR.

La Corte ha escluso che la personalizzazione dei contenuti e l'utilizzo coerente e senza interruzioni di tutti i prodotti offerti da *Meta Platforms* (Facebook, Instagram e Whatsapp) possano ritenersi necessari all'esecuzione del contratto concluso con la piattaforma. In *primis* perché potrebbe essere utile ma non necessario per l'offerta del *social* ed in *secundis* perché ognuno dovrebbe essere libero di usare un solo servizio invece che tutti (ad esempio, uso Facebook e non Instagram). Infatti, per trattamento necessario all'esecuzione del contratto si dovrebbe intendere solo quello che sia oggettivamente indispensabile per realizzare una finalità che costituirebbe parte integrante della prestazione contrattuale e in assenza del quale l'obbiettivo principale del contratto non potrebbe essere conseguito.

La Corte, nel suo argomentare, ha aggiunto che il trattamento operato da *Meta Platforms* potrebbe risultare lecito se fosse necessario a perseguire un legittimo interesse del titolare del trattamento o di terzi, ma a condizione che, su questo, non prevalgano i diritti e le libertà fondamentali dell'interessato.

Le valutazioni compiute dalla Grande Sezione hanno posto in rilievo che le politiche adottate da *Meta Platforms* non soddisferebbero quasi mai il requisito appena descritto.

Infatti, pur non escludendo a priori che l'interesse del titolare del trattamento al miglioramento del suo prodotto possa costituire un legittimo interesse giustificativo del trattamento, la Corte, nel caso concreto, ha ritenuto che, considerando la portata del trattamento in questione, i diritti fondamentali prevalgono sulle finalità pubblicitarie e sulle esigenze di miglioramento del prodotto. Allo stesso tempo, ha escluso che la salvaguardia degli interessi vitali dell'interessato o la comunicazione alle autorità preposte all'esercizio delle azioni penali possano essere delle esimenti pertinenti al caso di specie, in quanto il *social* è un operatore privato e pertanto estraneo a simili attività. E ancora, garantire la sicurezza del *social* potrebbe essere un legittimo interesse solo se i dati effettivamente trattati avessero questo scopo e non vi fossero modalità meno pregiudizievoli per raggiungere l'obbiettivo. Quest'ultima valutazione è stata rimessa al giudice del rinvio.

7. - Tra le tante problematiche, il caso affrontato dalla Corte investe anche lo stretto rapporto tra consenso e liceità del trattamento del dato quando questo abbia carattere personale, dal momento che il consenso costituisce la base di ogni trattamento.

La definizione europea di dato personale è molto ampia e, sinteticamente, corrisponde a qualsiasi informazione riguardante una persona fisica identificata o identificabile (art. 4, n. 1, del GDPR).

Fra le varie ipotesi in cui un trattamento è da considerarsi lecito anche in assenza di consenso, quelle rilevanti nel caso di specie sono riconducibili alla necessità dello stesso, quale elemento utile e indispensabile per poter, come già ricordato, dare esecuzione al contratto o alla necessità di salvaguardare gli interessi vitali dell'interessato. Questo a condizione che relativamente alle suddette ipotesi non prevalga la tutela dei diritti fondamentali dell'individuo.

Si può quindi affermare che la nozione di necessità del trattamento ricopra un ruolo centrale nelle politiche europee in materia di protezione dei dati personali e, per una sua corretta implementazione, è da considerarsi sottratta ad una declinazione nazionale differenziata (v. L. Ruggeri, *La dicotomia dati personali e dati non personali: il problema della tutela della persona nei c.dd. dati misti*, in *Diritto di famiglia e delle persone* (II), fasc. 2, 1 giugno 2023, 808 ss.). Ad ulteriore conferma si può ricordare che una precedente decisione della medesima Corte (Corte giust., sent. 16-12-2008, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland*), rilevante per aver garantito un equivalente livello di tutela a qualsiasi interessato in ogni Stato, ha affermato che la nozione di dato personale non può avere un contenuto variabile a seconda della definizione fornita dal singolo Stato membro, trattandosi di una nozione autonoma del diritto europeo.

Di per sé è irrilevante che il trattamento sia menzionato nel contratto o che esso sia solo utile per la sua esecuzione. Infatti, ad essere determinante è il fatto che il trattamento sia essenziale per la corretta esecuzione del contratto e che non vi siano alternative meno invasive. Ne deriva, come lucidamente evidenziato dalla Corte, che nel caso concreto né il contratto, né il legittimo interesse, né meno ancora l'interesse vitale o l'obbligo legale, possano essere considerati basi giuridiche idonee per l'uso dei dati al fine di determinare una pubblicità su misura.

Ciò detto, si deve ricordare, come già osservato in dottrina (v. C.A. Trovato, *La sentenza CGUE del 4.7.2023 nel caso C-252/21 sui rapporti tra privacy e antitrust, sulla pubblicità dei dati sensibili e sulla inadeguatezza della base del legittimo interesse per il trattamento dei dati inerenti la pubblicità comportamentale di Meta (sentenza Meta abuso di posizione dominante)*, in *Persona e mercato*, num. 3, anno 2023, 595), che la CGUE si è limitata, come doveva, ad esprimere un giudizio sul caso di specie analizzando le argomentazioni fornite dal titolare del trattamento. Si ricordi che *Meta Platforms* ha asserito che la pubblicità personalizzata fosse necessaria per offrire il servizio di *social network* e a tal riguardo i giudici europei hanno ritenuto che tutte le ragioni addotte, ad eccezione della finalità di garantire la sicurezza del *social*, che dovrà essere vagliata dal giudice del rinvio, non possano essere usate come fondamento giuridico dell'attività promozionale, la quale si può considerare utile ma non indispensabile per l'erogazione del servizio.

Sarebbe stato interessante verificare a quale conclusione sarebbe giunta la Corte se *Meta Platforms* avesse osato di più, sostenendo che la pubblicità "customizzata" sarebbe stata necessaria, come era evidente, a finanziare il *social network*, configurandosi come controprestazione contrattuale. La medesima dottrina ipotizza che ciò non sia avvenuto per evitare di proporre autonomamente un mutamento del proprio modello di *business* verso una sorta di modello *paywall*. Se così avesse fatto, avrebbe almeno dovuto offrire un'alternativa per la fruizione del *social* a pagamento in aggiunta a quella solo idealmente "gratuita". Ipotizzando che *Meta Platforms* avesse veramente voluto osare di più, il problema sarebbe stato verificare se i dati richiesti, ai fini della pubblicità personalizzata (quale

DPCE online
ISSN: 2037-6677

controprestazione/strumento di finanziamento), sarebbero stati necessari per l'esecuzione del contratto oppure no. La questione è spinosa sul piano interpretativo. Infatti, richiamando le linee guida sul consenso dell'EDPB, sarebbe stato altamente inopportuno mascherare o accorpare il consenso al trattamento dei dati personali all'esecuzione di un contratto o alla prestazione di un servizio per il quale i dati stessi non sarebbero necessari (v. EDBP, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, 11 ss., https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf). La norma che avrebbe potuto trovare applicazione, dipendendo dalla necessarietà o meno dei dati, sarebbe stata quella dell'art. 7, § 4, del GDPR, rubricata "condizioni per il consenso". Tale norma prevede che nella valutazione della libertà del consenso si tenga nella massima considerazione l'eventualità in cui l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati non necessari all'esecuzione. Nel caso concreto, sostenere che la pubblicità "customizzata" (basata sul consenso al trattamento dei dati personali) fosse necessaria quale controprestazione contrattuale, alla prestazione del *social* (mettere in contatto tra di loro gli utenti), avrebbe imposto alla Corte di indagare se non vi fosse stata altra strada meno "invasiva" per addivenire allo stesso risultato. Infatti, se l'unico modo di finanziare la prestazione contrattuale di Facebook fosse stato la pubblicità "customizzata", formata dai dati personali degli utenti, per quanto sensibili essi fossero, il contratto non sarebbe stato eseguibile senza questa controprestazione. Allora, il consenso al trattamento, forse, non sarebbe stato necessario in quanto si sarebbe rientrati nella deroga di cui all'art. 6 § 1, lett. b del GDPR. Sul punto, si segnala che l'EDPB, nelle linee guida 5/2020, prevede che se il titolare del trattamento offre un servizio equivalente che non implica un consenso al trattamento, allora non si tratterebbe di un servizio realmente condizionato a quella fornitura di dati personali. Ebbene, considerato che al tempo della decisione *Meta Platforms* non prevedeva un'alternativa a pagamento del medesimo servizio, si potrebbe ritenere, diversamente da oggi, che la prestazione contrattuale di Facebook era obbiettivamente condizionata al finanziamento mediante pubblicità "customizzata" sulla base dei dati personali. A questo punto la Corte avrebbe dovuto decidere se fosse stata comunque più meritevole di tutela, la salvaguardia dei diritti fondamentali o l'attività imprenditoriale del *social* necessariamente eseguita attraverso quella specifica pubblicità.

8. - Particolarmente ardua si rivela anche l'interpretazione del passaggio della pronuncia in cui la Corte ha affermato che «Pertanto, tali utenti 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, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati».

Meta Platforms, lungi dal seguire pedissequamente l'impostazione della Corte, da novembre 2023 ha introdotto per la prima volta nella sua offerta un abbonamento a pagamento (per Facebook e Instagram), sempre corredato da un trattamento dei dati personali. La soluzione predisposta non sembra però essere in linea con gli intenti della CGUE per due motivi che riguardano la modalità con cui è stata presentata questa possibilità e l'interruzione del trattamento dei dati personali (di cui la Corte ritiene sia vietato il trattamento) ai soli fini pubblicitari.

Sotto il primo profilo, si evidenzia che *Meta Platforms* ha "offerto" ai suoi clienti la possibilità di ottenere il medesimo servizio a fronte del versamento di una somma di denaro oppure di continuare ad usare "gratuitamente" la prestazione accettando di

ricevere annunci personalizzati (e subendo così un pieno trattamento dei propri dati personali). In verità, come è stato già fatto notare nel comunicato stampa n. 49 del 2023 da BEUC, *The European Consumer Organisation*, a cui aderisce anche l'Italia, non si sarebbe trattata di una vera scelta, dal momento che, attraverso un blocco parziale dell'utilizzo del servizio, si è creato un senso di urgenza che ha spinto molti consumatori a prendere una decisione non sufficientemente meditata.

A ciò si deve aggiungere che tanto il BEUC quanto il *Datatilsynet* (il garante della privacy norvegese) rilevano che l'opzione a pagamento escluderebbe il trattamento dei dati personali solo a fini pubblicitari, rimanendo inalterate raccolta, memorizzazione e utilizzazione dei dati ad altri scopi. Per rifarsi alle parole del responsabile della comunicazione di *Meta Platforms* in Europa, Matt Pollard, queste attività verranno comunque portate avanti per fornire agli utenti esperienze organiche e personalizzate che sono apprezzate su Facebook e Instagram, come i post consigliati e le raccomandazioni degli amici (v. M. Meaker, *Norway's Privacy Battle With Meta Is Just Getting Started*, in Wired UK, 2023, *https://www.wired.co.uk/article/line-coll-norway-datatilsynet-meta*).

Quanto accaduto è frutto di una lettura particolare della frase impiegata dalla Corte. Infatti, escluso da quest'ultima il fine pubblicitario, al *social* non serve altro che addurre che tale trattamento è necessario per l'esecuzione del contratto (ad esempio, per fini di miglioramento della prestazione e per la maggiore sicurezza del *social* stesso) e aggirare così la tutela apprestata dal giudice europeo.

La questione è senza dubbio un punto di intersezione tra le categorie del diritto alla tutela dei dati personali e il diritto della concorrenza, tanto più se si considera la scelta "offerta" all'utente. Quest'ultima, apparentemente, presenta l'abbonamento come gratuito, ma in realtà, da un punto di vista economico, la "cessione" dei propri dati personali risulta essere il corrispettivo per la fornitura dei contenuti digitali, che avvicina il rapporto tra *social* e utente alla specie dei rapporti in cui è presente un sinallagma contrattuale. Attualmente i dati personali rivestono un valore economico sempre maggiore e il consumatore/utilizzatore è sempre più portato a "pagare" mediante il consenso al trattamento dei propri dati personali. Peraltro, non è detto che il soggetto sia consapevole che il consenso reso ha un preciso valore economico, che costituisce una controprestazione rispetto al servizio di cui fruisce. (v. A. De Franceschi, *Il «pagamento» mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (cur.), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, 1388 ss.).

9. - A conclusione di questa analisi, è interessante notare che la pronuncia in esame, in riferimento alla tutela dei dati personali, sembra aver voluto risolvere il problema prendendo spunto tanto dall'approccio europeo, quanto da quello impiegato negli Stati Uniti d'America, ponendosi al crocevia di entrambi.

Il primo è caratterizzato dal tentativo di bilanciare lo sviluppo dell'economia digitale con un elevato livello di protezione dei dati personali e trova la sua fonte principale nel Regolamento (UE) 2016/679. Le caratteristiche più rilevanti del GDPR sono: un ampliamento dell'ambito di applicazione territoriale, requisiti avanzati di inventario dei dati, un aumento delle pene, la nomina di un responsabile della protezione dei dati (DPO, dall'inglese "*Data Protection Officer*"), obblighi più ampi e diretti per i responsabili del trattamento dei dati, una segnalazione di violazione dei dati personali più tempestiva, il diritto alla portabilità dei dati, il diritto alla cancellazione (il diritto all'oblio) e un ruolo più rilevante del consenso dell'interessato (v. E. Terolli, *Privacy e protezione dei dati personali Ue vs. Usa. Evoluzioni del diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 1, 2021, 49 ss.).

L'Italia, quale Stato membro dell'Unione europea, applica il GDPR al quale si aggiunge la normativa interna per la tutela dei dati personali. Quest'ultima viene

DPCE online
ISSN: 2037-6677

ricondotta al generale diritto della personalità garantito dall'art. 2 Cost. il quale viene integrato dal Codice Privacy, il d.lgs. 196/2003 che ha creato un corpo organico di disposizioni in questa materia.

Il Codice, attraverso il d.lgs. 101/2018, ha subito una profonda revisione per essere conforme alla disciplina europea (v. G. Finocchiaro, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro cur., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 1-26) e, nonostante questo, conserva ancora alcune disposizioni peculiari che non trovano corrispondenza nel diritto europeo (ad esempio, la protezione dei dati delle persone defunte e l'indicazione dei poteri e compiti del Garante Privacy). Il quadro normativo italiano in questa materia è completato dai provvedimenti e dalle pronunce del Garante, dai codici deontologici e di settore e dal d.lgs. 51/2018 (trasposizione delle Direttiva (UE) 680/2016) disciplinante i trattamenti svolti dall'autorità pubblica per le finalità di prevenzione, accertamento, repressione dei reati o tutela dell'ordine e della sicurezza pubblica (v. G. Bincoletto, *Il diritto alla protezione dei dati: una prospettiva comparata*, in P. Guarda e G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023, 111).

Il secondo approccio discende dalla visione U.S.A. dell'economia, nella quale deve operare la maggior libertà d'impresa possibile. Infatti, negli Stati Uniti la tutela dei dati personali a livello legislativo è limitata e manca un'unica cornice normativa applicabile al settore privato (v. F. Bignami, G. Resta, *Transatlantic privacy regulation: Conflict and cooperation*, in *Law and Contemporary Problems*, Vol. 78, n. 4, 2015, 231-266). La maggior parte delle regole si rivolge all'ambito pubblico, disciplinato dal *Privacy Act* che regola accesso, raccolta, trattamento e divulgazione dei dati personali da parte del governo federale (rapporto pubblico- privato, tra Stato/autorità e cittadino). Sul piano delle fonti di diritto, a livello federale, diversamente dall'art. 16 TFUE che a livello europeo sancisce un generale diritto alla *privacy*, la protezione dei dati personali è riconducibile, seppur indirettamente, al Quarto Emendamento del *Bill of Rights* e ad alcune leggi (*Privacy Act)* (v. C.M. Barrett, *Fbi internet surveillance: the need for a natural rights application of the fourth amendment to insure internet privacy*, 8 Rich. J.L. & Tech 16 (2002), in https://scholarship.richmond.edu/jolt/vol8/iss3/3), mentre nei singoli Stati la disciplina federale è completata dalle leggi statali e dal riconsocimento del diritto alla *privacy* nelle Costituzioni. Queste caratteristiche concorrono a formare una disciplina frammentata e settoriale, spesso frutto di situazioni emergenziali nella quale un ruolo rilevante viene svolto dal *case law* che interpreta le fonti scritte per garantire la protezione delle informazioni personali.

Peraltro, negli Stati Uniti non sono presenti autorità paragonabili al garante europeo (European Data Protection Board – EDPB) e a quelli degli Stati membri, manca infatti una specifica agenzia federale dedicata alla tutela dei dati personali (v. G. Bincoletto, *Il diritto alla privacy negli Stati Uniti d'America*, in P. Guarda e G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023, 35). La *privacy* viene considerata, più che un diritto fondamentale, un diritto del consumatore da bilanciare con le esigenze delle imprese con la conseguenza che alcune delle funzioni tipiche delle autorità di controllo europee vengono svolte dalla *Federal Trade Commission*, un'agenzia deputata alla tutela dei consumatori.

Sul punto la dottrina si è divisa fra chi sostiene che l'approccio americano, meno precauzionale e più orientato alla libertà economica, possa essere una soluzione al rapido progresso tecnologico favorendone l'espansione (v. T.E. Frosini, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, fasc. 1, 2022, 280 ss.) e chi ritiene che l'approccio europeo, assicurando il più alto livello di protezione a livello globale, possa influenzare positivamente il panorama della *privacy* anche oltreoceano ed in Cina (v. A. Bradford, *The Brussels Effect: How the European Union Rules the World*, in *Oxford University Press*, New York, 2020, 132 ss.; E. Terolli, *Privacy e protezione dei dati*

personali Ue vs. Usa. Evoluzioni del diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II", in *Diritto dell'Informazione e dell'Informatica*, fasc. 1, 2021, 49 ss.).

Nella pronuncia della CGUE si ammette che un'autorità che tutela la concorrenza, e quindi – in una certa prospettiva – il mercato e i consumatori, possa valutare il rispetto del GDPR da parte di un'impresa che si ritiene realizzi un abuso di posizione dominante nel mercato per aver violato lo stesso Regolamento. Questa decisione, come è facile capire, avvicina molto l'approccio europeo, finora immune da una simile azione, a quello statunitense.

La scelta della Corte dimostra come ci possa essere un terzo cammino percorribile fra i due approcci. I giudici, pur ponendo sempre come obbiettivo il più alto livello di protezione per l'individuo a discapito della libertà economica d'impresa, hanno saputo riconoscere i pregi del modello americano (l'impiego di un'autorità della concorrenza per la tutela dei dati personali) e farli propri nel rispetto della vigente disciplina europea, determinando una specie di "ibridazione dei due modelli".

In conclusione, si può dire che l'approccio europeo alla tematica della tutela dei dati personali è senza dubbio quello che, ponendo al centro la persona, realizza la più penetrante tutela attualmente possibile. Eppure, non si può nascondere che grandi sfide siano già presenti e richiedano un intervento delle Istituzioni europee secondo un modello che, bilanciando entrambi gli interessi in gioco (economici per le imprese e personali per l'individuo), riesca a introdurre più principi generali e meno normative di dettaglio (v. T.E. Frosini, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, fasc. 1, 2022, 281 ss.). Privilegiare una normativa fatta di principi generali piuttosto che di regole di dettaglio, sarebbe pregevole perché i primi sarebbero più generici e flessibili, capaci di adattarsi a tutte le evoluzioni tecnologiche, mentre le seconde sarebbero più stringenti e chiare in prima battuta ma difficilmente resterebbero al passo con le continue innovazioni. Ad una simile tecnica legislativa dovrebbe seguire un rafforzamento del ruolo dei giudici, chiamati a rendere un'interpretazione estensiva e adeguatrice dei principi generali (di nuova formulazione e/o riscoperti sulla base di valori già esistenti), e delle autorità indipendenti sempre più coinvolte in settori apparentemente non di loro competenza (come nel caso affrontato dalla CGUE).

Un simile epilogo, oltre che idoneo a creare un terreno favorevole per le attività di ricerca e sviluppo (ad esempio, assumere decisioni imparziali mediante algoritmi, accompagnare le scelte dell'uomo e migliorare il benessere generale anche sotto il profilo della salute attraverso l'impiego dell'*Artificial Intelligence*), sarebbe necessario a fronte della travolgente evoluzione tecnologica che rende facilmente obsolete le norme di dettaglio. Da qui la necessità di adottare innovative tecniche legislative che abbiano il pregio di essere tempestive.

Alessandro Giovanni Masotti
Dipartimento di Scienze Giuridiche
Università degli Studi di Udine
masotti.alessandrogiovanni@spes.uniud.it