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

OSSERVATORIO SULLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA N. 3/2023

1. LA SENTENZA *META PLATFORMS*: RIFLESSIONI IN MATERIA DI VALORE DEI DATI E LIBERA ESPRESSIONE DEL CONSENSO

1. Introduzione

Il 4 luglio 2023 la Corte di giustizia si è pronunciata in via pregiudiziale sul caso *Meta Platforms Inc.* c. *Bundeskartellamt*, relativo alla possibilità per le autorità nazionali della concorrenza di controllare, nell'ambito dell'esercizio delle loro competenze, la conformità di un trattamento di dati personali alle condizioni stabilite dal regolamento 2016/679.

La sentenza è stata accolta con entusiasmo dal Bundeskartellamt, a giudizio del quale essa avrà effetti importanti sui modelli di *business* dell'economia dei dati (qui). Tuttavia, già nei primi commenti pubblicati, è stato correttamente sottolineato come, sebbene la pronuncia in questione abbia il pregio di far chiarezza sulle interazioni tra protezione dei dati e concorrenza nonché sull'incompatibilità con il GDPR della politica di Meta sull'utilizzo dei dati personali (qui), la stessa lasci ancora aperti numerosi interrogativi, relativamente ai quali i giudici del Kirchberg avrebbero potuto assumere una posizione meno sfumata (qui).

Il giudice dell'Unione, nella sostanza, ha confermato la posizione assunta dall'avvocato generale Rantos nelle sue conclusioni del 20 settembre scorso, di cui ci siamo già occupati in quest'osservatorio (qui). Pertanto, nel presente lavoro non si tornerà sugli aspetti di carattere generale relative ai rapporti tra concorrenza, tutela dei dati personali e protezione dei consumatori, per le quali si rinvia al precedente commento, ma ci si soffermerà sui profili specifici affrontati in maniera più articolata dalla Corte, che sollevano alcuni spunti di riflessione.

2. I dati nel contesto della concorrenza

Solo per ragioni di chiarezza espositiva, ci si limita a ricordare che la vicenda trae origine da un procedimento avviato dal Bundeskartellamt nei confronti di Meta Platforms, Meta Platforms Ireland e Facebook Deutschland, in esito al quale l'Autorità federale garante della concorrenza ha vietato alle dette società di subordinare, nelle

condizioni generali, l'uso del *social network* Facebook da parte di utenti privati al trattamento dei loro dati c.d. *off* Facebook. Secondo il Bundeskartellamt, infatti, il trattamento dei dati degli utenti interessati, quale previsto dalle condizioni generali e attuato da Meta Platforms Ireland, costituiva uno sfruttamento abusivo della posizione dominante di tale società sul mercato dei *social network* per gli utenti privati tedeschi. A seguito di tale decisione, Meta Platforms ha avviato un'azione giudiziaria, nell'ambito della quale il Tribunale superiore del Land di Düsseldorf ha posto alcuni quesiti pregiudiziali alla Corte. In particolare, l'Oberlandesgericht Düsseldorf ha domandato alla Corte se sia compatibile con il RGPD che un'autorità garante della concorrenza constati, nell'ambito dell'esercizio di un controllo in materia di abuso di posizione dominante nei confronti di una determinata impresa, le condizioni contrattuali alla luce delle quali quest'ultima opera il trattamento dei dati personali dei suoi utenti.

In tal senso, confermando quanto suggerito dall'avvocato generale Rantos, il giudice dell'Unione, in termini generali, ha stabilito che un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, che le condizioni generali d'uso seguite dall'impresa relativamente al trattamento dei dati personali e alla loro applicazione non sono conformi a detto regolamento, qualora la constatazione sia necessaria per accertare l'esistenza dell'abuso. A tal riguardo, ha precisato che la circostanza che l'operatore di un *social network* occupi una posizione dominante nel relativo mercato non osta, di per sé, a che gli utenti di tale *social network* possano validamente acconsentire al trattamento dei loro dati personali come effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta all'operatore dimostrare.

Da questo punto di vista, è chiaro che la posizione assunta dalla Corte si ponga nell'ottica di una maggiore tutela degli utenti, senza creare particolari rischi di sovrapposizione di competenze tra autorità di controllo. D'altronde, è inevitabile che in un sistema economico basato prevalentemente sullo sfruttamento dei dati personali, qual è il mercato digitale e, soprattutto, quello dei *social network*, gli stessi acquisiscano un rilievo di primaria importanza anche in termini di concorrenza tra le imprese e, in particolare, in sede di esame di un abuso di posizione dominante. Tra l'altro, si deve tenere in considerazione che è proprio a causa della sua natura *data driven* che il capitalismo delle piattaforme digitali tende a rappresentare un fenomeno strutturalmente anticoncorrenziale, che manifesta una propensione alla produzione di monopoli [così F. CAGGIA, *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del consenso rafforzato*, in M. D'AURIA (a cura di) *I problemi dell'informazione nel diritto civile oggi. Studi in onore di Vincenzo Cuffaro*, Roma, 2022, p. 421], per cui creare degli steccati troppo rigidi tra la disciplina sulla protezione dei dati personali e il diritto della concorrenza sarebbe controproducente in termini di tutela dei consumatori. In tale contesto, l'azione di controllo delle differenti autorità non dev'essere interpretata in chiave di invasione delle reciproche sfere di competenza, ma in un'ottica di complementarietà, anche perché, come rilevato dalla Corte, quando un'autorità garante della concorrenza rileva una violazione del RGPD, essa, proprio per non sostituirsi all'autorità di controllo istituita ai sensi di

tale regolamento, non accerta l'applicazione né assicura il rispetto del RGPD «al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di facilitare la libera circolazione di questi ultimi all'interno dell'Unione […] [ma si limita] a rilevare la non conformità al RGPD di un trattamento di dati al solo scopo di constatare un abuso di posizione dominante ed imponendo misure volte a far cessare tale abuso sul fondamento di una base giuridica derivante dal diritto della concorrenza […] [Pertanto,] detta autorità non esercita alcuno dei compiti di cui all'articolo 57 [del RGPD], né fa uso dei poteri riservati all'autorità di controllo in forza dell'articolo 58 del medesimo regolamento» (punto 49). In quest'ottica, escludere le autorità garanti della concorrenza da qualsiasi forma di controllo rispetto al trattamento dei dati comporterebbe una riduzione del livello di tutela dei consumatori ed equivarrebbe ad ignorare un fenomeno ormai consolidato, cioè quello dell'affermazione di un sistema economico legato allo sfruttamento dei dati (sulla *Personal Data Economy*, cfr. S.-A. ELVY, *Paying for Privacy and the Personal Data Economy*, in *Columbia Law Review*, pp. 1369-1459).

Naturalmente, un sistema di controllo così articolato, al fine di evitare difformità interpretative, richiede uno stretto coordinamento tra le autorità operanti nei diversi settori di riferimento. Su questo punto, infatti, si era già espresso l'avvocato generale Rantos, ipotizzando un meccanismo basato sul principio di leale cooperazione, in cui sussisterebbe sempre una prevalenza dell'autorità competente ai sensi del RGPD e un obbligo di conformità alle sue decisioni (cfr. Conclusioni dell'avvocato generale Athanasios Rantos presentate il 20 settembre 2022, causa C-252/21, *Meta Platforms Inc., Meta Platforms Ireland Limited, Facebook Deutschland GmbH*, c. *Bundeskartellamt*, ECLI:EU:C:2022:704, parr. 30-31). Partendo da quel modello, quindi, il giudice dell'Unione ha definito in maniera dettagliata l'articolazione dei rapporti tra le diverse autorità, adottando, però un approccio più flessibile, che enfatizza la cooperazione istituzionale piuttosto che la fungibilità (così G. DE GREGORIO, G. FINOCCHIARO, O. POLLICINO, *Alternativa al compenso per garantire libertà e diritti nell'era digitale*, in *Il Sole 24 ore*, 7 luglio 2023, p. 38). La Corte, infatti, ha affermato che «qualora, nell'ambito dell'esame diretto a constatare un abuso di posizione dominante ai sensi dell'articolo 102 TFUE da parte di un'impresa, un'autorità nazionale garante della concorrenza ritenga che sia necessario esaminare la conformità di un comportamento di tale impresa alle disposizioni del RGPD, detta autorità deve verificare se tale comportamento o un comportamento simile sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o 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). Nel caso, invece, in cui non sia presente una precedente decisione dell'autorità sui dati personali, l'autorità garante della concorrenza, se nutre dei dubbi sull'interpretazione delle norme del RGPD, deve consultare l'autorità istituita ai sensi di quest'ultimo e chiederne la cooperazione, al fine di fugare i propri dubbi. Anche in questo caso, quindi, si tratta di una collaborazione fondata sul principio di leale cooperazione, che non pone le due autorità su un piano gerarchico. In tal senso, vale la pena di sottolineare che, a giudizio della Corte, l'autorità di controllo sui dati personali,

una volta ricevuta la richiesta di informazioni o di cooperazione, deve rispondere entro un termine ragionevole, comunicando tutte le informazioni di cui dispone utili a fugare i dubbi anzidetti (punto 58). Ovviamente, in assenza di risposta entro un termine ragionevole, l'autorità nazionale può proseguire la propria indagine.

3. La base giuridica del trattamento dei dati

Altro aspetto di particolare interesse su cui si è concentrata la Corte è quello relativo alla base giuridica a cui si può ricorrere per trattare i dati ai fini di pubblicità mirate. In tal senso, la posizione assunta tendenzialmente dalle piattaforme digitali è quella secondo cui un simile trattamento possa trovare fondamento nell'art. 6, par. 1, lett. f), cioè il legittimo interesse del titolare del trattamento o di terzi. Tale tesi troverebbe sostegno nel considerando quarantasette del RGPD, in cui si afferma che può essere considerato legittimo interesse trattare dati personali per finalità di *marketing* diretto.

Al riguardo, prima di entrare nel merito di quanto deciso dalla Corte, vale la pena di ricordare che il richiamo al *marketing* diretto di cui al considerando quarantasette, che non figurava nella proposta iniziale di RGPD ed è stato inserito solo in fase di prima lettura, si qualifica di per sé come una previsione caratterizzata per la sua delicatezza, stante il costante bilanciamento richiesto con gli interessi, i diritti e le libertà del soggetto interessato. Un bilanciamento che non può essere improntato su fattori di principio, ma che deve essere adattato alle caratteristiche particolari del singolo caso, poiché è essenziale valutare, di volta in volta, quali siano le ragionevoli aspettative dell'interessato, nonché la portata del trattamento di cui trattasi (G. PROIETTI, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati*, in *Contratto e impresa*, 2022, p. 891). In tal senso, la Corte ha da tempo ribadito che l'attuazione della clausola di cui all'art. 6, par. 1), lett. f) del RGPD non è automatica, ma è subordinata al rispetto di tre condizioni cumulative, vale a dire, in primo luogo, il perseguimento di un legittimo interesse del titolare del trattamento o di terzi; in secondo luogo, la necessità del trattamento dei dati personali per la realizzazione del legittimo interesse perseguito e, in terzo luogo, la condizione che gli interessi o i diritti e le libertà fondamentali dell'interessato dalla tutela dei dati non prevalgano sul legittimo interesse del responsabile del trattamento o di terzi [Sentenza della Corte (Seconda Sezione) del 4 maggio 2017, causa C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* c. *Rīgas pašvaldības SIA "Rīgas satiksme"*, ECLI:EU:C:2017:336, punto 28). Tra l'altro, ad ulteriore testimonianza del carattere restrittivo della disposizione in questione, giova ricordare che quest'ultima va letta insieme a quanto affermato nel considerando settanta del RGPD, ove si precisa che «qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione».

Invero, l'applicabilità dell'art. 6, par. 1, lett. f) del RGPD ai *social network*, in termini simili a quanto avvenuto nel caso di specie, era già stato oggetto d'attenzione da parte del

Garante per la protezione dei dati personali. Quest'ultimo, nel luglio del 2022, aveva adottato un provvedimento contro Tik Tok, a seguito della decisione di quest'ultimo di modificare la propria *privacy policy* al fine di ricorrere al legittimo interesse del titolare, e non più al consenso dell'utente, quale base giuridica per il trattamento dei dati degli utenti per finalità di *marketing* diretto. Tale comportamento, a giudizio dell'Autorità, era contrario alla direttiva *e-privacy* per diverse ragioni, in particolare perché non era stato esplicitato quale fosse il legittimo interesse perseguito dal titolare e da terzi (i *partner* pubblicitari); non era stato precisato se il trattamento riguardasse anche i dati di carattere particolare; il *test* di bilanciamento era stato indicato in modo generico e insufficiente a consentire un'adeguata valutazione della sua correttezza alla luce dei criteri forniti dalla giurisprudenza della Corte di giustizia dell'Unione europea.

Nel caso in esame, Meta Platforms, nel giustificare il ricorso al legittimo interesse, aveva fatto riferimento alla personalizzazione della pubblicità, alla sicurezza del *network*, al miglioramento del prodotto, all'informazione delle autorità competenti per l'esercizio dell'azione penale e per l'esecuzione di pene, al fatto che l'utente sia un minorenne, alla ricerca e all'innovazione per finalità sociali nonché all'offerta, destinata agli inserzionisti e ad altri *partner* professionali, di servizi di comunicazione commerciale destinati all'utente e di strumenti di analisi che consentano a questi ultimi di valutare le loro prestazioni. Per quanto riguarda, nello specifico, la profilazione a fini pubblicitari, la Corte ha stabilito che «malgrado la gratuità dei servizi di un *social network* quale Facebook, l'utente di quest'ultimo non può ragionevolmente attendersi che, senza il suo consenso, l'operatore di tale *social network* tratti i suoi dati personali a fini di personalizzazione della pubblicità. In tali circostanze, si deve ritenere che i diritti fondamentali e gli interessi di tale utente prevalgano sull'interesse dell'operatore a tale personalizzazione della pubblicità mediante la quale egli finanzia la sua attività, cosicché il trattamento da quest'ultimo effettuato a tali fini non può rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD» (punto 117). Una simile valutazione sarebbe rafforzata dal fatto che «il trattamento in causa nel procedimento principale è particolarmente esteso, giacché verte su dati potenzialmente illimitati e ha un notevole impatto sull'utente, di cui Meta Platforms Ireland controlla gran parte, se non la quasi totalità, delle attività online, il che può suscitare in quest'ultimo la sensazione di una continua sorveglianza della sua vita privata» (punto 118).

In questo modo, il giudice dell'Unione ha chiarito un principio di primaria importanza, cioè che il carattere formalmente gratuito dei servizi digitali, non solo i *social network*, non può legittimare la compressione dei diritti fondamentali, non solo in termini di tutela dei dati personali, ma anche di salvaguardia della vita privata degli utenti. Giova, infatti, ricordare che, secondo la sistematica della Carta dei diritti fondamentali, i due diritti non sono perfettamente sovrapponibili. In tal senso, nel caso di specie è emerso come la base giuridica del trattamento dei dati personali degli utenti debba essere valutata anche alla luce delle conseguenze che tale trattamento ha sulla vita privata delle persone. Per quanto riguarda il *marketing* diretto e le pubblicità mirate, tra l'altro, si potrebbe anche aggiungere che queste ultime, piuttosto che costituire uno strumento a vantaggio dei consumatori, appaiono spesso come fonte di molestie quotidiane nei loro confronti, il

che determina una violazione della vita privata al pari del senso di sorveglianza generato dal trattamento massiccio di dati personali.

Dello stesso tenore restrittivo è anche la posizione della Corte in merito alla clausola di cui all'art. 6, par. 1, lett. b) del RGPD, relativamente alla quale il giudice dell'Unione ha sottolineato che, affinché un trattamento di dati personali sia considerato necessario all'esecuzione di un contratto, ai sensi di tale disposizione, esso deve essere oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato. Ciò comporta che il responsabile del trattamento dev'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 (punto 98). In tal senso, la Corte ha stabilito che «per quanto riguarda, in primo luogo, la giustificazione relativa alla personalizzazione dei contenuti, occorre rilevare che, sebbene tale personalizzazione sia utile per l'utente, in quanto gli consente in particolare di visualizzare un contenuto in larga misura corrispondente ai suoi interessi, resta il fatto che, salvo verifica del giudice del rinvio, la personalizzazione dei contenuti non appare necessaria per offrire a tale utente i servizi del social network online. Tali servizi possono, eventualmente, essergli forniti sotto forma di un'alternativa equivalente che non implichi tale personalizzazione, che non è dunque oggettivamente indispensabile per una finalità che faccia parte integrante di detti servizi».

Ora, l'approccio utilizzato dalla Corte, da un lato, ha il pregio di riorientare il modello di *business* utilizzato dalle piattaforme *social* verso un sistema più attento alla tutela degli utenti, smontando definitivamente l'idea che l'essere "bersagliati" da messaggi pubblicitari ritagliati sui gusti e sugli interessi desunti dalle attività *online* possa costituire un interesse imprescindibile degli stessi e ponendo l'attenzione non solo sulla tutela dei dati personali, ma anche della vita privata. Dall'altro lato, però, resta da valutare quanto la pronuncia in questione possa concretamente impattare sulle dinamiche commerciali che si sono consolidate nel settore di riferimento. Nell'impossibilità di ricorrere alle suddette basi giuridiche, infatti, il trattamento dei dati sarà legittimo solo in presenza del consenso dell'interessato, cioè uno strumento che ha dimostrato scarsa efficacia nell'ecosistema digitale. È, infatti, ormai assodato che il livello di libertà e consapevolezza del consenso prestato dagli utenti sia insoddisfacente, ancor di più di fronte a grandi piattaforme (sul consenso nel mercato digitale, si consenta di rimandare a F. BATTAGLIA, *Il consumatore digitale nel diritto dell'Unione europea*, Napoli, 2023). In tal senso, nel caso in esame, la Corte ha giustamente rilevato come la circostanza che l'operatore di un *social network*, in quanto titolare del trattamento, occupi una posizione dominante sul mercato di riferimento, sebbene non osti, di per sé, a che gli utenti prestino liberamente il proprio consenso, «deve essere presa in considerazione 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, come indicato dal considerando 42 del RGPD» (punto 148).

In tal senso, nemmeno il *Digital Markets Act* (DMA) sembra offrire soluzioni efficaci, poiché, per quanto concerne il trattamento dei dati da parte dei *gatekeeper* prevede una serie di obblighi che non hanno un carattere particolarmente innovativo, ma che

sembrano desunti da precedenti desumibili dalla giurisprudenza della Corte ovvero dalla prassi della Commissione europea (cfr. G. CONTALDI, *Il regolamento 2022/1925 e la tutela della privacy online*, in *Quaderni AISDUE, Serie speciale, Atti del Convegno "Ambiente, digitale, economia: l'Unione europea verso il 2030"*, Napoli, 2023, p. 130). Anche con riferimento alla libera prestazione del consenso, le novità introdotte sono piuttosto timide e confinate nei considerando del regolamento. In particolare, il considerando trentasette, anche a seguito delle sollecitazioni presentate dal Garante europeo per la protezione dei dati nel corso dell'*iter* legislativo, afferma: «quando richiede il consenso, il *gatekeeper* dovrebbe presentare in modo proattivo all'utente finale una soluzione intuitiva per prestare, modificare o revocare il consenso in maniera esplicita, chiara e semplice. In particolare, il consenso dovrebbe essere prestato mediante dichiarazione o azione positiva inequivocabile con cui l'utente finale esprime una manifestazione di volontà libera, specifica, informata e inequivocabile, secondo la definizione di cui al regolamento (UE) 2016/679. Nel momento in cui presta il consenso, e soltanto ove pertinente, l'utente finale dovrebbe essere informato del fatto che non prestare il consenso può determinare un'offerta meno personalizzata ma che, per tutto il resto, il servizio di piattaforma di base resterà invariato e che nessuna funzionalità sarà rimossa». Lo stesso considerando, infatti, prevede che l'alternativa meno personalizzata non dovrebbe essere differente o di qualità inferiore rispetto al servizio fornito agli utenti finali che prestano il proprio consenso, a meno che il deterioramento della qualità non sia una conseguenza diretta del fatto che il *gatekeepe*r non possa procedere al trattamento dei dati personali o fare accedere con registrazione gli utenti finali a un servizio. Tuttavia, quanto indicato nel considerando in parola, non è stato tradotto in obblighi concreti nella parte dispositiva del DMA.

4. Il valore dei dati

Un aspetto, infine, di particolare rilievo che emerge dalla sentenza in esame è quello relativo al valore dei dati e alla possibilità che questi possano costituire una forma di controprestazione. Su questo punto la sentenza non si sofferma in maniera particolare, ma è presente un passaggio di rilievo, in cui il giudice dell'Unione afferma che «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» (punto 150, corsivo aggiunto). Evidentemente, quindi, se i dati possono costituire un'alternativa ad "un adeguato corrispettivo", essi hanno una funzione e una natura analoga a quest'ultimo.

D'altronde, questa è la strada verso cui sembra muovere il legislatore dell'Unione, sebbene in maniera timida e non sempre coerente, il che ha acceso un ampio e vivace dibattito in dottrina (cfr. *ex multis*, V. RICCIUTO, C. SOLINAS (a cura di), *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali*, Milano, 2022; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021). Come noto, infatti, l'art. 3, par. 1,

della direttiva 2019/770, afferma che essa «si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico». Tuttavia, la stessa direttiva, al considerando ventiquattro, riconosce «appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce». I dati, quindi, possono costituire la controprestazione di un servizio, ma devono restare entro i confini della tutela della personalità, il che implicherebbe la loro indisponibilità, imprescrittibilità e assolutezza. Tra l'altro, vale la pena di ricordare che la versione definitiva della disposizione in questione è frutto anche di una revisione di quella originale, che sembrava equiparare in maniera più diretta il pagamento in denaro e la controprestazione attraverso cessione di dati, soprattutto a seguito delle perplessità espresse dal Garante europeo per la protezione dei dati (cfr. I. SPEZIALE, *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione*, in *Contratto e impresa*, 2021, pp. 616-617).

Lo stesso approccio utilizzato nella direttiva 2019/770 è stato seguito nella direttiva 2019/2161, c.d. direttiva modernizzazione, la quale ha ampliato l'ambito di applicazione della direttiva 2011/83 ai contratti di servizi digitali nel cui ambito il consumatore fornisce al professionista dati personali e non paga alcun prezzo. Anche in questo caso, però, non vengono affrontate e regolate le problematiche che ne conseguono.

La sentenza in esame, quindi, si pone in continuità con la esigua legislazione vigente in materia, non solo in quanto sembra riconoscere il valore economico dei dati, ma anche perché mantiene lo stesso approccio ambiguo delle norme esaminate, il che pone una serie di problematiche che il legislatore dovrà necessariamente affrontare. Tra queste, giusto per richiamarne le più evidenti, c'è il sistema attraverso il quale possa essere definito, anche orientativamente, il valore dei dati nonché il modo in cui gli stessi possano essere utilizzati dagli utenti.

Ciò che appare indubbio è che la sentenza abbia definitivamente aperto ad una pratica che si sta diffondendo di recente, cioè quella dei *cookie paywalls*, rispetto alla quale hanno già indagato talune autorità nazionali, giungendo anche a soluzioni di tenore opposto rispetto a quelle della Corte; sulla questione ha aperto un fascicolo pure il Garante per la protezione dei dati personali. Anche in questo caso, però, resta da vedere in che termini il pagamento di un prezzo possa costituire un'alternativa al consenso ai fini dell'accesso ad un sito internet. Su questo punto sarà interessante vedere se e come la materia sarà regolata dal regolamento *e-privacy*, ancora in fase di proposta.

5. Considerazioni conclusive

In definitiva, la sentenza *Meta Platforms* chiarisce tre punti essenziali, rispetto ai quali, però, si aprono numerosi interrogativi.

Il primo è che le autorità le autorità garanti della concorrenza di uno Stato membro possono constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, se le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione siano conformi al

RGPD, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso. Ciò, naturalmente, pone una serie di problemi, non solo in termini di sovrapposizione delle discipline giuridiche, ma anche di cooperazione tra diverse autorità. Su tale aspetto, il giudice dell'Unione ha indicato una soluzione, fondata sul principio di leale cooperazione, che resta da vedere come sarà attuata in pratica.

Il secondo punto è che, nell'ambito dei *social network*, il trattamento di dati raccolti dalle attività dell'utente in siti terzi difficilmente può risultare legittimo in assenza del consenso dell'interessato. Si è visto, infatti, come, secondo l'interpretazione restrittiva adottata dalla Corte, difficilmente i *social networks* potranno ricorrere ad altre basi giuridiche di cui all'art. 6 del RGPD. Resta aperta, però, la problematica della scarsa efficacia del consenso nell'ecosistema digitale.

Infine, il terzo aspetto è quello del valore dei dati quale corrispettivo di una prestazione. Su questo punto la sentenza segue lo stesso approccio presente nelle direttive 2019/770 e 2019/2161, aprendo però alla possibilità di prassi come quella dei *cookie paywalls*. Anche in questo caso, tuttavia, non hanno trovato soluzione i complessi interrogativi che la dottrina discute da tempo, *in primis* in materia di quantificazione di tale valore.

FRANCESCO BATTAGLIA