

Data economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata

Guido d'Ippolito

Corte di giustizia, 4 luglio 2023, C-252/21, *Meta c. Bundeskartellamt*

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'art. 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi al regolamento (UE) 2016/679, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso. Alla luce dell'obbligo di leale cooperazione, l'autorità nazionale garante della concorrenza non può discostarsi da una decisione dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila competente che riguardi tali condizioni generali o condizioni generali analoghe. Laddove nutra dubbi sulla portata di tale decisione, o dette condizioni siano, al contempo, oggetto di esame da parte di tali autorità, o, ancora in assenza di un'indagine o di una decisione di dette autorità, ritenga che le condizioni in questione non siano conformi al regolamento (UE) 2016/679, l'autorità nazionale garante della concorrenza deve consultare dette autorità di controllo. 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.

Il trattamento di dati personali effettuato da un operatore di un social network online può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.

Il trattamento di dati personali effettuato da un operatore di un social network online può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perse-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

guito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse del titolare del trattamento o di terzi.

La circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire al trattamento dei loro dati personali 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 a detto operatore dimostrare.

Sommario

1. Introduzione. – 2. Il fatto. – 3. Le considerazioni della Corte. – 3.1. Sulla valutazione incidentale del GDPR da parte di un'autorità per la concorrenza. – 3.2. Sull'applicazione delle norme del GDPR. – 3.3. Sul contratto e il consenso come base giuridica di alcuni trattamenti tra cui la pubblicità personalizzata. – 4. Conclusioni.

Keywords

abuso di posizione dominante - contratto e consenso - pubblicità personalizzata - autorità indipendenti - data economy.

1. Introduzione

La regolazione delle piattaforme digitali e della c.d. “*data economy*” è un aspetto centrale di quello che è stato definito “costituzionalismo digitale”¹. L'enorme disponibilità di informazioni, la loro facile reperibilità sulle piattaforme di intrattenimento e *social networking*, insieme allo sviluppo tecnologico che ha trasformato gli algoritmi in complessi “sistemi di intelligenza artificiale”, ha permesso la nascita di modelli di business fondati sulla remunerazione dell'attenzione e del tempo “speso” dagli utenti sulle piattaforme digitali; piattaforme divenute sempre più potenti e titolari di un'influenza non solo economica ma quasi “sociale”².

¹ Per una disamina sugli autori e le teorie alla base del concetto di costituzionalismo digitale si veda O. Pollicino, *Potere digitale* (voce), in *Enciclopedia del diritto*, Milano, V, 2023, 410 ss.

² P. Stanzone (a cura di), *I “poteri privati” delle piattaforme e le nuove frontiere della privacy*, Torino, 2022; L. Bolognini (a cura di), *Privacy e libero mercato digitale. Convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Milano, 2021; E. Cremona, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023; Con riferimento ai rapporti “*Platform-to-Business*” quale particolare forma di asimmetria nei rapporti tra imprese, si veda F. Ruggeri, *Poteri privati e mercati digitali. Modalità di esercizio e strumenti di controllo*, Roma, 2023, disponibile in *open access* sul [sito dell'editore](#); S. Martinelli, *I contratti nella platform economy. Ruoli e responsabilità delle piattaforme*, Torino, 2023; A. Iannotti della Valle, *Le regole di Internet tra poteri pubblici e privati. Tutela dei diritti e ruolo dell'antitrust in una prospettiva costituzionale*, Napoli, 2023.

In quelli che sono stati definiti “mercati dell’attenzione”³ la risorsa principale e contesa dai fornitori di servizi digitali sono le informazioni e i dati personali degli utenti; il modo per ottenerli è catturare la loro attenzione: più questi sono attratti dai servizi offerti più resteranno sulla piattaforma e più l’interazione con quest’ultima produrrà informazioni di rilievo commerciale come i gusti, gli interessi, le abitudini, la capacità di spesa o gli orientamenti di consumo dell’utente nel tempo, ecc. Il rovescio della medaglia di questo sistema è, come rilevato in letteratura⁴, un sistema basato sul tracciamento e monitoraggio continuo dell’attività degli utenti su larga scala.

Quest’incetta di dati e informazioni è alla base dei principali modelli di business nei mercati digitali. Dal punto di vista giuridico ciò conduce ad almeno due temi: quello ancora tutt’altro che risolto della monetizzazione e commercializzazione dei dati personali⁵; quello della regolazione della pubblicità online (*display advertising*), in particolare nella sua forma automatizzata e basata su profilazione degli utenti, ossia la pubblicità personalizzata, profilata o, anche, “targettizzata”⁶.

Tali temi sono oggetto di esame da parte del legislatore europeo, nell’ambito della corposa regolazione sulla “*European Strategy for data*”, e sempre più al centro di pronunce dalle autorità giurisdizionali e amministrative dei vari Stati membri.

In tale contesto si inserisce la Corte di giustizia dell’UE con la sentenza del 4 luglio 2023.

Quest’ultima acquisisce importanza non solo per le tematiche di particolare attualità e rilievo sulle quali la Corte è stata chiamata a pronunciarsi, ma anche per lo straordinario raggio di azione della sua analisi.

A partire dal rapporto tra la normativa in materia di protezione dei dati personali e quella a tutela della concorrenza, la Corte esamina le norme del regolamento (UE) 2016/679 (in seguito, anche, “Regolamento” o “GDPR”) fornendo indicazioni alcune delle quali costituenti l’esito e il riconoscimento di riflessioni già avviate, altre invece, risultano più innovative e si pongono come preziosa regolamentazione del settore.

³ Y.N. Harari, *21 lezioni per il XXI secolo*, Milano, 2018, 116.

⁴ Sebbene la letteratura e i report, anche di istituzioni e autorità di controllo, sul tema siano sempre più abbondanti, basti qui richiamare S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell’umanità nell’era dei nuovi poteri*, Roma, 2019. La stessa Corte di giustizia in commento sembrerebbe riprendere tale concetto al punto 118 laddove afferma che trattamenti particolarmente “estesivi” hanno un notevole impatto sull’utente tanto da «suscitare in quest’ultimo la sensazione di una continua sorveglianza della sua vita privata».

⁵ Tra la sempre più corposa dottrina: E. Cremona–F. Laviola–V. Pagnanelli (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022; V. Ricciuto, *Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in *Rivista di diritto dell’impresa*, 2, 2021, 261 ss.; Id., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, e A. De Franceschi, *Il “pagamento” mediante dati personali*, entrambi in V. Cuffaro–R. D’Orazio–V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 23 ss. e 1389 ss.; G. Malgieri–B. Custers, *Pricing privacy: the right to know the value of your personal data*, in *Computer Law & Security Review*, 2017.

⁶ Per una generale analisi del trattamento di profilazione e la disciplina della pubblicità personalizzata online sia consentito rinviare a: G. d’Ippolito, *Profilazione e pubblicità targettizzata online. Real-Time Bidding e behavioural advertising*, Napoli, 2021.

2. Il fatto

Con sentenza del 4 luglio 2023 la Corte di giustizia si occupa della competenza di un'autorità nazionale per la concorrenza ad esaminare i comportamenti di un'impresa alla luce di talune disposizioni del Regolamento, soffermandosi anche sull'applicazione di alcuni istituti: come il rapporto tra il contratto e il consenso quale base giuridica di alcuni trattamenti.

Il caso origina dall'istruttoria dell'autorità federale tedesca garante della concorrenza (Bundeskartellamt) che ha portato al divieto per Meta di trattare taluni dati personali sulla base delle condizioni generali di utilizzo del social network Facebook.

In particolare, l'oggetto della contestazione del Bundeskartellamt è la raccolta e il trattamento dei dati esterni alla piattaforma, i dati cc.dd. "Off Facebook": derivanti dalla consultazione di pagine Internet e applicazioni di terzi collegate al servizio Facebook o riguardanti l'utilizzo degli altri servizi appartenenti al gruppo Meta come Instagram, WhatsApp o Oculus.

Per la raccolta e il trattamento dei dati Off Facebook Meta utilizzava quale base giuridica il contratto *ex art. 6, par. 1, lett. b)*, del Regolamento.

Poiché Meta considerava il trattamento di tali dati come necessario al servizio (Facebook) offerto all'utente ne disciplinava la raccolta e l'utilizzo all'interno delle sue condizioni contrattuali⁷. Essendo questo un documento che l'utente può solo accettare o rifiutare, secondo il noto approccio "*take it or leave it*", la conseguenza pratica è che il trattamento di dati ulteriori a quelli prodotti dalla piattaforma Facebook è sottratto ad una specifica valutazione e autorizzazione dell'utente. Semplificando, per il trattamento di questi dati non è richiesto un autonomo consenso agli utenti/interessati del trattamento⁸.

Il Bundeskartellamt, nel ritenere il trattamento dei dati Off Facebook non conforme al GDPR, ha concluso che ciò costituisse uno sfruttamento abusivo della posizione dominante di Meta sul mercato dei social network online.

Sicché, con decisione del 6 febbraio 2019, ha vietato a Meta di subordinare l'uso del social network Facebook, tramite condizioni generali di contratto, al trattamento dei dati Off Facebook e di procedere, senza il consenso degli utenti, al trattamento di tali dati. Inoltre, ha ordinato di adeguare le condizioni generali in modo che 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, chiarendo che tale consenso non è valido se inteso come una condizione per l'utilizzo del social

⁷ Sui presupposti per il ricorso al contratto come fondamento di liceità del trattamento si vedano le linee guida del Comitato europeo per la protezione dei dati personali: EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, versione 2.0, 8 ottobre 2019.

⁸ Può essere utile rilevare che tale costruzione è sostanzialmente analoga a quella eseguita, sempre da Meta, con riferimento alla pubblicità personalizzata, in particolare nella sua forma più invasiva di pubblicità comportamentale (*behavioural advertising*). Anche in questo caso Meta inseriva il trattamento di profilazione degli utenti per finalità pubblicitarie nelle sue condizioni contrattuali senza richiedere un autonomo consenso agli interessati e, anche in tale caso, è stata contestato a Meta il ricorso alla base giuridica contrattuale. La vicenda si è conclusa con la decisione sanzionatoria del 31 dicembre 2022 della Data Protection Commission irlandese.

network.

Avverso tale decisione, l'11 febbraio 2019 Meta presentava ricorso dinanzi all'Oberlandesgericht Düsseldorf (Tribunale superiore del Land di Düsseldorf). Successivamente apportava modifiche alle proprie condizioni generali: indicando espressamente che l'utente, invece di pagare per l'uso dei prodotti Facebook, acconsente alle inserzioni pubblicitarie⁹; introducendo la possibilità per gli utenti Facebook di visualizzare un riepilogo delle informazioni che le società del gruppo Meta ottengono in relazione alle loro attività su altri siti Internet e applicazioni e di scollegare tali dati dal loro account Facebook.com, sia per il passato che per il futuro.

L'Oberlandesgericht Düsseldorf, nel nutrire dubbi sulla possibilità per le autorità per la concorrenza di controllare, nell'ambito dell'esercizio delle loro competenze, la conformità di un trattamento di dati personali alle condizioni stabilite nel GDPR, sospendeva il procedimento per sottoporre alla Corte alcune questioni pregiudiziali.

Innanzitutto si chiede alla Corte di esprimersi sulla possibilità di un'autorità per la concorrenza di uno Stato membro di constatare, nell'ambito dell'esame di un abuso di posizione dominante ai sensi dell'art. 102 TFUE, che le condizioni contrattuali operate da tale impresa siano conformi al Regolamento e, eventualmente, accertarne la violazione e disporre la fine. In aggiunta, si chiede alla Corte l'interpretazione di alcune norme del Regolamento.

3. Le considerazioni della Corte

La Corte di giustizia chiarisce innanzitutto che: «Il modello economico del social network online Facebook si fonda sul finanziamento tramite la pubblicità online, che viene creata su misura per i singoli utenti del social network in funzione, in particolare, del loro comportamento di consumo, dei loro interessi, del loro potere d'acquisto e della loro situazione personale. Il presupposto tecnico per questo tipo di pubblicità è la creazione automatizzata di profili dettagliati degli utenti del network e dei servizi online offerti a livello del gruppo Meta. A tal fine, oltre ai dati che gli utenti forniscono direttamente al momento della loro iscrizione ai servizi online di cui trattasi, vengono raccolti, all'interno e all'esterno di detto social network e dei servizi online forniti dal

⁹ Tale diversa strategia comunicativa implica un primo ancorché ancora ambiguo riconoscimento del fenomeno della commercializzazione dei dati personali non solo in senso astratto ma anche con specifico riferimento alla piattaforma Facebook che, fino a quel momento, quanto meno nelle aule di tribunale per fini difensivi, aveva sostenuto l'impossibilità di scambiare servizi contro dati personali. A tal riguardo si veda la vicenda giudiziaria che ha visto lo scontro tra Facebook e l'Autorità Garante della Concorrenza e del Mercato che, con provvedimento n. 27432, procedimento PS11112, del 29 novembre 2018, ha contestato a Facebook una pratica commerciale ingannevole per aver pubblicizzato come "gratuito" l'accesso al proprio servizio mentre questo era remunerato tramite il trattamento dei dati degli utenti. Tale ricostruzione è stata confermata dapprima dal Tar Lazio, Sez. I, 10 gennaio 2020, n. 260, e poi dal Consiglio di Stato, sez. VI, 29 marzo 2021, n. 2631.

Il riconoscimento della fornitura "gratuita" del servizio digitale in cambio dell'ostensione di inserzioni pubblicitarie sta inoltre apparendo nelle informative di altri servizi digitali come, per esempio, TikTok, dove nei suoi Terms of Service, al §4, si legge: «*We don't charge you a fee to use most of the features of the Platform. Instead, businesses and organisations pay us to show you ads for their products and services, and we may also charge sellers a commission on products sold on TikTok Shops.*».

gruppo Meta e messi in relazione ai loro diversi account di utenza, anche altri dati relativi a tali utenti e ai loro dispositivi. Il quadro generale di tali dati consente di trarre conclusioni dettagliate sulle preferenze e sugli interessi dei medesimi utenti»¹⁰.

La Corte riassume il principale modello di business delle piattaforme digitali, quello definito “*zero-price*”, nel quale viene offerto un servizio in cambio non di un corrispettivo monetario bensì dell’autorizzazione dell’utente al trattamento dei propri dati per finalità commerciali (c.d. “patrimonializzazione”¹¹ o “valorizzazione” dei dati personali): dalla vendita delle informazioni o dei *pattern* statistici, ossia gli schemi di consumo degli utenti, all’invio di messaggi pubblicitari personalizzati, ecc.¹².

3.1. Sulla valutazione incidentale del GDPR da parte di un’autorità per la concorrenza

Sebbene le norme del Regolamento non si rivolgano alle autorità nazionali per la concorrenza ma disciplinino la cooperazione tra le autorità nazionali di controllo (in materia di protezione dei dati personali) interessate e l’autorità di controllo capofila nonché, se del caso, la cooperazione con il Comitato europeo per la protezione dei dati (EDPB), nonché il fatto che le autorità di controllo e le autorità per la concorrenza perseguano obiettivi e compiti propri, la Corte osserva che l’accesso e lo sfruttamento dei dati personali è di fondamentale importanza per l’economia digitale.

Questo conduce a ritenere il trattamento dei dati personali un parametro significativo della concorrenza. Escludere le norme in materia di protezione dei dati personali dall’analisi concorrenziale significherebbe ignorare la realtà di tale evoluzione economica e pregiudicare l’effettività della concorrenza nell’Unione Europea.

Sicché conclude la Corte: «nell’ambito dell’esame di un abuso di posizione dominante da parte di un’impresa su un dato mercato, può risultare necessario che l’autorità garante della concorrenza dello Stato membro interessato esamini anche la conformità del comportamento di tale impresa a norme diverse da quelle rientranti nel diritto della concorrenza, quali le norme in materia di protezione dei dati personali previste dal GDPR»¹³.

La Corte specifica che l’esame del GDPR è un accertamento incidentale nell’ambito della constatazione di un abuso di posizione dominante e che l’autorità per la concorrenza non si sostituisce all’autorità di controllo. Non è compito dell’autorità per la concorrenza sindacare il rispetto del Regolamento né far uso dei poteri riservati alle

¹⁰ CGUE, C-252/21, *Meta c. Bundeskartellamt* (2023), § 27. I modelli di business basati sulla raccolta e riutilizzo dei dati personali per fini commerciali e, più specificatamente, per finalità di pubblicità personalizzata, sono ormai noti alla giurisprudenza, come Consiglio di Stato n. 2631 del 29 marzo 2021, ma anche l’Autorità Garante della Concorrenza e del Mercato. Si vedano a tal riguardo, oltre a quelli altrove citati, anche i provvedimenti del 9 novembre 2021, n. 29888, PS11150, contro Apple (iCloud) e del 16 novembre 2021, n. 29890, PS11147, contro Google Drive-Sweep.

¹¹ TAR Lazio, sez. I, 10 gennaio 2020, n. 260.

¹² Sui modelli di business si veda M. Mursia–C.A. Trovato, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in questa *Rivista*, 3, 2021, 165 ss.

¹³ CGUE, C-252/21, cit., § 48.

autorità di controllo.

Da ciò ne segue che anche l'autorità per la concorrenza sarà soggetta all'interpretazione che le autorità di controllo o la stessa Corte danno al Regolamento e a questa dovrà conformarsi, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto alla concorrenza. Nei casi dubbi o sui quali non è rinvenibile un precedente, l'autorità per la concorrenza e quella di controllo dovranno cooperare tra loro.

Tale cooperazione si sostanzia nel fatto che, qualora l'autorità per la concorrenza abbia necessità di esaminare la conformità di un'attività al Regolamento e tale attività non sia già stata oggetto di una decisione da parte dell'autorità di controllo o della Corte e ciononostante ritenga che tale attività non sia conforme alle disposizioni del Regolamento, oppure quando nutra dubbi sulla valutazione effettuata dall'autorità di controllo o un'attività simile sia, al contempo, oggetto di esame da parte di tali autorità, in tutti questi casi l'autorità per la concorrenza dovrà consultare l'autorità di controllo al fine di fugare i propri dubbi o determinare se attendere l'adozione di una decisione da parte quest'ultima prima di iniziare la propria valutazione¹⁴.

Dall'altra parte, l'autorità di controllo deve rispondere alla richiesta di cooperazione entro un termine ragionevole comunicando le informazioni di cui dispone e che possano consentire di fugare i dubbi o, se del caso, informando dell'intenzione di avviare il procedimento di cooperazione di cui agli artt. 60 e seguenti del Regolamento¹⁵.

La Corte crea così un'ipotesi di parere obbligatorio per i casi dubbi o nuovi, vincolante con riferimento all'interpretazione del GDPR ma non con riferimento agli accertamenti di natura concorrenziale, bilanciato da un meccanismo di silenzio assenso. Infatti, in assenza di risposta dell'autorità di controllo o nel caso in cui questa non sollevi obiezioni a che si prosegua senza una sua decisione, l'autorità per la concorrenza potrà proseguire la propria indagine¹⁶.

La ricostruzione di tale meccanismo si basa più su un riconoscimento pratico delle difficoltà sottese agli accertamenti istruttori delle autorità che sulla forma giuridica e, tanto più, tale approccio risulta condivisibile nella misura in cui mira a garantire una tutela effettiva all'utente. Rafforzando la collaborazione tra autorità si dà così attuazione al principio di leale cooperazione sancito all'articolo 4, par. 3, TUE che si affianca, così, alla giurisprudenza che regola i rapporti tra normativa consumeristica e sul corretto trattamento dei dati personali¹⁷.

Recentemente il Consiglio di Stato¹⁸ ha ricostruito il rapporto tra la normativa a tutela del consumatore e quella sul corretto trattamento di dati personali non in termini di “compartimenti stagni di tutela” bensì come “tutela multilivello” suscettibile di

¹⁴ Ivi, § 57.

¹⁵ Ivi, § 58.

¹⁶ *Ibid.*

¹⁷ Con riferimento alla disciplina consumeristica si veda la Corte di giustizia del 13 settembre 2018, nelle cause riunite C-54/17 e C-55/17, ECLI:EU:C:2018:710, che ha avuto origine e impatti nella giurisprudenza nazionale alla quale si farà cenno nel prosieguo con riguardo all'art. 27, c. 1-*bis*, d.lgs. 206/2005.

¹⁸ Cons. Stato, sez. VI, 29 marzo 2021, n. 2631.

amplificare la garanzia dei diritti delle persone. In altre parole, la disciplina sul corretto trattamento dei dati personali e quella del Codice del consumo (d.lgs. 206/2005) presentano ambiti operativi differenti ma non contrastanti. Non si rinviene «alcuna incompatibilità o antinomia tra le previsioni del “Regolamento privacy” e quelle in materia di protezione del consumatore, in quanto le stesse si pongono in termini di complementarità, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell’altro alla corretta informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole»¹⁹.

La cooperazione descritta dalla Corte acquisisce, inoltre, particolare importanza laddove, non solo l’Autorità Garante della Concorrenza e del Mercato (AGCM)²⁰ sembra già porre alla base delle sue valutazioni in tema di concorrenza il rispetto del GDPR – da ultimo nell’importante caso relativo all’ipotesi di abuso di posizione dominante da parte di Google per aver ostacolato l’esercizio del diritto alla portabilità dei dati *ex art.* 20 GDPR²¹ – ma soprattutto perché questo principio sembrerebbe già rintracciabile, sebbene con riferimento alle pratiche commerciali scorrette, nell’art. 27, c. 1-*bis*, d.lgs. 206/2005²².

La norma dispone che nei casi di pratiche commerciali scorrette integrate da comportamenti regolati da specifiche normative europee, l’AGCM conserva la sua competenza ad intervenire a condizione che richieda il parere della “Autorità di regolazione competente” in quel settore.

La sua applicazione era stata rivendicata dal Garante per la protezione dei dati personali (in seguito, anche, “Garante” o “GPDP”) all’esito del provvedimento con il quale l’AGCM aveva sanzionato Telepass per una pratica commerciale ingannevole nell’attività di distribuzione di polizze assicurative. La contestazione della pratica ingannevole derivava dall’aver accertato che le società del gruppo Telepass non avevano adeguatamente informato gli utenti che i loro dati sarebbero stati condivisi con compagnie e intermediari di assicurazione o comunque raccolti e utilizzati anche a fini commerciali²³. In sede di ricorso al TAR il Garante si era costituito contestando il difetto di istruttoria e la violazione delle regole del procedimento poiché l’AGCM non aveva richiesto il suo parere come prescritto dalla norma citata.

Il TAR Lazio rigetta tale motivo ritenendo non applicabile la norma in quanto il Garante non sarebbe una “autorità regolatoria di settore” ma una “autorità generalista preposta alla tutela trasversale di un diritto fondamentale”. Inoltre, sostiene il giudice amministrativo, i piani tra tutela del consumatore e corretto trattamento dei dati

¹⁹ TAR Lazio, sez. I, 10 gennaio 2020, n. 260, § 8.

²⁰ Oltre all’autorità tedesca, che ha portato la questione dinanzi la Corte di giustizia, e all’AGCM, si rileva anche l’attività dell’Autorité de la concurrence francese che, a luglio 2023, ha avviato un’istruttoria per abuso di posizione dominante contro Apple per condizioni discriminatorie, non obiettive e non trasparenti sull’utilizzo dei dati degli utenti a fini pubblicitari. Il comunicato stampa del 25 luglio 2023 è disponibile sul [sito dell’autorità](#).

²¹ AGCM, provvedimento 18 luglio 2023, n. 30736, procedimento A552.

²² M. Cappai, *Quando l’erosione dei limiti costituzionali avviene dall’interno: il caso dell’art. 27, comma 1-bis del codice del consumo e della sua (presunta) natura interpretativa*, in *Rivista AIC*, 2, 2018, 1 ss.

²³ AGCM, provvedimento del 9 marzo 2021, n. 28601, procedimento PS11710.

personali sono “autonomi” e nulla in più avrebbe aggiunto il parere del Garante sul provvedimento finale²⁴.

Quand’anche tale pronuncia possa essere considerata conforme alla giurisprudenza previgente²⁵, spicca il differente approccio del TAR rispetto a quello della Corte dinanzi una questione analoga. Mentre la Corte di giustizia è andata al cuore del problema, il TAR ha fatto perno su una logica giuridica che ci restituisce però una tutela formale e probabilmente non più al passo coi tempi.

Al contrario, proprio un approccio più concreto e il focus sul principio di leale cooperazione tra autorità amministrative nonché il meccanismo di consultazione introdotto dalla Corte di giustizia potrebbero consentire un’interpretazione estensiva della norma tale da considerare anche il Garante quale autorità preposta all’applicazione di una normativa europea e, quindi, quale “autorità regolatoria” di un certo “settore”²⁶. Ciò, ovviamente, non al fine di contestare l’ormai pacifica competenza dell’AGCM in materia di pratiche commerciali scorrette bensì di fornire alla stessa, in ottica di leale cooperazione, appunto, ulteriori e utili elementi di valutazione per la sua attività di tutela del mercato e dei consumatori.

L’auspicio è quindi che la cooperazione tra AGCM e Garante possa rafforzarsi e indirizzarsi verso i binari di un confronto stabile a tutto vantaggio della tutela di un soggetto che, a prescindere dalla specifica nomenclatura di settore, consumatore o interessato del trattamento, nel contesto digitale coincide sostanzialmente con la persona²⁷.

3.2. Sull’applicazione delle norme del GDPR

Successivamente la Corte si sofferma sull’analisi degli altri quesiti prospettati dal giudice del rinvio e riguardanti pratiche diffuse tra i fornitori di servizi digitali.

Con riferimento alle categorie particolari di dati personali *ex* art. 9 del Regolamento, la Corte afferma che, ferma la necessità di un accertamento in concreto, in generale nel caso in cui un utente di un social network consulti siti Internet oppure applicazioni correlate a una o più delle categorie particolari di dati, il trattamento di tali dati da parte dell’operatore del social network – consistente nel raccogliere dati risultanti dalla con-

²⁴ TAR Lazio, sez. I, 9 novembre 2022, n. 603.

²⁵ Per una disamina sulla giurisprudenza in materia di conflitti di attribuzione tra le diverse autorità, in particolare tra AGCM e autorità di settore, ivi compresa la già citata Corte di giustizia 13 settembre 2018, nonché il passaggio dall’art. 23, c. 12-*quinquiesdecies*, del decreto legge n. 95 del 2012 al c. 1-*bis*, dell’art. 27, d.lgs. 206/2005, si veda M. Cappai, *La repressione delle pratiche commerciali scorrette nei mercati regolati: cosa aspettarsi dalla Corte di giustizia?*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 3-4, 2017, 879 ss.

²⁶ A tal fine può essere utile rilevare che la posizione rivendicata dal Garante può essere sovrapposta a quella che, a suo tempo, l’Adunanza Plenaria del Consiglio di Stato ha attribuito all’Autorità per le Garanzie nelle Comunicazioni (AgCom) in casi analoghi a quello Telepass: anche nei casi Vodafone e Wind le pratiche commerciali considerate dall’AGCM scorrette erano state realizzate tramite la violazione di obblighi informativi oggetto di una disciplina speciale, quella afferente al settore delle comunicazioni elettroniche di competenza dell’AgCom, così come nel caso Telepass gli obblighi informativi afferiscono al settore della protezione dei dati personali di competenza del Garante. Cfr. Cons. Stato, Adunanza Plenaria, nn. 3 e 4 del 2016.

²⁷ Anche qui si veda Cons. Stato, sez. VI, 29 marzo 2021, n. 2631.

sultazione di tali siti e applicazioni nonché i dati inseriti dall'utente, oppure nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo – deve essere considerato un trattamento di categorie particolari di dati lecito solo nel rispetto dell'art. 9 del Regolamento²⁸.

L'art. 9, par. 2, lett. e), del Regolamento consente il trattamento di questi dati se l'interessato li ha resi “manifestamente pubblici”. Rileva però la Corte che questo avviene soltanto se l'interessato abbia espresso chiaramente la sua volontà in tal senso, sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, o se vi abbia esplicitamente acconsentito sulla base di un'informazione espressa fornita dal sito o applicazione prima di tale inserimento o attivazione²⁹.

Sicché quando un utente consulta siti Internet oppure applicazioni correlate ad una o più delle categorie particolari di dati ed inserisce tali dati o attiva pulsanti come «Mi piace» o «Condividi» o i pulsanti che consentono all'utente di identificarsi utilizzando il proprio account, numero di telefono o indirizzo di posta elettronica, dati poi raccolti e utilizzati dall'operatore di social network mediante cookie o altri marcatori, l'utente non rende manifestamente pubblici tali dati solo per queste attività. I dati potranno essere considerati resi manifestamente pubblici soltanto se l'utente abbia esplicitamente e preventivamente acconsentito a far ciò, oppure tale intenzione la si può desumere dall'aver l'utente impostato, tramite gli strumenti messi a disposizione dalla piattaforma e, come sottolinea la Corte, “con piena cognizione di causa”, la sua interazione con la piattaforma in modo da rendere i suoi dati pubblicamente accessibili a un numero illimitato di persone³⁰.

Sebbene le osservazioni riguardino specificamente le categorie particolari di dati personali, la Corte sembra applicare il principio generale per cui i dati non possono essere né raccolti né trattati né riutilizzati³¹ in assenza di una giustificazione legalmente riconosciuta³². Ciò vale, sia per i dati comuni che per le categorie particolari di dati che, come osserva la Corte, possono essere trattati solo sulla base dei fondamenti di liceità dell'art. 9 GDPR.

Secondo la Corte, se il sito o l'applicazione utilizzata è idonea a rivelare la presenza di categorie particolari di dati allora il trattamento riguarderà categorie particolari di dati e non dati comuni, con le restrizioni e maggiori garanzie dell'art. 9 GDPR rispetto all'art. 6.

²⁸ CGUE, C-252/21, cit., § 73.

²⁹ Ivi, §§ 82-83.

³⁰ Ivi, §§ 84-85.

³¹ Le condizioni e i presupposti per il “riutilizzo” dei dati sono contenuti in diversi atti normativi tra cui i recenti Data Governance Act e Data Act. Ciononostante, il principio base sembrerebbe rinvenirsi nel principio di “limitazione delle finalità del trattamento”, di cui all'art. 5, par. 1, lett. b), GDPR, per il quale i dati personali possono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità». Sul tema sia consentito rinviare a G. d'Ippolito, *Il principio di limitazione delle finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data*, in *Il diritto dell'informazione e dell'informatica*, 6, 2018, 943 ss.

³² Tale principio è declinato nelle varie norme del GDPR ma ha le sue radici già nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea che, al par. 2, recita: «[I dati di carattere personale] devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge».

Si tratta dell'affermazione di un principio che potrebbe avere criticità applicative non sempre prevedibili tant'è che la Corte ne subordina l'applicazione a una valutazione caso per caso; infatti: «spetterà al giudice del rinvio stabilire se i dati in tal modo raccolti [...] consentano effettivamente di rivelare informazioni di questo tipo»³³.

Inoltre, la Corte rileva che per “riutilizzare” dati presenti o ottenibili in qualunque modo online (*rectius*, per trattare i dati disponibili online per fini diversi o ulteriori rispetto a quelli per cui sono stati originariamente resi disponibili) non si può invocare la base giuridica di cui all'art. 9, par. 2, lett. e), del Regolamento perché i dati semplicemente disponibili online non sono per ciò solo “manifestamente pubblici” in assenza di un elemento volitivo in più: la prova che l'utente voglia effettivamente rendere pubblicamente disponibili i suoi dati.

Si sconfessa così la diffusa quanto erronea credenza che tutto ciò che è online, per il fatto solo di essere disponibile, sia anche riutilizzabile. Ciò vale per le opere dell'ingegno così come per i dati personali quali ulteriori beni immateriali. Ma, soprattutto, tale specificazione sembra colpire tutte quelle attività che, senza idonea base giuridica, raccolgono i dati prodotti dall'interazione con la piattaforma o tramite c.d. “*scraping*”, una sorta di pesca a strascico di dati disponibili online³⁴, da riutilizzare per diversi fini: dall'*enrichment* delle proprie banche dati, al *training* degli algoritmi, attività strategica specie per i recentemente noti sistemi di Intelligenza Artificiale generativa³⁵.

3.3. Sul contratto e il consenso come base giuridica di alcuni trattamenti tra cui la pubblicità personalizzata

Dopodiché la Corte si sofferma sui presupposti di due tra i più discussi e controversi fondamenti di liceità previsti dall'art. 6 del Regolamento: il contratto e il legittimo interesse.

Possono i c.d. dati “Off Facebook” – ossia provenienti da altri servizi, diversi da quello principale, o derivanti dalla consultazione di altri siti o applicazioni di terzi – essere messi in relazione o “incrociati” con i dati del social network sulla base della necessità di eseguire il contratto con gli utenti, oppure per il perseguimento del legittimo interesse del titolare o di terzi?

³³ CGUE, C-252/21, cit., § 72.

³⁴ Nel provvedimento del 10 febbraio 2022, n. 50, doc. web n. 9751362, contro Clearview AI, il Garante per la protezione dei dati personali rilevava che: «Quanto, in particolare al *data scraping*, trattasi di una modalità particolare di raccolta che avviene a completa insaputa degli interessati. Sulla scorta di quanto sopra, si può ragionevolmente concludere che la raccolta di dati personali liberamente disponibili in Internet mediante tecniche di *web scraping* costituisce un trattamento di dati personali, che deve trovare legittimazione in una delle basi giuridiche previste dall'art. 6 del Regolamento». Con riferimento alla costituzione di elenchi telefonici a partire da numeri disponibili online si veda GPDP, Provvedimento del 17 maggio 2023, n. 201, doc. web n. 9903067.

³⁵ Tra le contestazioni mosse dal Garante per la protezione dei dati personali alla società OpenAI e che ha portato alla limitazione provvisoria del trattamento dei dati degli utenti italiani tramite ChatGPT si rinviene «l'assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT». GPDP, provvedimento 30 marzo 2023, n. 112, doc. web n. 9870832.

La Corte rileva innanzitutto che affinché un trattamento di dati personali sia considerato necessario all'esecuzione di un contratto di cui all'art. 6, par. 1, lett. b), del Regolamento, esso deve essere oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato. Bisogna quindi dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento che si intende operare; non basta che il trattamento sia semplicemente "utile", semplifichi o in altro modo agevoli l'esecuzione della prestazione principale offerta all'utente ma il trattamento deve essere "essenziale" per la corretta esecuzione del contratto stipulato con l'interessato³⁶.

È, questa, un'interpretazione rigorosa del concetto di "necessità"³⁷ che giustifica il ricorso al contratto ma in linea con una giurisprudenza³⁸ che, dopo la Corte di giustizia, è difficile non considerare "consolidata" se non "granitica".

Per quanto riguarda il legittimo interesse, la stessa giurisprudenza della Corte³⁹ ha individuato le condizioni che devono cumulative ricorrere per il suo utilizzo: il perseguimento di un interesse considerato "legittimo"; la "necessità" del trattamento per la realizzazione del legittimo interesse perseguito; la condizione che gli interessi o i diritti e le libertà fondamentali dell'interessato alla tutela dei dati non prevalgano sul legittimo interesse del titolare del trattamento o di terzi (c.d. *balancing test*)⁴⁰.

Ciò premesso la Corte conclude che la personalizzazione dei contenuti, ancorché utile per l'utente⁴¹, non appare necessaria per offrire a tale utente i servizi del social network online.

Allo stesso modo, per utilizzare Facebook non è necessario iscriversi agli altri servizi del gruppo Meta e il trattamento di dati provenienti da servizi diversi da quello principale non sembra essere necessario per consentire la fornitura di quest'ultimo servizio⁴². Con riferimento al legittimo interesse, la Corte esamina alcuni trattamenti.

Per svolgere attività di pubblicità personalizzata sulla base del legittimo interesse bisogna tenere in considerazione alcuni elementi come la necessità del trattamento, la minore età dell'interessato o le aspettative degli utenti. Proprio in considerazione di tali

³⁶ CGUE, C-252/21, cit., §§ 97 ss.

³⁷ CGUE, C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* (2008), ECLI:EU:C:2008:724.

³⁸ CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke e Eifert* (2010), EU:C:2010:662; Si veda, inoltre, EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento*, cit., § 25 ss. e, da ultimo, la vicenda giudiziale che ha visto contrapposto la DPC contro Meta con riferimento all'utilizzo del contratto quale base giuridica della pubblicità comportamentale: EDPB, *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)*, 5 December 2022; e, conseguentemente, DPC, *Decision concerning a complaint directed against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) in respect of the Facebook Service decision*, 31st day of December 2022.

³⁹ CGUE, C-13/16, *Rigas satiksme* (2017), EU:C:2017:336, §§ 28 ss.; C-597/19, *M.I.C.M.* (2021), EU:C:2021:492.

⁴⁰ Sui presupposti del legittimo interesse si veda anche: WP29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014, 41 ss.

⁴¹ Non mancano studi di carattere economico che rilevano come la personalizzazione dei contenuti esponga al rischio di messaggi pubblicitari di prodotti di qualità media a prezzi superiori: E.A. Schnadower Mustri-I. Adjerid-A. Acquisti, *Behavioral advertising and consumer welfare: an empirical investigation*, Federal Trade Commission PrivacyCon 2022.

⁴² CGUE, C-252/21, *Meta c. Bundeskartellamt*, §§ 102 ss.

aspettative la Corte afferma che: «malgrado la gratuità dei servizi di un social network online 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 GDPR»⁴³.

È questo uno dei passaggi della sentenza su cui più si è soffermata l'attenzione di giornalisti, studiosi ed esperti in quanto regolamenta uno dei trattamenti principali per il modello di business delle piattaforme digitali: quello della pubblicità personalizzata online.

Già le autorità di controllo, con propri provvedimenti⁴⁴ o linee guida dell'EDPB⁴⁵, avevano sostanzialmente ricondotto la pubblicità personalizzata al consenso quale base giuridica. Il mercato era poi stato "scosso" dalla pronuncia dell'autorità di controllo irlandese (DPC) che, su parere vincolante dell'EDPB, aveva precluso il ricorso al contratto quale base giuridica⁴⁶.

La sentenza della Corte di giustizia, anch'essa suscettibile di avere effetti e ripercussioni ben più ampi del singolo caso da cui ha avuto origine, completa l'opera precludendo anche il ricorso al legittimo interesse⁴⁷ e, di fatto, riportando la scelta sull'unica base giuridica allo stato utilizzabile: il consenso.

Proprio tale sentenza è divenuta l'occasione per l'autorità di controllo norvegese di vietare a Meta di svolgere trattamenti di pubblicità comportamentale sulla base del legittimo interesse⁴⁸, base giuridica a cui la società americana aveva fatto ricorso proprio a causa della "bocciatura" dello strumento negoziale da parte della DPC.

Che il consenso sia, nei fatti, la base giuridica allo stato ritenuta adeguata per la pubblicità comportamentale sembrerebbe, infine, essere riconosciuto anche dalla stessa Meta che, dopo l'intervento dell'autorità norvegese, ha annunciato di abbandonare ogni proposito di ricorso al legittimo interesse per adottare il consenso⁴⁹. Ciò quantomeno per

⁴³ Ivi, § 117.

⁴⁴ Oltre ai provvedimenti già citati si vedano, con specifico riferimento al consenso, anche: CNIL, *Délibération de la formation restreinte n° SAN-2023-009 du 15 juin 2023 concernant la société Criteo*; CNIL, *Délibération SAN-2019-001 du 21 janvier 2019 concernant Google*; in generale, con riferimento all'utilizzo di cookie e marcatori, la normativa impone il ricorso al consenso (in Italia l'art. 122 d.lgs. 196/2003). Obbligo normativo ripreso dalle linee guida delle diverse autorità di controllo nazionali.

⁴⁵ Oltre alle linee guida sul contratto, si vedano: WP29, *Parere 2/2010 sulla pubblicità comportamentale online*, 22 giugno 2010; EDBP, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020; EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media*, Versione 2.0, 13 aprile 2021.

⁴⁶ EDPB, *Binding Decision 3/2022, cit.*; DPC, *Decision concerning a complaint directed against Meta, cit.*

⁴⁷ In tal senso si era espresso anche il Garante per la protezione dei dati personali che con provvedimento del 7 luglio 2022, n. 248, doc. web n. 9788429, avvertiva TikTok che il proposito di fondare la pubblicità personalizzata sulla base del legittimo interesse avrebbe potuto configurare una violazione della normativa.

⁴⁸ Datatilsynet, *Urgent and Provisional Measures – Meta*, 21/03530-16, 14.07.2023. Disponibile anche il [comunicato stampa sul sito dell'autorità](#).

⁴⁹ Meta, *How Meta Uses Legal Bases for Processing Ads in the EU*, January 4, 2023 update on August 01,

il mercato dell'UE, dello Spazio Economico Europeo e della Svizzera, Regno Unito escluso⁵⁰. Potrebbe questo essere l'epilogo di una battaglia legale durata anni e che Meta ha condotto non solo per sé ma a difesa di un intero modello di business largamente adoperato.

Con questa sentenza della Corte, i fornitori di servizi digitali si trovano per la seconda volta in meno di un anno⁵¹, solo per l'imitarsi al settore della pubblicità online, dinanzi la scelta di proseguire come prima o rinnovarsi e ripensare il mercato con modelli di business più sostenibili.

Dopo la pubblicità personalizzata, l'esame della Corte si volge verso altri trattamenti. Con riferimento alla sicurezza del network, che ben può, astrattamente, configurare un legittimo interesse del titolare, per utilizzare tale base giuridica bisognerà in concreto verificare che tale obiettivo non possa ragionevolmente essere raggiunto in modo altrettanto efficace ma con mezzi meno pregiudizievole e nel rispetto del principio della minimizzazione dei dati. Nello specifico, con riferimento alla fattispecie portata dal giudice del rinvio, bisognerà verificare se e in quale misura il trattamento di dati personali raccolti a partire da fonti esterne al social network Facebook risulti effettivamente necessario per garantire che non sia compromessa la sicurezza interna di tale network⁵². Con riferimento ai trattamenti diretti al "miglioramento del prodotto o servizio", per quanto anche questo astrattamente in grado di integrare un interesse del titolare meritevole di tutela, la Corte avanza dubbi che possa prevalere sui diritti fondamentali e sugli interessi degli utenti, tanto più se minorenni⁵³.

Relativamente al trattamento riguardante l'informazione delle autorità preposte all'esercizio di azioni penali e all'esecuzione di pene dirette ad evitare, individuare e a perseguire reati, tale obiettivo non può, in linea di principio, costituire un legittimo interesse ai sensi dell'art. 6, par. 1, lett. f), del GDPR⁵⁴.

Infine, con riferimento ai dati "Off Facebook" la Corte conclude che tale trattamento: possa essere considerato necessario per l'esecuzione di un contratto solo a condizione

2023: «Today, we are announcing our intention to change the legal basis that we use to process certain data for behavioural advertising for people in the EU, EEA and Switzerland from 'Legitimate Interests' to 'Consent'. This change is to address a number of evolving and emerging regulatory requirements in the region, notably how our lead data protection regulator in the EU, the Irish Data Protection Commission (DPC), is now interpreting GDPR in light of recent legal rulings, as well as anticipating the entry into force of the Digital Markets Act (DMA). Historically, businesses operating in this region have relied on a variety of legal bases under GDPR for the purpose of processing data for advertising. GDPR states that there is no hierarchy between legal bases, and none should be considered more valid than any other. However, we have listened carefully to regulatory feedback from the Irish DPC, including how it is interpreting recent decisions by the European Court of Justice, in deciding to make this change».

⁵⁰ Si veda, a riguardo, la [dichiarazione del 2 agosto 2023 di Stephen Almond](#), Executive Director of Regulatory Risk dell'Autorità di controllo inglese (ICO): «We're aware of Meta's plans to seek consent from users for behavioural advertising in the EU, to the exclusion of the UK. This follows related findings by the Court of Justice of the European Union, Irish Data Protection Commission and Norwegian Data Protection Authority. We are assessing what this means for information rights of people in the UK and considering an appropriate response».

⁵¹ Tre se si conta anche l'importante pronuncia dell'autorità belga del febbraio 2022 contro IAB Europe e il sistema pubblicitario basato sul protocollo TCF: BE DPA, *Complaint relating to Transparency & Consent Framework. Decision on the merits 21/2022*, 2 February 2022.

⁵² CGUE, C-252/21, cit., §§ 19 ss.

⁵³ Ivi, § 123.

⁵⁴ Ivi, § 124.

che sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata agli utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento⁵⁵, cosa che non si realizza nel caso concreto⁵⁶; mentre può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi solo a condizione che si informino gli utenti che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse⁵⁷.

Infine, con riguardo alla possibilità di trattare i dati Off Facebook per la salvaguardia di interessi vitali (art. 6, par. 1, lett. d), Regolamento) o per adempiere a un obbligo legale (art. 6, par. 1, lett. c), Regolamento), la Corte rileva, rispettivamente, che: un operatore, la cui attività riveste carattere essenzialmente economico e commerciale, non può addurre la protezione di un interesse essenziale alla vita dei suoi utenti o di un'altra persona per giustificare la liceità di tale trattamento⁵⁸; mentre tale trattamento potrà avvenire allorché sia effettivamente necessario per adempiere un obbligo legale rispondente ad un obiettivo di interesse pubblico e a questo proporzionato nei limiti dello stretto necessario⁵⁹.

3.4. Sul rapporto tra posizione di dominanza e validità del consenso

Una ulteriore e rilevante questione sottoposta alla Corte si incentra sulla possibilità di considerare valido, ai sensi del Regolamento, il consenso prestato dall'utente nei confronti di un operatore in posizione dominante in un certo mercato.

La Corte premette una serie di rilievi. Innanzitutto, il consenso non può 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, oppure quando esiste un evidente squilibrio tra l'interessato e il titolare del trattamento⁶⁰.

In aggiunta si sofferma su una norma che ha creato non poche questioni applicative⁶¹: l'art. 7, par. 4, del Regolamento che prevede che, nel valutare se il consenso sia stato

⁵⁵ Ivi, §125.

⁵⁶ Ivi, § 104: «Pertanto, e salvo verifica del giudice del rinvio, un trattamento di dati personali provenienti da servizi diversi da quello del social network online, proposti dal gruppo Meta, non sembra essere necessario per consentire la fornitura di quest'ultimo servizio».

⁵⁷ Ivi, § 126.

⁵⁸ Ivi, § 137.

⁵⁹ Ivi, § 138.

⁶⁰ EDBP, *Linee guida 5/2020 sul consenso*, cit., § 13 ss. Si veda anche il considerando 43 del GDPR.

⁶¹ G. Resta-V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2, 2018, 411 ss.; S. Thobani, *Operazioni di "tying" e libertà del consenso*, in *Giurisprudenza italiana*, 3, 2019, 533 ss. Si veda anche, con riferimento alla "fungibilità" dei trattamenti, Cass. civ., sez. I, 25 luglio 2018, n. 17278.

liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto⁶².

È la norma che disciplina il c.d. *tying* o *bundling*, di grande attualità specie con riferimento alla questione dei *cookie wall* e *pay wall* implementati da diversi editori online: ossia condizionare la prestazione di un servizio al conferimento del consenso a un trattamento di dati a questo non necessario. Principio che, nel caso dei *cookie wall*, si è tradotto nella scelta, rimessa all'utente, tra consentire la profilazione tramite cookie per accedere al sito oppure pagare una certa somma di denaro.

La liceità di tale condotta è stata oggetto di interpretazione restrittiva da parte dell'EDPB⁶³ così come dall'Autorità di controllo francese (CNIL). Quest'ultima, in seguito all'intervento del Conseil d'Etat⁶⁴, è ritornata sui propri passi per disciplinare i casi di condizionalità lecita⁶⁵.

La questione è, inoltre, attualmente *sub iudice* dinanzi il Garante italiano⁶⁶.

Su tali temi la Corte conclude che, certamente, anche l'operatore titolare del trattamento che occupi una posizione dominante sul mercato dei social network può ricorrere al consenso come base giuridica ma, allo stesso tempo, tale circostanza deve essere presa in considerazione nella valutazione della validità del consenso in quanto può incidere sulla libertà di scelta dall'utente. L'utente potrebbe quindi non essere in grado di rifiutare o di revocare il consenso senza subire pregiudizio⁶⁷. Proprio l'esistenza di una posizione dominante è suscettibile di creare uno squilibrio evidente tra l'interessato e il titolare che può favorire l'imposizione di condizioni non strettamente necessarie all'esecuzione del contratto.

La Corte di giustizia afferma quindi che: «tali utenti devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro

⁶² La seconda frase del considerando 43 del GDPR precisa che si presume che il consenso non sia stato liberamente espresso, dove l'uso dell'espressione «si presume», così come interpretato dall'EDPB nelle linee guida sul consenso (v. punto 35 di dette linee guida) indica che i casi di validità del consenso saranno estremamente eccezionali. Cfr. EDBP, *Linee guida 5/2020 sul consenso*, cit., punto 14, dove si rileva che l'inciso «tra le altre» indica che l'art. 7, par. 4, GDPR non è stato redatto in modo esaustivo e può comprendere altre eventualità, compresa qualsiasi azione di pressione o influenza inappropriata sull'interessato, che impedisca a quest'ultimo di esercitare il suo libero arbitrio, § 25 e, in particolare, il § 26 dove si rileva che il GDPR assicura che il trattamento dei dati personali per cui viene richiesto il consenso non possa trasformarsi direttamente o indirettamente in una controprestazione contrattuale e, quindi, che le due basi legittime per la liceità del trattamento, il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte.

⁶³ EDBP, *Linee guida 5/2020 sul consenso*, cit., punto 39 dove si legge: «Affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente (i cosiddetti "cookie wall")».

⁶⁴ Conseil d'État, Décision du 19 juin 2020; si veda anche CNIL, *Cookies et autres traceurs: le Conseil d'État rend sa décision sur les lignes directrices de la CNIL*, 19 juin 2020.

⁶⁵ CNIL, *Cookie walls: la CNIL publie des premiers critères d'évaluation*, 16 mai 2022.

⁶⁶ GPDP, *Cookie wall: all'esame del Garante privacy le iniziative degli editori*, 18 ottobre 2022, doc. web n. 9815415.

⁶⁷ CGUE, C-252/21, §§ 148-149.

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»⁶⁸.

È quindi opportuno che possa essere prestato un consenso separato per il trattamento dei dati Off Facebook. Diversamente, anche in considerazione della posizione dominante⁶⁹ di Meta e fermo restando che grava sul titolare l'onere di dimostrare che l'interessato ha validamente prestato il proprio consenso, si deve presumere⁷⁰ che il consenso di detti utenti al trattamento dei dati Off Facebook non sia stato prestato liberamente.

In conclusione, l'eventuale posizione dominante dell'operatore integra gli elementi di valutazione alla base dell'applicazione dell'art. 7, par. 4, del Regolamento. Circostanza che può essere particolarmente utile in alcuni casi, non ultimo quello dei *cookie wall* posti in essere dagli editori online.

Se pure la Corte fornisce alle autorità di controllo un elemento di valutazione in più, incentrato sulla posizione di dominanza dell'operatore, non si risolve comunque l'interpretazione del vero punto dolente: quando un servizio alternativo possa dirsi "equivalente" a quello condizionato e quindi quando questo possa rendere lecito il sempre più diffuso fenomeno della condizionalità⁷¹.

Ad ogni modo, mentre in apertura si riconosceva alle autorità per la concorrenza la possibilità di accertare, *incidenter tantum*, le norme del Regolamento, qui la Corte sembrerebbe riconoscere anche alle autorità di controllo di fare lo stesso con la normativa sulla concorrenza, consentendogli di porre, alla base delle loro valutazioni sulla validità del consenso, anche l'analisi sulla dominanza del titolare in un certo mercato.

4. Conclusioni

Nell'avallare le tesi del Bundeskartellamt la Corte di giustizia ha emesso una sentenza che avrà importanti ripercussioni su tutto il settore della *data economy*. Ne risulta inoltre rafforzata quella corrente di pensiero che vede in una maggior trasversalità applicativa delle normative la chiave per garantire alla persona nel mondo dei bit una tutela completa ed effettiva.

Si possono poi individuare alcune tendenze in materia di pubblicità personalizzata e regolazione delle piattaforme.

Con riferimento alla base giuridica della pubblicità personalizzata, dopo report del

⁶⁸ Ivi, § 150.

⁶⁹ Nelle sue conclusioni, l'Avvocato Generale Athanasios Rantos, al § 75, specificava che: «Occorre, tuttavia, precisare, da un lato, che, affinché una situazione siffatta di potere sul mercato sia rilevante sotto il profilo dell'applicazione del GDPR, essa non deve necessariamente essere equiparata al livello di posizione dominante ai sensi dell'articolo 102 TFUE e, dall'altro, che tale circostanza non può da sola, in linea di principio, privare di qualsiasi validità un consenso».

⁷⁰ Considerando 43 GDPR.

⁷¹ EDPB, *Linee guida 5/2020 sul consenso*, cit., § 37; CNIL, *Cookie walls*, cit.

Parlamento europeo⁷², diverse pronunce delle autorità di controllo⁷³, linee guida e interventi dell'EDPB⁷⁴, e, ora, la sentenza della Corte di giustizia, è difficile continuare a sostenere che gli attuali modelli di business, spesso basati su *dark pattern*⁷⁵ e un ridotto potere di controllo degli interessati sui propri dati, possano continuare a prevedere una profilazione degli utenti per fini pubblicitari o commerciali su una base giuridica diversa dal consenso.

Per quanto lecite e condivisibili le istanze del mercato sulla necessità di remunerare la loro attività tramite la profilazione degli utenti si può osservare che la normativa, così come l'interpretazione della stessa, non mira a limitare l'attività d'impresa o lo sviluppo economico, cosa che sarebbe in contrasto, tra le varie norme, anche con l'art. 1 dello stesso Regolamento⁷⁶, bensì a tener conto anche della volontà degli utenti nel trattamento dei loro dati. Se, dunque, quella di offrire servizi “a prezzo zero” è una libera scelta di mercato diretta ad abilitare la forma più remunerativa ma anche invasiva di pubblicità personalizzata (la pubblicità comportamentale⁷⁷), dall'altro lato non lo si potrà fare contro la volontà dell'utente, condizionando o forzando la stessa o a sua insaputa.

In altre parole, qualora si scelga di svolgere un trattamento particolarmente impattante sulla sfera giuridica dell'interessato si dovrà contestualmente assumere il rischio che l'utente possa non essere d'accordo. Rischio in realtà condiviso anche dall'utente vista la facilità con cui si ottiene il consenso tutt'altro che consapevole dello stesso, cosa che ha messo in crisi i sistemi normativi basati sul concetto di “consenso informato”.

Nell'ottica non solo del GDPR ma anche della nuova legislazione europea, dal *Digital Services Act* e *Data Markets Act* fino al *Data Governance Act* e *Data Act*, la tendenza è quella di rendere l'utente sempre più parte dell'economia digitale e anch'esso protagonista dei trattamenti che estraggono valore dalle informazioni a lui riferite⁷⁸.

⁷² European Parliament, *Regulating targeted and behavioural advertising in digital services. How to ensure users' informed consent*, 30 August 2021.

⁷³ *Ex multis*, le decisioni della Data Protection Commission irlandese: del 31 dicembre 2022, contro Meta Platforms Ireland Limited con riferimento ai servizi Facebook e Instagram; del 12 gennaio 2023, contro WhatsApp Ireland Limited; Garante per la protezione dei dati personali, provvedimento n. 248 contro TikTok del 7 luglio 2022, doc. web n. [9788429](#).

⁷⁴ EDPB, *Linee guida 8/2020 sul targeting*, cit.; EDPB, *Binding Decision 3/2022 on Irish SA and Meta*, cit.

⁷⁵ EDPB, *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, version 2.0, 14 February 2023.

⁷⁶ V. Ricciuto, *L'equivoco della privacy. Persona vs. dato personale*, Napoli, 2022, 87 e ss, che, a proposito, afferma: «per il diritto il dato circola e può circolare *solo e se* “protetto”: se e in quanto, cioè, trattato coerentemente e conformemente con il particolare statuto normativo che definisce presupposti, limiti, e condizioni della possibilità (*rectius*: del diritto) di compiere sullo stesso operazioni di trattamento, così come delineato dal GDPR. Sicché proteggere i dati personali non equivale (né deve equivalere) a limitare la loro circolazione/trattamento nei processi di impresa in ragione di un'aprioristica prevalenza degli interessi e dei diritti della persona rispetto al fenomeno circolatorio ed agli ulteriori interessi ad esso sottesi e da esso implicati. Protezione dei dati personali e loro circolazione si integrano; il dato personale protetto non è il dato segreto, inaccessibile, ma il dato che circola e viene trattato. Il che, detto in altri termini, equivale a dire che la libera circolazione dei dati garantita dall'ordinamento e meritevole di tutela è una circolazione protetta, perché protetto è il suo oggetto».

⁷⁷ G. d'Ippolito, *Online Behavioural advertising e protezione dei dati personali*, in D. Buzzelli-M. Palazzo (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, 2022, 125 ss.

⁷⁸ D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2, 2023, 367 ss.

L'elemento da considerare, passando quindi al tema della regolazione delle piattaforme digitali, è la necessità di tener conto della scelta dell'utente, tanto antecedente all'inizio del trattamento, quindi sotto forma di consenso, quanto che sia in costanza di questo, quindi sotto forma di esercizio dei diritti, in particolare quale diritto di opposizione *ex art. 21 del Regolamento*.

Il consenso costituisce quindi un'ulteriore variabile del mercato, suscettibile di incidere sul modello di business adottato dal fornitore del servizio e non vincolabile tramite condizioni contrattuali perché esercizio di un diritto fondamentale: il corretto trattamento dei dati personali che si esplica nel più ampio potere di controllo sugli stessi⁷⁹. Valori, questi, in linea anche con l'art. 41 della Costituzione italiana laddove subordina l'iniziativa economica all'utilità sociale e alla dignità umana⁸⁰.

Dinanzi soggetti che hanno accumulato un potere economico che nemmeno gli Stati riescono a fronteggiare, continuare a ritenere il contratto lo strumento migliore per contemperare le contrapposte esigenze, tanto più in un contesto in cui anche i tradizionali rimedi contro l'asimmetria informativa (come gli obblighi di trasparenza o le clausole vessatorie) si rivelano una tutela debole o formale, rischia di agevolare il consolidamento di un ecosistema squilibrato a vantaggio non solo della primazia dell'economia sul diritto ma a vantaggio di pochi grandi soggetti nei confronti della moltitudine di attori oggi operanti sui mercati digitali (non solo utenti e *start-up* o piccoli operatori come i produttori di app, i *content creator* o *influencer*, ma anche soggetti che si comportano da intermediari⁸¹ o finanche soggetti pubblici o svolgenti compiti di interesse pubblico). Ecco perché le norme contenute nel GDPR sono solo il principale esempio di un nuovo modo di legiferare che, in linea con le esigenze del costituzionalismo digitale, pone dei paletti all'iniziativa economica a presidio di principi che non solo tutelano la persona ma presidiano un più ampio sistema di valori⁸². Principi ovviamente non derogabili

⁷⁹ Come noto, il corretto trattamento dei dati personali quale diritto fondamentale è rinvenibile nell'art. 8, c. 1, della Carta dei diritti dell'Unione europea e nell'art. 16, par. 1, del TFUE. In generale si vedano: M. Bassini, *Il diritto costituzionale alla "privacy" nel prisma dell'evoluzione tecnologica*, in *Diritto costituzionale*, 1, 2023, 83 ss.; O. Pollicino, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, 3, 2014, 1 ss.; 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*, 22, 2018, 1 ss.

⁸⁰ Ma anche alla salute, all'ambiente, alla sicurezza, alla libertà. In linea generale, inoltre, è anche possibile rilevare che, tradizionalmente, l'art. 1322 c.c. subordina l'autonomia negoziale ai «limiti imposti dalla legge» e agli «interessi meritevoli di tutela secondo l'ordinamento giuridico».

⁸¹ Si veda, a proposito la segnalazione di Hoda contro Google per abuso di posizione dominante nel settore della portabilità dei dati: AGCM, provvedimento 18 luglio 2023, n. 30736, cit.

⁸² Autorevole dottrina parla, a proposito, del modello del c.d. "consenso remunerato", ossia di un sistema di integrazione tra strumenti privatistici e strumenti pubblicistici che consente di far coesistere la libera circolazione dei dati con un alto livello di protezione dei diritti coinvolti, e in particolare del diritto fondamentale alla protezione dei dati personali sancito dall'art. 8, c. 1, della Carta dei diritti fondamentali UE, nonché del modello del "contratto conformato", ossia dell'accordo negoziale a cui l'ordinamento pone specifiche limitazioni e garanzie a tutela di un'adesione all'intesa contrattuale che sia espressione libera e consapevole di autonomia nelle scelte. G. Resta, *Contratto e diritti fondamentali*, in *Enc. dir.*, I, Milano, 2021, 304 ss. Altra autorevole dottrina parla di "diritto privato regolatorio" e di "contratto funzionalizzato" per indicare che il contratto stipulato dai privati è vagliato in relazione alla sua compatibilità con il sistema degli scambi nel quale esso si inserisce (il mercato) ed è altresì conformato *ab externo* rispetto alle esigenze e ai valori che caratterizzano l'assetto di *quel* mercato. V. Ricciuto, *L'equivoco della privacy*, cit., 83 ss; Infine, altra dottrina parla di "contratto amministrato" dalle Autorità amministrative indipendenti che, in presenza di una regolazione del mercato tendente a instaurare e

dall'autonomia contrattuale e che dovrebbero essere considerati dal mercato come la bussola per sviluppare modelli di business più sostenibili e rispettosi dell'autodeterminazione della persona⁸³.

In questo schema regolatorio, l'esigenza di una rinnovata e più forte collaborazione delle autorità di controllo, così come di un'applicazione trasversale delle normative coinvolte, è strumentale alla tutela di valori come la concorrenza, il corretto trattamento dei dati personali, il pluralismo, ecc. E deriva appunto dalla consapevolezza di dover dare all'utente, alla persona, al cittadino digitale, una tutela effettiva e completa.

La normativa europea fa dell'utente un attore non secondario dei mercati digitali e questa qualifica deve essere valorizzata, non sminuita.

Senza questa consapevolezza, senza riconoscere agli utenti un reale e immediato potere di incidere sul funzionamento dei servizi digitali, così come alle autorità di collaborare per riconoscere allo stesso una tutela effettiva, a poco servono i diritti e i rimedi *ex post* e, ancor meno, aumentare gli obblighi informativi.

garantire principi di rilievo costituzionale (concorrenza, pluralismo, ecc.) nonché dell'inadeguatezza dei privati nell'attuare loro stessi tali principi, rinviene nelle Autorità indipendenti il potere di conformare i contratti ai valori ai quali è improntato l'assetto di un dato mercato. C. Solinas, *Il contratto "amministrato". La conformazione dell'operazione economica privata agli interessi generali*, Napoli, 2018, 207 ss.

⁸³ Sfida effettivamente colta da alcuni operatori che fanno, meritoriamente, della protezione dei dati personali un elemento di concorrenza: dagli *add-on* per il blocco o la selezione di cookie, a browser che aumentano il potere di controllo sui propri dati o sistemi operativi che riconoscono all'utente la scelta se inibire il tracciamento pubblicitario delle app sui propri smartphone, fino ai tentativi e alle richieste di "sandbox" regolatorie per sviluppare sistemi di profilazione pubblicitaria più in linea con i principi europei.