

Digitalizzazione e profilazione degli utenti: la Corte di giustizia sul consenso informato e sulla responsabilità degli operatori online

ANGELA CORRERA*

Sommario: 1. Premessa. – 2. Il *webtracking* comportamentale: il vantaggio economico derivante dalla profilazione degli utenti e le principali questioni pratiche. – 3. Il consenso dell'interessato al trattamento dei dati acquisiti mediante *cookie*. – 4. *Segue*: la responsabilità congiunta. – 5. Considerazioni a margine degli orientamenti della Corte di giustizia.

1. Lo sviluppo dei mercati digitali ha comportato un aumento esponenziale dei dati impiegati nel processo produttivo e una moltiplicazione delle fonti di raccolta e delle forme di utilizzo dei medesimi. In particolare, la disponibilità di una varietà sempre più vasta di dati elettronici relativi a ciascun individuo, dovuta alla diffusione del *webtracking* comportamentale, è stata alimentata dalla grande frequentazione dei *social media* e dall'utilizzo di dispositivi mobili e di sorveglianza collegati in rete.

* Dottoranda di ricerca in Diritto dell'Unione europea. Università Parthenope, Napoli.

Infatti, attraverso il monitoraggio a fini commerciali e di *marketing* del comportamento degli internauti, gli operatori del *web* sono in grado di elaborare un vero e proprio profilo a cui inviare messaggi pubblicitari perfettamente corrispondenti agli interessi dedotti ¹. Il successo di questa operazione è garantito dall'impiego di *cookie* che, una volta attivati sul *computer* dell'interessato all'apertura di un sito *web*, permettono di osservarne le abitudini di navigazione e di identificarne gli interessi, così che gli operatori *online* possano rivolgersi in maniera più mirata alle diverse fasce di utenti ².

Tali sistemi di tracciamento, una volta creati dai grandi operatori del *web*, non di rado, sono utilizzati dagli sviluppatori di *app* o di siti *online*; conseguentemente, i dati acquisiti dai primi entrano nella disponibilità anche dei secondi, trasformandosi in uno strumento di ricchezza clamoroso.

È facile dedurre che, in tal modo, le piattaforme *online* sono divenute il luogo di elezione per la raccolta di dati ai fini della profilazione degli utenti. Ma è altresì vero che, troppo spesso i frequentatori dei

¹ Per un approfondimento sulla tecnologia del *tracking cookie*, si rinvia al parere 2/2010 del gruppo di lavoro «Articolo 29» per la protezione dei dati, del 22 giugno 2010, sulla pubblicità comportamentale.

² Cfr. M. HUBERTY, *Awaiting the Second Big Data Revolution: From digital noise to value creation*, in *Journal of Industry, Competition and Trade*, 2015, p. 35 ss.; OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, 2015; R. DAVIES, European Parliamentary Research Service (EPRS), *Big Data and Data analytics. The potential for innovation and growth*, settembre 2016; Commissione europea, 2 luglio 2014, COM(2014) 442 final, *Verso una florida economia basata sui dati* {SWD(2014) 214 final}; Id., *Building a european Data economy*, 10 gennaio 2017, COM(2017) 9 final e il relativo Staff Working Document (2017) 2 final del 10 gennaio 2017 *On the free flow of Data and emerging issues of the European Data economy*; *Big Data Value Europe, Big Data Value Strategic Research & Innovation European Agenda (BDV-SRIA)*, Version 3.0, gennaio 2017.

social network - primo tra tutti in termini di diffusione, *Facebook*, sono assolutamente ignari delle insidie e dei rischi a cui i loro dati sono esposti.

Muovendo da queste premesse, il presente contributo analizza le implicazioni pratiche derivanti dalle possibilità di impiego dei dati degli utenti da parte delle principali piattaforme digitali, alla luce degli orientamenti della Corte di giustizia.

In particolare, l'analisi, pur muovendo dalla ovvia considerazione per cui le piattaforme *online* svolgono un ruolo di facilitazione e di intermediazione nel rapporto tra "cliente/utente" e "operatore online/venditore", evidenzia il dato non più trascurabile del potere che esse hanno acquisito, che ha radicalmente stravolto le dinamiche concorrenziali in numerosi mercati e da cui è derivata una vera e propria ibridazione dei ruoli, oltre che una inedita sovrapposizione di discipline, con interessanti ripercussioni in termini di responsabilità per il trattamento dei dati personali.

In questo quadro, la pervasività dell'*Information Technology* ha posto al centro dell'attenzione l'individuo, concepito non più solo come mero "utente/consumatore", ma anche e soprattutto come "produttore" di dati personali utilizzati dalle imprese.

2. Occorre preliminarmente rilevare che il tema della commercializzazione di dati da parte delle piattaforme *online* e della rilevanza economica dei contenuti generati dagli utenti è al centro del dibattito in ambito consumeristico e *antitrust*.

Al riguardo è stato rilevato che i servizi offerti dalle *Internet platforms* si nascondono dietro una gratuità solo apparente³, atteso che essi sono fruibili. Così, nell'ipotesi esemplificativa più diffusa della creazione di un account su una piattaforma *social*, l'oggetto della controprestazione del contenuto digitale, al quale l'utente-consumatore accede gratuitamente, è sovente costituito dalla possibilità per la piattaforma di sfruttare le informazioni dallo stesso condivise per finalità commerciali⁴.

In proposito, la prassi dimostra che la disponibilità di dati personali può attribuire un forte vantaggio competitivo alle imprese e, dunque, rilevare ai sensi della disciplina della concorrenza⁵.

Difatti, taluni servizi digitali sono controllati da operatori dominanti che non appaiono soggetti a significative pressioni competitive. Basti pensare all'attività di *Google*, con riferimento ai servizi di ricerca *online*, alla posizione di *Facebook* sul fronte dei *social network* e a quella di *Amazon* nell'*e-commerce*, rispetto ai quali, in taluni casi, è già stata accertata la sussistenza di posizioni dominanti dalle autorità *antitrust* europee⁶.

³ Sul punto, v. Relazione annuale dell'AGCM sull'attività svolta nel 2016, p. 252. Inoltre, v. caso No. COMP/M.7217 – FACEBOOK/WHATSAPP, §129 ss.

⁴ Cfr. in tal senso e per una compiuta ricostruzione dei diversi modelli di *business* delle piattaforme *online*, v. S. PERUGINI, *I mercati dell'informazione e benessere dei consumatori. Nuovi scenari in ambito europeo e possibili riflessi sull'attività dell'Autorità Garante della Concorrenza e del mercato*, in *Consumerism 2015, Ottavo Rapporto annuale, Il consumatore nell'era della condivisione*.

⁵ Cfr. G. PITRUZZELLA, *Big Data, competition and privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, 2016, p. 15 ss.; *Id.*, *Big Data and antitrust enforcement*, in *Italian Antitrust Review*, 2017, p. 77 ss.

⁶ Sul punto, v. Commissione Europea (2019), “AT.40411 Google Search (AdSense)”; (2018), “AT.40099 Google Android”; (2017), “AT.39740 Google Search (Shopping)”;

A tanto si aggiungano le problematiche connesse alla disciplina consumeristica evidenziate nella versione riveduta degli orientamenti relativi alla direttiva sulle pratiche commerciali sleali ⁷. Nell'occasione sono stati descritti una serie di fenomeni che caratterizzano l'attività dei *social media* e che, secondo la Commissione europea, integrano pratiche commerciali scorrette.

La *policy* adottata da *Facebook*, in occasione dell'acquisto di *WhatsApp*, ne è una testimonianza. Ed invero aveva attirato l'attenzione delle autorità europee e nazionali ⁸, in quanto a fronte di un consenso implicitamente acquisito mediante il meccanismo del c.d. *opt-out*, i dati e i contenuti resi accessibili dagli utenti su *WhatsApp* venivano condivisi su *Facebook* per scopi promozionali.

In sede nazionale, l'AGCM ⁹ aveva qualificato tale condotta come un comportamento rilevante in materia di pratiche commerciali scorrette e clausole vessatorie. Più precisamente, secondo l'AGCM, il noto *social network* aveva realizzato una pratica ingannevole, vietata dagli

Bundeskartellamt (2019) B6-22/16 *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing.*

⁷ SWD (2016) 163 final, del 25 maggio 2016, in cui l'Esecutivo europeo mostra di riconoscere che la piattaforma trae un beneficio economico dal valore commerciale dei dati e delle informazioni fornite dagli utenti.

⁸ *cf.* Merger procedure, Case No. COMP/M.7217 – *Facebook/WhatsApp*, 3 ottobre 2014; 'Refining the EU merger control system', Speech by Commissioner Vestager, Studienvereinigung Kartellrecht, Brussels, 10 March 2016; caso No. COMP/M.7217 – FACEBOOK/WHATSAPP, §129 ss.

⁹ Cfr. provv. n. 26597 dell'11 maggio 2017, PS/10601, *Whatsapp trasferimento dati a Facebook*, in Boll. 18/2017; Provv. n. 26596 dell'11 maggio 2017, CV/154, *Whatsapp clausole vessatorie*, in Boll. 18/2017. Per un approfondimento, v. M. CAPPAL, S. PERUGINI, *Social economy e tutela dei consumatori: il ruolo dell'AGCM*, in *Consumerism 2017 – Dalla Sharing alla Social alla Data economy*, 24 novembre 2017. Inoltre, v. provv. n. 27432, PS/1112, *Facebook-Condivisione dati con terzi*, 29 novembre 2018, in Boll. 46/2018.

artt. 21 e 22 del Codice del consumo, avendo adottato una informativa carente nella fase di prima registrazione dell'utente nella piattaforma. Attraverso lo *slogan* «Iscriviti, è gratis e lo sarà per sempre», *Facebook* aveva informato gli utenti solo della gratuità del servizio, omettendo le finalità commerciali di utilizzo dei dati raccolti.

L'AGCM aveva, altresì, rilevato che il *social network* aveva posto in essere una pratica aggressiva, vietata dagli artt. 24 e 25 del Codice del consumo, nei confronti degli utenti registrati, i cui dati erano stati trasmessi per finalità di profilazione e commerciali dalla piattaforma social ai siti *web/app* di terzi e viceversa, senza preventivo consenso espresso dell'interessato, preselezionando la funzione di “attivazione della Piattaforma”. A fronte di tale preimpostazione automatica, all'utente sarebbe stata accordata una mera facoltà di *opt-out*, peraltro disincentivata dalla prospettazione di conseguenze penalizzanti, sia nella fruizione dei servizi offerti da *Facebook*, sia nell'accessibilità e nell'utilizzo di siti *web* e *app* di terzi ad esso collegati.

La vicenda che, come noto, è stata oggetto di valutazione anche da parte del *Bundeskartellamt*, dimostra che la violazione della normativa *data protection* può essere censurata, non solo dal punto di vista della disciplina consumeristica, ma anche sotto il profilo *antitrust*¹⁰. Secondo l'autorità tedesca, la *data policy* messa a punto da *Facebook*, imponendo agli utenti, in mancanza del prescritto consenso, di fondere nel profilo *Facebook.com* tutti i dati personali provenienti

¹⁰ Cfr. Comunicato stampa del 2 marzo 2016, da cui si evince che il *Bundeskartellamt* ha definito il mercato del prodotto come quello dei “social network”, così segmentando il (ben più ampio) mercato dell’“advertising-financed internet services”, all'interno del quale sarebbe più complicato dimostrare la posizione dominante di *Facebook*. E, ancora, v. *Bundeskartellamt, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, 15 February 2019.

dalle varie fonti, al fine di sfruttarli per scopi commerciali, configurava una violazione del divieto di abuso di posizione dominante di cui all'art. 19(1) GWB.

3. Cionondimeno, come evidenziato dalla stessa autorità indipendente tedesca, la mancata informazione dei consumatori del modo in cui saranno utilizzati i dati relativi alle loro preferenze, i dati personali e i dati generati dagli utenti, integra anzitutto una violazione della disciplina di protezione dei dati.

In proposito, alla luce della diffusa frequentazione delle piattaforme *online*, l'impostazione tradizionale secondo cui il dato viene ottenuto direttamente dall'interessato sulla base del consenso, o comunque individuando preventivamente le responsabilità del trasferimento delle informazioni che lo riguardano, viene sempre più spesso a confrontarsi col fenomeno del tutto inedito della raccolta dei dati personali acquisiti tramite *app* e siti *web* ¹¹.

Si pensi, per quanto in questa sede di interesse, ai dati degli utenti *online* raccolti mediante l'impiego di *cookie*, il cui uso varia dalla mera identificazione degli internauti, alla memorizzazione delle loro preferenze e alla raccolta di informazioni per finalità pubblicitarie o di *marketing* comportamentale *online*.

Sebbene la maggior parte dei *browser web* contempli la possibilità per i singoli utenti di preimpostare il rifiuto di *cookie* o di eliminarli

¹¹ Per approfondimenti sulle problematiche connesse alla configurazione delle app con specifico riferimento alle corrette modalità di manifestazione del consenso da parte degli utenti delle stesse, si rinvia allo studio condotto da ENISA, *Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR*, Novembre 2017.

all'occorrenza, solo di rado chi naviga sulla rete è accorto a modificare le impostazioni predefinite ¹².

Viene, in tal modo, in rilievo l'aspetto dell'individuazione dei requisiti in presenza dei quali il consenso al trattamento dei dati possa essere qualificato come liberamente manifestato, a fronte di un processo di accumulazione di tali dati generato da *cookie* di parti terze. La risposta passa necessariamente attraverso la soluzione del quesito se esista una differenza tra il mero trattamento dei dati personali e l'installazione di *cookie* con relativo accesso.

Il problema è stato sottoposto alla Corte di giustizia dal *Bundesgerichtshof* tedesco, nell'ottobre 2019 ¹³, attraverso un rinvio pregiudiziale avente ad oggetto la manifestazione del consenso all'utilizzo di *cookie*, nel quadro della disciplina europea di cui alla direttiva 2002/58, in combinato disposto con la direttiva 95/46, oggi con il GDPR.

La fattispecie concreta da cui è originato il giudizio riguarda l'utilizzo da parte di una società tedesca di una casella di spunta pre-selezionata mediante la quale gli internauti che aspirano a partecipare a giochi a premi esprimono, al contempo, il consenso all'installazione di *cookie* diretti a raccogliere informazioni a fini pubblicitari.

¹² V. O. LYNKEY, *Trak(ing) changes: an examination of EU Regulation of online behavioural advertising through a data protection lens*, in *European Law Review*, 2011, p. 878.

¹³ Cfr. Corte giust. (Grande Sezione), del 1° ottobre 2019, causa C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband eV / Planet49 GmbH*, ECLI:EU:C:2019:246.

È utile ricordare, nell'esame della controversa questione dell'ammissibilità delle impostazioni predefinite per le attività *online*, che l'art. 5, par. 3 della direttiva *e-Privacy*, come modificata nel 2009, si fonda sul sistema del previo consenso dell'utente (cd. *opt-in* informato) al trattamento dei dati tramite *cookie*, in armonia con quanto stabilito nella direttiva 95/46 e poi confermato nel GDPR ¹⁴.

Coerentemente con la *ratio* della previsione normativa da ultimo richiamata, che è quella di richiamare l'attenzione dell'utente rispetto al trattamento dei propri dati, la Corte ha sostenuto che il consenso all'installazione e alla consultazione di *cookie* sull'apparecchiatura terminale del soggetto interessato non è validamente manifestato in presenza di una casella di spunta preselezionata che lo stesso deve, peraltro, deselezionare al fine di negare l'autorizzazione al trattamento di propri dati.

A tal fine, la Corte di giustizia ha sottolineato la necessaria specificità del consenso che *«deve riferirsi precisamente al trattamento dei dati interessati e non può essere desunto da una manifestazione della volontà avente un oggetto distinto»*¹⁵. Pertanto, il fatto che un individuo attivi il pulsante di partecipazione ad un gioco a premi non è sufficiente per ritenere che quella manifestazione di volontà si estenda automaticamente all'installazione di *cookie* ¹⁶.

Tant'è che, hanno chiarito i giudici, il periodo di attività di *cookie*, nonché la possibilità o meno per i terzi di avere accesso ad essi rien-

¹⁴ Come osservato dal Gruppo di Lavoro Articolo 29, nelle *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 28 novembre 2017 e successivamente emendate il 10 aprile 2018, p. 5, secondo cui la «nozione di consenso rimane sostanzialmente simile a quella della direttiva 95/46/CE».

¹⁵ Cfr. sentenza *Planet49 GmbH*, cit. p. 58.

¹⁶ Cfr. sentenza *Planet49 GmbH*, cit. p. 59.

trano tra le informazioni che il fornitore di servizi deve comunicare all'utente, tenendo presente che le informazioni contenute nell'art. 10 della direttiva 95/46, e ora nell'art. 13, par. 2, lett. a), GDPR, «non sono elencate in modo esaustivo». Pertanto, «*l'informazione sul periodo di attività dei cookie deve essere considerata rispondente al requisito del trattamento leale dei dati previsto dal suddetto articolo, in quanto un lungo periodo di attività, o addirittura un periodo illimitato, implica la raccolta di numerose informazioni sulle abitudini di navigazione e sulla frequenza delle eventuali visite dell'utente ai siti dei partner pubblicitari dell'organizzatore del gioco a premi*»¹⁷.

Non vi sono dubbi, quindi, che le “informazioni” di cui alla direttiva *e-Privacy* costituiscano “dati personali”, con tutte le implicazioni che ne conseguono in termini di disciplina. In altri termini, se a seguito dell'inserimento o del trasferimento di informazioni attraverso *cookie* o meccanismi analoghi, esse possono essere considerate alla stregua di dati personali, oltre alla direttiva *e-Privacy*, si applica la direttiva 95/46 e, dunque, il GDPR¹⁸.

La soluzione accolta risponde all'esigenza di coordinare le diverse discipline e ben si concilia con lo spirito sotteso alla normativa in materia di protezione dei dati personali, in particolare con il principio di minimizzazione di essi, in forza del quale, qualora il titolare intenda raccogliere dati ulteriori rispetto a quelli in suo possesso o trattarli per finalità diverse da quelle per le quali sono stati originariamente

¹⁷ Cfr. sentenza *Planet49 GmbH*, cit. p. 78. Inoltre, v. in merito la posizione enunciata il 14 novembre 2019 dall'Hamburg Commissioner for Data Protection and Freedom of Information, *Google Analytics and similar services can only be used with consent*.

¹⁸ Diversamente, nella causa *Wirtschaftsakademie*, la Corte ha applicato la direttiva 95/46, sebbene il trattamento dei dati sottostante coinvolgesse anche ambiti che rientrano nel campo di applicazione materiale della direttiva *e-Privacy*.

raccolti, deve sempre chiedere nuovamente il consenso dell'interessato.

4. L'adeguata informazione e il previo consenso degli utenti alla raccolta e all'utilizzo dei dati personali, dunque, costituiscono gli aspetti cruciali della disciplina sull'uso delle tecnologie di *webtracking* contenuta nella direttiva *e-Privacy*.

In attuazione di tali precisazioni tutti i siti *web* hanno installato un "cookie bar", cioè una barra che informa gli utenti sulla presenza di meccanismi di monitoraggio rispetto all'uso dei quali sono invitati a prestare il proprio consenso.

Pur tuttavia, la valutazione di conformità delle operazioni di monitoraggio comportamentale degli utenti alla normativa dell'Unione europea, ha richiesto l'intervento della Corte di giustizia per chiarire l'ampiezza della nozione di "responsabile del trattamento" e degli obblighi connessi.

In proposito, emblematica è la giurisprudenza in materia di corresponsabilità dell'amministratore di una *fanpage* di *Facebook* e dello stesso *social network* per il trattamento dei dati personali dei visitatori della pagina ¹⁹ e quella in materia di responsabilità congiunta di *Facebook* e del gestore di un sito Internet corredato del pulsante "mi

¹⁹ Cfr. Corte giust. 5 giugno 2018, causa C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, su cui sia consentito rinviare a A. CORRERA, *Dati personali: la nozione di "responsabile del trattamento" include il gestore di una fanpage presente su un social network*, in *DPCE Online*, oct. 2018.

piace” dello stesso *social*, per la raccolta e la trasmissione dei dati personali dei visitatori del sito ²⁰.

In particolare, il giudice di Lussemburgo ha esteso la nozione di “responsabile del trattamento” ²¹ all’amministratore di una *fanpage* (*Wirtschaftsakademie*), oltre che al gestore del *social network*, e ne ha ravvisato la responsabilità congiunta con riferimento al trattamento dei dati degli utenti.

Tale conclusione si fonda sulla premessa per cui, creando la *fanpage*, l’amministratore offre al *social network* «la possibilità di posizionare cookie sul computer o su qualsiasi altro dispositivo della persona che ha visitato la pagina» ²² e compie un’«azione d’impostazione dei parametri» ²³, attraverso cui di fatto partecipa con il *social* alla determinazione delle finalità e degli strumenti del trattamento dei dati personali dei visitatori medesimi. Il trattamento in questione, come ben rilevato dalla Corte, consente sia alla *Facebook Ireland* sia alla *Wirtschaftsakademie* «di migliorare il proprio sistema di pubblicità», accrescendone reciprocamente la visibilità sul *web*.

Considerazioni non dissimili caratterizzano il giudizio *Fashion ID*, in virtù del quale il gestore di un sito Internet, che con un *plug-in social* consente al *browser* del visitatore del medesimo sito di richiamare

²⁰ Cfr. Corte giust. 20 luglio 2019, causa C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW e V.*

²¹ v., in tal senso, *Wirtschaftsakademie*, cit., punti 26 e 27

²² v., in tal senso, *Wirtschaftsakademie*, cit., punto 35.

²³ v., *Wirtschaftsakademie*, cit., punto 36, ove la Corte osserva che «la creazione di una *fanpage* su Facebook [Ireland] implica da parte del suo amministratore un’azione d’impostazione dei parametri in base al suo pubblico destinatario nonché agli obiettivi di gestione o di promozione delle sue attività, che influisce sul trattamento di dati personali ai fini della creazione di statistiche stabilite a partire dalle visite della *fanpage*».

contenuti del fornitore del *plug-in* e trasferire allo stesso fornitore i dati personali del visitatore, deve essere considerato “responsabile del trattamento” insieme al *social network*.

Va osservato che, sebbene la *Fashion ID*, diversamente dalla *Wirtschaftsakademie* coinvolta nel precedente giudizio, non determinasse i parametri delle informazioni relative agli utenti del suo sito Internet, anche in tal caso, il “beneficio” ambito è la pubblicità gratuita dei prodotti commercializzati. E, quantunque l’uso specifico dei dati non sia lo stesso, tanto la *Fashion ID* quanto la *Facebook Ireland* perseguono complessivamente scopi commerciali reciprocamente complementari; ciò vale a dire che, pur se non è rinvenibile un’identità, c’è quantomeno un’unità di intenti connessa al comune scopo commerciale e pubblicitario ²⁴.

Le fattispecie ricordate dimostrano che, affinché un soggetto possa essere considerato come responsabile del trattamento, non è necessario che disponga di un potere di controllo completo su tutti i singoli profili del trattamento medesimo ²⁵. In particolare, a fronte della natura ormai complessa dei “trattamenti dei dati”, in cui sono coinvolti soggetti diversi che esercitano gradi di controllo differenti, è verosimile che la loro compartecipazione assuma forme varie e che, pertanto, possa non essere ripartita in modo uguale.

Così, la Corte ha escluso che il riconoscimento di una corresponsabilità comporti un automatico ed equivalente grado di responsabilità dei diversi operatori. È necessario cioè procedere ad una valutazione

²⁴ Cfr. Conclusioni dell’Avvocato generale Michael Bobek, 19 dicembre 2018, in causa C-40/17, *Fashion ID*, punto 105.

²⁵ In senso conforme, v. Corte giust. 10 luglio 2018, causa C-25/17, *Jehovan todistajat*, punti da 68 a 72.

delle circostanze del caso concreto e del livello di coinvolgimento dei singoli operatori nel trattamento dei dati, di modo che la responsabilità di ciascuno sarà limitata alla propria area di influenza effettiva ²⁶.

5. Le problematiche esposte si inseriscono in processi in continuo divenire che, a fronte di un apparato normativo non sempre adeguato, impongono alla Corte di giustizia di confrontarsi con il dinamismo che li caratterizza.

L'inadeguatezza del quadro giuridico europeo, non congegnato nell'era di *Internet* e dei *Big Data* propri del web 2.0 ²⁷, è stata solo in parte superata dall'intervento del legislatore, rendendo necessario quello chiarificatore e costante della Corte di Lussemburgo.

In questa ottica, il regolamento europeo sulla protezione dei dati personali ha tracciato due direttrici fondamentali: da una parte, la maggiore responsabilizzazione dei soggetti attivi del trattamento; dall'altra parte, la previsione di strumenti atti ad accrescere il livello di consapevolezza degli utenti sull'uso dei propri dati.

Entrambe le linee d'azione hanno evidentemente guidato l'attività interpretativa della Corte di giustizia nelle pronunce richiamate, in cui, accanto ad un innalzamento del livello di controllo sui dati degli individui, nella difesa di alcuni canoni tradizionali del diritto dell'Unione, la cui solidità non è revocabile in dubbio ²⁸, non si può

²⁶ Cfr. *Fashion ID*, cit., punto 70.

²⁷ in tal senso, S. FARO, N. LETTIERI, *Big Data e Internet delle cose: opportunità, rischi e nuove esigenze di tutela per gli utenti della Rete*, in L. RUGGERI, C. PERLINGIERI (a cura di), *Internet e diritto civile*, Napoli, 2015, p. 279.

²⁸ Vedi conclusioni dell'avvocato generale Szpunar nella causa *Planet49*, cit., p. 57 ss. E ancora, dello stesso avvocato generale, conclusioni del 4 marzo 2020, in causa

non registrare anche un inevitabile aggravamento degli oneri e dei pesi imposti alle imprese digitali.

Entro questo quadro, i giudici europei preservano la *ratio* del consenso, quale caratteristica essenziale della disciplina sulla protezione dei dati dell'Unione, che trova espressa menzione nell'art. 8, par. 2, della Carta dei diritti fondamentali²⁹. Sicché, soltanto se il consenso è libero, specifico e informato ottempera ai criteri del regolamento 2016/679 e protegge ciascun individuo da situazioni per loro stessa natura asimmetriche.

Accanto a questo profilo, tuttavia, l'operazione di adeguamento del sistema di tutela in esame, in punto di responsabilità dei soggetti coinvolti nel trattamento dei dati personali, compiuta dalla Corte Ue ha probabilmente deluso le aspettative. Non può ignorarsi che sarebbe stato opportuno un maggiore sforzo esplicativo da parte dei giudici europei nell'indicare i criteri utili a distinguere il diverso coinvolgimento degli operatori *web* nell'attività di trattamento dei dati digitali. Al contrario, la Corte si è limitata ad affermare che la nozione di

C-61/19, *Orange România SA c. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, punti 34-47. V. altresì D. HECKMANN, A. PASCHKE, *Artikel 7*, in E. EHMANN, M. SELMAYR, (a cura di), *Datenschutz-Grundverordnung, Kommentar*, Munich, 2018, p. 9.

²⁹ Cfr. F. PICOD, S. VAN DROOGHENBROECK, *Charte des droits fondamentaux de l'Union européenne: Commentaire article par article*, Bruxelles, 2018; O. POLLICINO, M. BASSINI, *Commento all'art. 8 CdfUE*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, 2017, p. 132; F. DONATI, *Protezione dei dati personali*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001, p. 83; J. RIDEAU, *Droit institutionnel de l'Union et des Communautés européennes*, Parigi, 2006, p. 349; G. GONZÁLEZ FUSTER, R. GELLER, *The fundamental right of data protection in the European Union: in search of an uncharted right*, in *International Review of Law Computers and Technology*, 2012, p. 73.

“responsabile del trattamento” deve essere interpretata in senso ampio³⁰ e a configurare in via generica un controllo e una responsabilità congiunti³¹, pur nella diversità tecnica delle fasi di raccolta e trasferimento dei dati. Il che lascia al giudice interno la valutazione in dettaglio delle situazioni, rischiando di complicare il contesto normativo e di alterare il rapporto tra gli oneri e i pesi imposti agli attori interessati³².

Nonostante le criticità che le assimilazioni tra i soggetti coinvolti nel trattamento dei dati pongono all’interprete, va, però, sottolineato che esse si accompagnano ad opportunità, ancora inesplorate, connesse alla possibilità di sovrapporre i diversi impianti normativi coinvolti, quello consumeristico e *antitrust* con quello sulla *privacy*.

Su tale versante, la tutela dei dati personali potrebbe essere complementare alla normativa a tutela del consumatore e a quella *antitrust*, poiché quanto più gli utenti/consumatori sono informati, consapevoli e liberi nelle loro scelte, tanto più le imprese sono proiettate a competere tra di loro attraverso una diversificazione dei servizi digitali che offrano una qualità più alta sotto forma di *privacy*. In definitiva, più intensa è la tutela della persona, più si argina il potere di mercato del-

³⁰ La Corte, in particolare, richiama espressamente il suo precedente del 13 maggio 2014, causa C-131/12, *Google Spain*.

³¹ Sul punto, v. J. MAROSI, *Who Controls a Facebook Page?*, in *VerfBlog*, 6 giugno 2018.

³² Proprio nel tentativo di fare chiarezza, il Comitato europeo per la protezione dei dati ha ridiscusso e aggiornato le linee guida con riferimento ai soggetti rilevanti per il trattamento dei dati personali. Cfr. [Guidelines on the concepts of controller, processor and joint controllership under Regulation \(EU\) 2018/1725](#), che analizzano i concetti di titolare, responsabile e contitolare riconfermando in buona sostanza le indicazioni e le classificazioni fornite dal WP29 nell’Opinion 1/2010.

le piattaforme *online*, garantendo il risultato di una più compiuta tutela del consumatore³³.

Alla luce di ciò, il legislatore dell'Unione dovrebbe tendere alla realizzazione di uno standard di tutela uniforme, all'occorrenza adattando gli strumenti regolativi esistenti all'obiettivo della trasparenza e del controllo.

³³ Cfr. C. SCHEPISI, *Comunicazione, nuove tecnologie e tutela dei consumatori. L'evoluzione del diritto dell'Unione europea*, in *Mercato e consumatori*, Edizione speciale quaderno informativo, 2019, p. 47 ss.