GIUSTIZIA INSIEME

Europa e Corti Internazionali*

Trasferimento dati del visitatore di sito web tramite social plug-in e titolarità del loro trattamento. La forma della protezione dei dati - il caso Fashion id (nota a Corte giust. Ue, 29 luglio 2019, causa C-40/17) di Federico Sartore

di Federico Sartore

10 luglio 2020

Trasferimento dati del visitatore di sito *web* tramite *social plug-in* e titolarità del loro trattamento. La forma della protezione dei dati - il caso *Fashion id* (nota a Corte giust. Ue, 29 luglio 2019, causa C-40/17)

di Federico Sartore

Corte giust. Ue, 29 luglio 2019, causa C-40/17 - Sez. II - *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*[*]

Privacy (tutela della) - Internet - Direttiva 95/46/CE, GDPR, e-privacy - Dati personali - Trasferimento su piattaforma *social* - Trattamento - Gestore sito - Titolarità.

(direttiva 95/46/ce, art. 2(d), art. 7(f), art. 7(a), art. 2(h), art. 10; regolamento (ue) 2016/679, art. 26)

1. *Il gestore di un sito internet che implementa un* social plug-in *che trasferisca alla piattaforma* social *dati personali del visitatore, può essere considerato titolare del trattamento. Questa qualifica è tuttavia limitata all'operazione o all'insieme delle operazioni di trattamento dei dati personali per le quali il gestore determina effettivamente finalità e mezzi (nel caso di specie la raccolta e la comunicazione mediante trasmissione).*

Privacy (tutela della) - Internet - Direttiva 95/46/CE, GDPR, e-privacy - Dati personali - Trasferimento su piattaforma *social* - Gestore sito - Fornitore di piattaforma social - Contitolarità - Legittimo interesse - Consenso.

2. *Affinché i trattamenti di dati personali siano leciti nel caso di implementazione di un* social plug-in*, è necessario che sia il gestore del sito, sia il fornitore della piattaforma* social *perseguano ciascuno un legittimo interesse.*

[v. Corte giust. Ue, 5 giugno 2018, C-210/16 *Wirtschaftsakademie Schleswig-Holstein*; Corte giust. Ue, 10 luglio 2018 C-25/17, *Tietosuojavaltuutettu v. Jehovan todistajat*]

Abstract

Analizzando una recente pronuncia della Corte di Giustizia, l'articolo ragiona sulla complessa conciliazione delle categorie giuridiche della protezione dei dati personali in un ambiente fortemente dematerializzato come quello online. In particolare, rispetto al delicato regime della contitolarità tra Direttiva 95/46/CE e Regolamento (UE) 2016/679. In conclusione, si affronta il tema, anche politico, dell'applicabilità della normativa in materia di protezione dei dati ai giganti del tech.

By analysing a recent case before the Court of Justice of the European Union, the paper focuses on the complex conciliation of legal categories of data protection in the highly dematerialized online environment. Particular attention is paid to the intricate legal regime of joint controllership, between Directive 95/46 / EC and Regulation (EU) 2016/679. Conclusions are devoted to the means of enforcement of data protection vis-à-vis the so-called data barons.

1. Premessa

Come è noto, il regime giuridico europeo posto a tutela dei dati personali ha trovato il suo primo statuto di dettaglio nella Direttiva 95/46/UE[1], il cui impianto concettuale e definitorio è stato poi sostanzialmente mutuato dal Regolamento (UE) 2016/679[2] (l'ormai celebre GDPR). Una volta delineato l'oggetto della tutela, il legislatore europeo del '95 ha avuto il merito di risalire la corrente dei dati per strutturare i poli di responsabilità sui quali poggiare il sistema degli obblighi. Questa operazione di necessaria semplificazione ed astrazione ha portato all'elaborazione delle ben note figure di «titolare» e «responsabile» del trattamento[3]. Nel corso degli anni, la prassi applicativa e lo sviluppo tecnologico hanno sottoposto a notevoli torsioni concettuali la flessibilità di queste categorie, al punto che oggi l'interprete si trova quotidianamente dinanzi all'interrogativo circa la qualificazione più corretta da dare ai numerosi «soggetti dati» che si avvicendano e intersecano nella gestione e determinazione dei trattamenti di dati personali[4]. Anche le Autorità di sorveglianza, chiamate a svolgere il proprio ruolo di guida all'interpretazione del dettato normativo, hanno faticato a gestire in maniera lineare la qualificazione in concreto; utilizzando a volte criteri *extra*-testuali per risolvere le situazioni più controverse, facendo riferimento ad esempio alla percezione dell'utente e all'affidamento dell'interessato rispetto al contenuto delle attività di trattamento[5] ovvero, in altri casi, aderendo al dettato letterale del Regolamento e utilizzando come criterio determinante il fatto che si tratti di attività delegate all'esterno dell'organizzazione da parte del titolare del trattamento[6]. Diversamente da quest'ultima linea interpretativa, e solo a titolo di esempio, l'*Information Commissioner Office* britannico (ICO) ritiene che alcune professioni siano soggette ad obblighi deontologico-professionali tali da escludere in radice la possibilità di qualsivoglia forma di etero-direzione, configurandosi quindi *in re ipsa* come svolte da autonomi titolari del trattamento[7]. Al contempo, come si avrà modo di approfondire nel corso della trattazione, la Corte di Giustizia dell'Unione Europea (anche, CGUE) ha negli anni ritenuto preferibile l'adozione di un criterio teleologico, consistente nel garantire un livello elevato di protezione per i diritti e le libertà degli interessati, arricchendo implicitamente in questo modo la silhouette normativa delle disposizioni in materia dei dati secondo il principio per cui i casi di qualificazione controversa devono essere risolti nel senso di preferire la configurazione più tutelante per gli interessati. Piegando e subordinando così la qualificazione giuridica di (con)titolari e responsabili del trattamento a seconda delle menzionate necessità di tutela. Nel caso che si discute in questa nota, la Corte di giustizia UE ha confermato questa tendenza tipicamente orientata ai fini, esponendosi alle critiche di chi ha ritenuto superficiale l'analisi di una situazione di fatto caratterizzata dall'intrecciarsi di trattamenti di dati non facilmente distinguibili, sottovalutando (financo svilendo) la complessità e le modalità di funzionamento della tecnologia sottesa al caso di specie[8]. L'importanza e la complessità del ruolo svolto dalla

Corte in questa pronuncia sono altresì confermati dal tenore e dalla vicinanza cronologica delle pronunce della medesima autorità in merito al significato da darsi in concreto alle definizioni di titolare e responsabile del trattamento**[9]**; senza dimenticare la recente emanazione di specifiche linee guida in materia da parte dello *European Data Protection Supervisor* (EDPS), l'autorità Garante per i trattamenti svolti dalle istituzioni europee**[10]**.

Nel caso in analisi la CGUE ha dovuto confrontarsi con la qualificazione e il ruolo di contitolari del trattamento ai sensi della normativa in materia di protezione dei dati personali**[11]**. In particolare, con riferimento alla relazione intercorrente tra il gestore di una pagina web ed il fornitore di un *plug-in***[12]** incorporato all'interno della pagina stessa, nonché sui presupposti di liceità (anche detti basi giuridiche) di simili trattamenti di dati personali. Si sottolinea che le questioni sottese al rinvio pregiudiziale alla Corte di Giustizia UE riguardano l'interpretazione delle disposizioni dell'abrogata Direttiva 95/46/UE. Tuttavia, stante la sostanziale continuità giuridico-normativa tra Direttiva Madre e GDPR rispetto agli istituti descritti ed affrontati dalla Corte, le valutazioni svolte dai giudici di Lussemburgo trovano piena applicazione anche in riferimento al GDPR. Tuttavia, nel caso in cui le differenze tra regimi giuridici dovessero riverberarsi sulle conseguenze tratte dalla Corte, sarà cura di chi scrive sottolineare le sfumature, anche connesse al (parzialmente) mutato impianto concettuale di riferimento.

2. La vicenda e le questioni pregiudiziali sottoposte alla corte

Nel caso in analisi, la *Fashion ID*, un'impresa di abbigliamento moda *online* ha incorporato all'interno del proprio sito *web* il *plug-in* «Mi Piace» di Facebook, il noto *social network*. Per far funzionare queste tipologie di software, il gestore del sito principale deve includere al proprio sito internet un collegamento con il contenuto offerto dal fornitore del servizio. Nel momento in cui un visitatore chiede al proprio *browser* di mostrargli il sito in questione, la pagina *web*, mediante il collegamento, richiama il contenuto esterno e lo incorpora nella propria presentazione grafica (secondo le preferenze dei programmatori). Affinché ciò accada, il *browser* deve necessariamente comunicare al *server* del fornitore esterno l'indirizzo IP**[13]** del terminale dell'utilizzatore, i dati tecnici del *browser* medesimo oltre ad altre informazioni sul contenuto richiesto. Infatti, solo in questo modo il *server* può stabilire in quale formato il contenuto esterno debba essere inviato a tale indirizzo IP. Un'importante precisazione a livello tecnico riguarda il controllo del gestore del sito su raccolta e successiva utilizzazione delle informazioni raccolte da parte del fornitore del *plug-in*: infatti, il gestore che integra un *plug-in* all'interno del proprio sito non può verificare che dati il *browser* trasmetta e, ovviamente, nemmeno gli utilizzi successivi

svolti dal terzo**[14]**. Un ultimo ed importante elemento da sottolineare riguarda l'ampiezza e consapevolezza della platea dei visitatori interessati dalla raccolta e trasmissione dei dati mediante il *plug-in*. Infatti, risulta che la trasmissione dei dati avviene a prescindere che il visitatore sia o meno iscritto al *social network* ovvero interagisca in alcun modo con il pulsante « *Like*» e, in ogni caso, senza che ne sia consapevole**[15]**.

La vicenda giudiziaria da cui è originato il rinvio pregiudiziale alla Corte vedeva la Verbraucherzentrale NRV (associazione per la tutela dei diritti dei consumatori) contestare alla Fashion ID la trasmissione di dati personali dei visitatori a Facebook Ireland perché (a) avvenuta in assenza di manifestazioni di consenso e (b) in violazione degli obblighi informativi stabiliti dalla normativa in materia di protezione dei dati**[16]**. Al fine di veder cessare questo flusso di dati personali a favore di Facebook Ireland, la Verbraucherzentrale NRV proponeva un'azione di natura inibitoria nei confronti della Fashion ID, dinanzi al Landgericht Düsseldorf**[17]**. Interpellato, il Landgericht accoglieva solo in parte le pretese dell'associazione dei consumatori tedesca**[18]**. A sua volta, la parzialmente soccombente Fashion ID proponeva appello dinanzi all'Oberlandesgericht Düsseldorf. Contestualmente la Verbraucherzentrale NRV proponeva appello incidentale al fine di estendere la pronuncia favorevole ai capi esclusi**[19]**.

Proprio l'Oberlandesgericht Düsseldorf, ritenuto di trovarsi dinanzi a questioni di interpretazione di normativa Ue, sospendeva il procedimento e sottoponeva alla Corte di Giustizia UE sei questioni pregiudiziali.

In particolare, il giudice a quo si è chiesto preliminarmente se (a) la Direttiva 95/46 ponesse limiti agli Stati Membri rispetto al riconoscimento ad associazioni per la tutela dei consumatori del diritto di agire in giudizio nei confronti degli autori di eventuali violazioni. Solo in caso di riscontro positivo alla prima questione, il giudice del rinvio ha interrogato la Corte con questioni di merito. Si è quindi domandato (b) se la Fashion ID potesse essere considerata, ai sensi dell'art. 2(d) della DPD, «titolare del trattamento» dei dati trasmessi a Facebook Ireland, pur non esercitando alcuna forma di dominio sulle operazioni di trattamento. Subordinatamente ad una risposta negativa alla seconda questione, alla Corte è stato richiesto (c) se la Direttiva dettasse una disciplina completa in materia di responsabilità (ostando infatti alla proposizione di azioni civili nei confronti di soggetti non titolari del trattamento e ugualmente coinvolti in processi di trattamento). Muovendo poi dalla qualificazione dei ruoli alla liceità dei trattamenti svolti, la Corte tedesca si è posta il problema di (d) quale fosse il legittimo interesse**[20]** perseguito [dal titolare] al fine di svolgere il bilanciamento richiesto dall'art. 7(f) della Direttiva**[21]**. Infine, alla Corte di Giustizia è stato chiesto (e) a chi dovrebbe essere eventualmente reso il consenso al

trattamento dei dati previsto dall'art. 7(a) e 2(h) della DPD, nonché (f) se gli obblighi di trasparenza di cui all'art. 10 della Direttiva riguardassero anche Fashion ID – in quanto soggetto che aveva attivamente inserito il *plug-in* di Facebook, ponendosi quindi come antecedente causale al trattamento dei dati da parte di quest'ultima.

3. La legittimazione attiva delle associazioni di tutela dei consumatori

Come menzionato, la prima questione pregiudiziale affronta una tematica di natura procedurale, ossia la vincolatività in senso negativo o meno degli articoli 22, 23 e 24 della DPD rispetto a normative nazionali che consentano ad associazioni per la tutela dei consumatori di agire in giudizio contro il presunto autore di una lesione del diritto alla protezione dei dati**[22]**. Sebbene la questione non sia triviale – anche perché la Direttiva non contiene previsioni esplicite in questo senso – bisogna sottolineare che la Corte si è già espressa in passato in connessione a procedimenti intentati da associazioni dei consumatori**[23]**. Alla legittima precisazione secondo cui la Corte in dette occasioni non sarebbe stata investita direttamente della questione interpretativa può ribattersi che la stessa avrebbe potuto in ogni caso, magari in forma di *obiter dicta*, sollevare qualche dubbio sulla sussistenza della legittimazione attiva in capo all'associazione, eventualità mai verificatasi.

In sintesi, la Corte ribadisce il principio chiave della propria giurisprudenza in materia di protezione dei dati, ossia che uno degli obiettivi della DPD è quello di garantire una tutela efficace e completa dei diritti e delle libertà delle persone fisiche rispetto al trattamento dei dati personali**[24]**. In secondo luogo, la Corte chiarisce correttamente che l'assenza di previsione espressa non può in alcun caso ritenersi equivalente ad un divieto, di modo che l'assenza di norme esplicite in senso positivo non fanno venir meno la possibilità per i legislatori nazionali di contemplare le associazioni per la tutela dei consumatori nel novero dei legittimati attivi in questioni aventi ad oggetto la protezione dei dati. Da ultimo, ricollegandosi concettualmente al menzionato principio di tutela efficace e completa, la pronuncia ribadisce l'ampio margine di discrezionalità lasciato agli Stati membri per il perseguimento degli obiettivi tracciati dalla Direttiva Madre**[25]**. Da ciò ne consegue il carattere non ostativo del dettato normativo della Direttiva rispetto alla legittimazione attiva delle associazioni dei consumatori prevista ai sensi degli ordinamenti nazionali**[26]**.

In merito alla prima questione si sottolinea la scarsa rilevanza pratica del tema in ottica futura: infatti, il neo-introdotto art. 80(2) del GDPR contempla in maniera esplicita tale possibilità per gli

stati membri[27]. Tuttavia, come sottolinea Globocnik, non è escluso che la risposta della Corte possa avere un più ampio respiro in materia di protezione del consumatore e pratiche commerciali scorrette[28]. Infatti, la decisione chiarisce che il fatto che la Direttiva non rientri tra le direttive elencate dall'Allegato I della Direttiva 2009/22/CE[29] non preclude la possibilità per gli Stati Membri di introdurre norme che garantiscano la legittimazione attiva alle associazioni poste a tutela dei consumatori. In senso maggiormente tecnico, la Corte ha chiarito che la Direttiva 2009/22/CE, ai sensi dell'art. 7 della medesima, non ha operato un'armonizzazione esaustiva, lasciando quindi anch'essa ampio margine di discrezionalità agli Stati Membri[30]. Dello stesso avviso si è dimostrato l'avvocato generale Bobek, il quale ha sottolineato la sorpresa che avrebbe generato una conclusione opposta – che avrebbe quindi interpretato l'elenco esemplificativo contenuto nell'Allegato I della Direttiva 2009/22/CE nel senso di privare gli stati membri della loro potestà di scelta in merito a come dare attuazione alla DPD, come invece previsto dall'art. 288 del TFUE[31].

4. La (con)titolarità del trattamento di *Fashion id*

Dopo aver esaurito con esito positivo la disamina della prima questione, di natura marcatamente procedurale, la Corte si è apprestata ad affrontare il tema centrale della decisione: se la Fashion ID, per il fatto di inserire un *plug-in social* che consente di trasferire a Facebook dati personali del visitatore, possa essere considerato titolare del trattamento[32].

Rispetto al nucleo centrale del tema a sua volta centrale, la Corte si muove sicura nel solco tracciato dalle proprie decisioni precedenti sullo stesso tema. Infatti, ricordato che la nozione di titolare del trattamento deve essere interpretata estensivamente al fine di garantire l'elevato grado di tutela dei diritti di cui sopra[33], la Corte conferma la conclusione a cui era giunta nel caso *Wirtschaftsakademie Schleswig-Holstein* – quando aveva stabilito che l'amministratore di una pagina Facebook è titolare dei dati che raccoglie congiuntamente al *social network*[34]. Tuttavia, così come fatto nel caso *Jehovan todistajat,* i giudici aggiungono ulteriori elementi al ragionamento logico-giuridico svolto in *Wirtschaftsakademie Schleswig-Holstein*. In primo luogo, la Corte non ritiene più così essenziale la valutazione di chi stabilisca i parametri del trattamento, elemento che aveva giocato un ruolo preminente nel valutare la titolarità dell'amministratore della pagina, che era infatti in grado di influenzare le categorie di dati raccogliende[35]. Infatti, è stata ritenuta sufficiente e determinante la possibilità di Fashion ID di inserire o meno il *plug-in* di Facebook all'interno del proprio sito, quasi come se si trattasse di un interruttore, che non ammette modulazioni tra *on* e *off*[36]. Successivamente, la Corte effettua il

test di contitolarità rilevando la contestuale presenza di determinazione congiunta di mezzi e finalità da parte di Fashion ID e Facebook[37]. Il secondo movimento di differenziazione rispetto a *Wirtschaftsakademie Schleswig-Holstein* riguarda i limiti alla responsabilità del gestore del sito internet, circoscritti alla raccolta e alla comunicazione mediante trasmissione dei dati[38].

Proprio sul tema dei confini della responsabilità tra le parti si confrontano come antagoniste le esigenze di tutela perseguite dalla Corte nel suo ruolo quasi-legislativo e la ricerca di soluzioni stilisticamente più eleganti e aderenti alla lettera della DPD (e del Regolamento). Infatti, la Corte, distanziandosi dal mero atteggiamento ricognitivo mostrato in *Wirtschaftsakademie Schleswig-Holstein*, ci tiene a spiegare che l'esistenza di una responsabilità congiunta non implica necessariamente una responsabilità equivalente.

È avviso di chi scrive che a questo punto si crei una sorta di cortocircuito nel ragionamento dei giudici di Lussemburgo. Infatti, la CGUE prima spiega che «*[i contitolari] possono essere coinvolti in fasi diverse di tale trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie*»; poi tuttavia aggiunge che «*le operazioni di trattamento di dati personali di cui la Fashion ID, congiuntamente con la Facebook Ireland, può determinare le finalità e gli strumenti sono, […],* la raccolta e la comunicazione *mediante trasmissione dei dati personali dei visitatori del suo sito Internet*». Considerando che (i) la finalità per cui la Fashion ID trattava i dati, ossia l'incorporazione del *plug-in* di Facebook all'interno della propria pagina web, non poteva essere raggiunta con le mere operazioni di raccolta e comunicazione dei dati[39] e che (ii) la Corte ha ribadito la propria massima secondo cui la responsabilità congiunta di vari soggetti per un medesimo trattamento, ai sensi di tale disposizione, non presuppone che ciascuno di essi abbia accesso ai dati[40], la naturale conseguenza sarebbe stata estendere la (con)titolarità della Fashion ID ad ogni operazione di trattamento dati necessaria al caricamento del *plug-in*. Tuttavia, così facendo si sarebbe probabilmente perso un criterio certo per delimitare le reciproche sfere di responsabilità. Il ragionamento seguito dalla Corte per giungere al proprio riparto di responsabilità è spiegato con dovizia di particolari dall'AG Bobek, il quale, ricordando che nel diritto moderno la responsabilità oggettiva deve essere concepita come eccezione giustificata, spiega per immagini che grandi responsabilità devono essere associate a grandi poteri[41].

A questo punto la Corte avrebbe potuto abbracciare integralmente le premesse dell'AG Bobek, utilizzando la signoria effettiva sulle operazioni di trattamento come criterio di allocazione di ruoli e responsabilità ovvero avrebbe potuto estendere l'ambito della contitolarità a tutti i

trattamenti necessari al raggiungimento del fine condiviso, a prescindere dal potere effettivo, utilizzando poi detto criterio per una ripartizione (a questo punto non graficabile) della responsabilità reciproca tra le parti. La Corte ha stranamente deciso di incrociare queste due linee argomentative, giungendo ad una conclusione ibrida e, per questo motivo, criticabile. Infatti, ha usato il criterio del potere sulle operazioni non tanto per delimitare le responsabilità ma per segnare con un tratto di penna il limite esterno della contitolarità. La conclusione a cui giunge la Corte potrebbe anche essere ritenuta coerente, a patto di passare dal regime di contitolarità a quello di autonoma titolarità del trattamento. Infatti, la netta cesura rappresentata dalla comunicazione dei dati a Facebook ben potrebbe sposarsi con una configurazione dei ruoli che vedesse la Fashion ID raccogliere i dati e comunicarli ad un altro titolare del trattamento per il perseguimento ciascuno delle proprie finalità (che infatti la Corte identifica come distinte). Tuttavia, così facendo si sarebbe dovuto contraddire (correttamente) l'estensione del regime di contitolarità operato negli anni dalla giurisprudenza UE.

Diversamente, un'interpretazione che avesse ravvisato l'unicità del fine e dei mezzi tra le parti avrebbe dovuto estendere l'ambito dei trattamenti in contitolarità fino al completo caricamento del *plug-in*, non arrestandosi quindi alla comunicazione dei dati da Fashion ID a Facebook Ireland. In questa seconda configurazione i confini della responsabilità sarebbero stati sicuramente più sfuggevoli da identificare ma comunque ipotizzabili come asimmetrici in ragione dei diversi ruoli svolti tra le parti.

Provando a speculare sulle ragioni della Corte, è innegabile che limitare l'ambito di responsabilità della Fashion ID alle operazioni di raccolta e comunicazione dei dati fornisce un quadro applicativo chiaro per tutti i gestori di siti che implementano al proprio interno *social plug-in*. Tuttavia, il rischio che si corre è quello di trascurare le complessità (e l'opacità) delle operazioni necessarie al caricamento del *plug-in* sul *browser* del visitatore. Pur comprendendo le esigenze di tutela che hanno guidato i giudici europei, nonché le difficoltà di convivenza tra le categorie definitorie della DPD e l'ambiente online, è innegabile che la scelta di impostare teleologicamente le proprie decisioni porti necessariamente la Corte a dover incappare in alcune (più o meno apprezzabili) contraddizioni – che rendono più complessa l'attività di analisi e allocazione del rischio da parte di attori economici e interpreti nazionali.

5. Applicabilità della direttiva *e-privacy* e legittimo interesse

Dismessa per irrilevanza la terza questione pregiudiziale, la Corte è chiamata a spiegare se in un caso come in quello in analisi il giudice *a quo* debba indagare la sussistenza del legittimo interesse perseguito dal gestore del sito ovvero dal *social network*, al fine di valutare la liceità o meno del trattamento.

Come primo passaggio logico-argomentativo, la CGUE ritiene sia compito del giudice del rinvio verificare se la Facebook Ireland avesse accesso a informazioni archiviate nell'apparecchiatura terminale, ai sensi dell'art. 5(3), della Direttiva 2002/58/CE**[42]** (la Direttiva e-Privacy)**[43]**. In questo modo la Corte purtroppo fa un passo di lato, decidendo di non fornire la propria opera ermeneutica rispetto alla disciplina speciale dettata dalla Direttiva e-Privacy. Il dibattito sul punto è stato molto acceso e, anche in ragione della complessa gestazione che sta vivendo il processo di riforma della e-Privacy**[44]**, si ritiene importante toccare tangenzialmente la questione**[45]**. Secondo la Commissione, infatti, la questione posta alla Corte è irrilevante poiché il consenso dell'utente deve essere in ogni caso prestato**[46]**. Tuttavia, l'AG e ed il collegio giudicante ritengono che poiché i dati trasmessi non si limitano necessariamente ad informazioni archiviate sui terminali degli utenti, la questione circa l'applicabilità di una base giuridica «generale» ai sensi della DPD non possa essere elusa.

Ciò chiarito, la decisione ricorda cosa si intenda per legittimo interesse del titolare o di terzi e come debba essere applicato per costituire una base giuridica per il trattamento**[47]**. Tanto chiarito, la CGUE giunge sbrigativamente alla conclusione per cui in una situazione come quella del caso di specie è necessario che ciascuno dei titolari persegua un interesse legittimo autonomo al fine di poter addurre una giustificazione per dette operazioni di trattamento. Tuttavia, una volta data risposta al quesito del giudice *a quo*, effettivamente non particolarmente ispirato, la Corte non fornisce ulteriori elementi di guida sulla natura di detti interessi legittimi – i quali saranno da valutare da parte della Corte tedesca.

6. Trattamento dei dati in forza del consenso degli interessati

Con la quinta e la sesta questione, affrontate congiuntamente dalla Corte, si rimane nella sfera della liceità del trattamento, *sub specie* consenso**[48]**. Inoltre, si discute su quale soggetto insistano gli obblighi di informativa.

Anche in questo caso, la risposta della Corte è estremamente sbrigativa, oltre che poco propensa a comprendere le complessità di natura pratica connesse al mondo online. Infatti, la CGUE, sostenendo che (i) il consenso deve essere espresso prima della raccolta e della comunicazione

mediante trasmissione dei dati, che (ii) spetta al gestore del sito ottenere tale consenso e che (iii) quest'ultimo copre unicamente i trattamenti per cui il gestore determina finalità e mezzi, costringe i soggetti coinvolti in situazioni assimilabili a quella in analisi a duplicare gli oneri di raccolta del consenso e di informativa. Inoltre, pare sorprendente quanto la Corte non tenga (o non voglia tenere) in considerazione che la trasmissione dei dati al fornitore del social *plug-in* è contestuale alla pressione del comando di caricamento della pagina *web* da parte dell'utente. Bisognerebbe quindi costringere i gestori delle pagine internet a bloccare il caricamento di determinati elementi fino all'ottenimento del consenso specifico dell'utente in tal senso. Inoltre, per il vizio logico già discusso secondo cui (a) la Fashion ID determina finalità e mezzi di raccolta e trasmissione, (b) altre operazioni di trattamento sono necessarie da parte di Facebook per il corretto caricamento del *plug-in* e (c) il consenso dell'utente copre unicamente raccolta e trasmissione, il caricamento del *plug-in* richiederebbe due consensi – il primo per raccogliere e comunicare i dati a Facebook e il secondo per condurre ogni ulteriore e necessaria operazione da parte di Facebook al fine di caricare correttamente il *plug-in* –. Basta anche una scarsa dimestichezza con il mondo *online* per comprendere la totale inadeguatezza di un processo del genere rispetto alle esigenze degli operatori economici e alle aspettative degli utenti.

A onor del vero, bisogna rammentare che non si tratta del c.d. *consenso cookie* e che la possibilità di far leva sugli altri presupposti di legittimità del trattamento (in particolare del citato legittimo interesse del titolare o di un terzo) rende la discussione estremamente teorica.

Per quanto parallelamente riguarda gli obblighi di informativa (molto simili tra DPD e GDPR), l'enfasi posta dalla CGUE è minima: la Corte affronta infatti congiuntamente le due questioni, limitandosi a rammentare che così come il consenso dovrà essere raccolto unicamente per le fasi di trattamento di cui il gestore determina finalità e mezzi, alle sole e medesime fasi è circoscritto ogni obbligo informativo.

7. Riflessioni conclusive

Provando a guardare al di là della coltre di fumo del tecnicismo giuridico, bisogna sicuramente riconoscere che la decisione della Corte nel caso *Fashion ID* avrà un'eco non solo mediatica, ma anche pratico-applicativa. Infatti, l'integrazione dei siti web mediante contenuti di terza parte è una realtà estremamente ramificata e di complessa catalogazione: basti pensare, oltre ai *social network*, ad ogni *plug-in* che contenga una mappa o delle previsioni del tempo. Inoltre, non bisogna dimenticare, anche in ottica futura, la peculiarità dei dati oggetto di trattamento nella

fattispecie in esame. Infatti, l'indirizzo IP dinamico rientra nella categoria di dati che hanno necessitato l'intervento della stessa CGUE per essere ritenuti personali, vista la necessità di combinarli con altri dati[49]. Si aggiunga inoltre che tali dati semi-personali (non nel senso che rappresentino una nuova categoria ma semplicemente che siano personali al ricorrere di condizioni aggiuntive ed estrinseche) sono trattati in un ambiente caratterizzato da logiche imposte più da ragioni di funzionalità ed efficienza delle macchine che da profondi ragionamenti sul corretto design giuridico dei flussi di dati. Sicuramente la decisione in commento segna un ulteriore passo verso la riconciliazione tra la linearità[50] del modello di regolamentazione scelto per la protezione dei dati e la realtà economica dell'economia c.d. *data-driven.*

Dall'altro lato, come discusso, non può negarsi una certa perplessità sulle modalità argomentative scelte dalla Corte, nonché sulla solidità logico-giuridica delle conclusioni. La sensazione è che le esigenze di tutela e certezza dei ruoli tra le parti abbiano prevalso sulla chiarezza e linearità della ricostruzione. Inoltre, non vanno trascurate le complessità di *enforcement* nei confronti delle *big tech companies*; la tendenza delle associazioni dei consumatori come la Verbraucherzentrale NRV è infatti quella di preferire l'azione nei confronti di soggetti relativamente più piccoli, come la Fashion ID, al fine di raggiungere indirettamente Facebook mediante le interconnessioni di natura tecnologica tra le parti[51]. In ogni caso, dalla Corte di giustizia ci si sarebbe potuti attendere un maggior rigore nella ricostruzione dei ruoli tra le parti. Infatti, con il passaggio dalla disciplina embrionale della DPD in materia di contitolarità del trattamento a quella più di dettaglio del GDPR[52] il mondo dei titolari del trattamento, con particolare riguardo ai gruppi industriali, è alla ricerca di preziosi elementi interpretativi da parte delle autorità e delle Corti. A tale proposito è importante ricordare che alla contitolarità, anche asimmetrica, è associato il regime della responsabilità in solido nei confronti degli interessati: ciò si traduce in maggiori tutele (teoriche) per gli interessati e in contestuali maggiori rischi per i soggetti dati convolti nelle operazioni di trattamento[53].

Inoltre, anche se per ragioni in fondo condivisibili, ci si rammarica che la tematica dell'applicabilità e dei limiti della direttiva e-Privacy sia stata solo sfiorata dalle valutazioni dei giudici di Lussemburgo. In ogni caso, la decisione della Corte nel caso Fashion ID sta facendo e farà discutere animatamente pratici e teorici della protezione dei dati. Proprio per questo, oltre alla centralità dei temi trattati, è molto probabile diventi un parametro di riferimento per lo sviluppo della giurisprudenza in materia.

[1] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera

circolazione di tali dati; anche detta Direttiva Madre o Data Protection Directive (DPD).

[2] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Sulla sostanziale continuità tra categorie cfr. *ex multis* Passaglia, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media tra regole generali e ricerca di una specificità*, in *Consulta online*, 3, 2016, 7.

[3] Come è noto, per questioni di traduzione e trasposizione normativa il testo (italiano) della Direttiva e, di rimando, le pronunce della CGUE fanno riferimento al *data controller* indicandolo come responsabile del trattamento e al *data processor* indicandolo come incaricato. Tuttavia, fin dal primo recepimento della DPD mediante la l. n. 675/1996, il legislatore italiano ha tradotto *data controller* con l'espressione «titolare del trattamento» e *data processor* come «responsabile del trattamento». La traduzione ufficiale del GDPR ha quindi mutuato questa nomenclatura ormai invalsa nel nostro paese. Si precisa quindi che in questa nota si utilizzerà la nomenclatura corretta, attualmente in uso da parte del GDPR. In realtà, si ritiene che la traduzione originaria sia più allineata al significato della terminologia di lingua inglese. Questa, infatti, associa al termine *controller* una forma di dominio (e quindi di responsabilità) sui dati personali; mentre il ruolo di *processor*, mero «masticatore» di dati e giuridicamente privo di un'autonoma volontà, ben si sposerebbe con il termine di «incaricato del trattamento». Tuttavia, vista l'introduzione dell'autonoma figura dell'incaricato del trattamento nel panorama italiano (la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile), è stato necessario introdurre un nuovo termine, ossia quello di «titolare». Sul punto, v. anche Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino 2016, 196; e Kirschen, *Codice della Privacy, tradizione ed innovazione*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano 2006.

Il Garante italiano ha affrontato il tema fin dalla propria istituzione, «*Titolare, responsabile, incaricato - Precisazioni sulla figura del "titolare"*» - 9 dicembre 1997, doc. web n. 39785.

[4] Si ricorda che per «dato personale» deve intendersi: «*qualsiasi informazione riguardante una persona fisica identificata o identificabile (detta «interessato»)*». Ai sensi del GDPR, «*si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica,*

fisiologica, genetica, psichica, economica, culturale o sociale».

Per quanto invece riguarda le operazioni manipolative dei dati, si definisce «trattamento» « *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*».

[5] Il Garante si è espresso in tal senso, inter alia, nel Provv. n. 230 del 15 giugno 2011 - *Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali.* Per giungere a tale conclusione si fa riferimento ai criteri indicati dall'Opinion 1/2010 sui ruoli di «titolare» e «responsabile» del trattamento, emanata dal WP29. In questa sede il Gruppo di lavoro *ex* art. 29 ha chiarito che ai fini dell'individuazione della titolarità concretamente esercitata occorre esaminare anche «*elementi extracontrattuali, quali il controllo reale esercitato da una parte, l'immagine data agli interessati e il legittimo affidamento di questi ultimi sulla base di questa visibilità*». Sulla natura non formale del concetto di titolare, Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, 80 s.

[6] Cfr. sul punto la *Risposta del Garante a un quesito relativo al ruolo del consulente del lavoro dopo la piena applicazione del Regolamento (UE) 679/2016* del 22 gennaio 2019. Nel caso di specie il Consiglio Nazionale dei Consulenti del Lavoro aveva interpellato l'autorità per ottenere chiarimenti circa il ruolo dei consulenti. L'Autorità, in maniera forse eccessivamente netta, ha tracciato come linea di demarcazione il fatto che si tratti di attività delegate o meno dal cliente (eventualmente) titolare del trattamento al fornitore di servizi (a prescindere dalla natura degli stessi), il quale agirebbe quindi come responsabile del trattamento senza che le valutazioni in merito al margine di autonomia connesso alla professione o funzione di volta in volta svolte assumano un significato giuridico.

[7] V. Information Commissioner Office, *What are 'controllers' and 'processors'?*, in *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors.*

L'esempio dell'ICO affronta il caso dei commercialisti ed esperti contabili: «*A firm uses an accountant to do its books. When acting for his client, the accountant is a controller in relation to*

the personal data in the accounts. This is because accountants and similar providers of professional services work under a range of professional obligations that oblige them to take responsibility for the personal data they process. For example, if the accountant detects malpractice while doing the firm's accounts he may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so, an accountant would not be acting on the client's instructions but in line with his own professional obligations and therefore as a controller in his own right.

If specialist service providers are processing data in line with their own professional obligations, they will always be acting as the controller. In this context, they cannot agree to hand over or share controller obligations with the client».

[8] Globocnik, *On Joint Controllership for Social Plug-ins and Other Third-Party Content - A Case Note on the CJEU Decision in Fashion ID*, in IIC - *International Review of Intellectual Property and Competition Law* (2019) 50: 1033-1044.

[9] Cfr. in particolare le decisioni Corte giust. Ue, 13 maggio 2014, causa C-131/12, *Google Spain e Google*; Corte giust. Ue, 5 giugno 2018, causa C-210/16 *Wirtschaftsakademie Schleswig-Holstein*; Corte giust. Ue, 10 luglio 2018, causa C-25/17, *Tietosuojavaltuutettu v. Jehovan todistajat*. In merito a quest'ultima si segnala inelegantemente Panetta-Sartore, *Proselitismo religioso e protezione dei dati personali: tra esigenze di tutela e particolarità della fattispecie*, in questa *Rivista*, 2019, 101 ss.

[10] European Data Protection Supervisor, *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* - 7 novembre 2019.

[11] Sul tema della contitolarità cfr. *ex plurimis* D'Ottavio, Ruoli e funzioni *privacy principali ai sensi del Regolamento*, in Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019; Bassini, *Data Controller: A Shifting Paradigm in the Digital Age*, in *Bocconi Legal Papers* , 13, 2019, 103 ss.; Pelino, *I soggetti del trattamento*, in Bolognini-Pelino-Bistolfi (a cura di), *Il regolamento privacy europeo*, Milano, 2016, 133 ss.; L. Greco, *I ruoli: titolare e responsabile*, in Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 251 ss.; Salvati, *Art.26*, in Riccio-Scorza-Belisario (a cura di), *GDPR e normativa privacy*, Padova, 2018, 258 ss.; Zipponi, *Art. 26* , in Bolognini-Pelino (a cura di), *Codice della disciplina privacy*, Milano, 2019, 206 ss.

[12] Si tratta di *software* per computer in grado di aggiungere nuove funzioni a un programma ospite senza alterarne la natura.

[13] Si ricorda che la Corte ha stabilito che, al ricorrere di determinate circostanze, un indirizzo IP deve essere considerato alla stregua di un dato personale. Sul punto cfr. Corte giust. Ue, 29 luglio 2019, causa C-582/14, *Breyer*, punti 33-49.

[14] Corte giust. Ue, 29 luglio 2019, causa C-40/17, *Fashion ID*, punto 26, in commento.

[15] Corte giust. Ue, 29 luglio 2019, causa C-40/17, *Fashion ID*, punto 27, in commento.

[16] Corte giust. Ue, 29 luglio 2019, causa C-40/17, *Fashion ID*, in commento, punto 28.

[17] Corte giust. Ue, 29 luglio 2019, causa C-40/17, *Fashion ID*, in commento, punto 29.

[18] Corte giust. Ue, 29 luglio 2019, causa C-40/17, *Fashion ID*, in commento, punto 30.

[19] Corte giust. Ue, 29 luglio 2019, causa C-40/17, *Fashion ID*, in commento, punto 31.

[20] Come nel caso discusso alla nota 3, il traduttore della direttiva in italiano ha trasposto *legitimate interest* con l'espressione «interesse legittimo», forse inconsapevole del significato di questo binomio nel diritto italiano. Per questo motivo, contrariamente al testo tradotto della pronuncia in esame, si utilizzerà la più corretta (ancorché ambigua) espressione «legittimo interesse», adoperata anche dal traduttore del GDPR.

[21] Sul fatto che si tratti o meno di bilanciamento in senso stretto si è aperto un interessante dibattito, riguardo al quale si segnala Van der Sloot, *Editorial*, in *European Data Protection Law Review*, 1, 2017.

[22] L'art. 22 della Direttiva stabilisce che: «*[f]atti salvi ricorsi amministrativi che possono essere promossi, segnatamente dinanzi all'autorità di controllo di cui all'articolo 28, prima che sia adita l'autorità giudiziaria, gli Stati membri stabiliscono che chiunque possa disporre di un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle disposizioni nazionali applicabili al trattamento in questione*».

[23] *Ex multis*, può menzionarsi Corte giust. Ue, 28 luglio 2016, causa C-191/15, *Verein für Konsumenteninformation*.

[24] Corte giust. Ue, 29 luglio 2019, causa C-582/14, *Breyer*, punto 50.

[25] Ivi, punti 47-49.

[26] Ivi, punto 63.

[27] È previsto infatti che «*[g]li Stati membri possono prevedere che un organismo, organizzazione o associazione [i cui obiettivi statutari siano di pubblico interesse e che sia attiva nel settore della*

protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali], indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento».

[28] Globocknik, *op. cit*., 1035.

[29] Direttiva 2009/22/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa a provvedimenti inibitori a tutela degli interessi dei consumatori.

[30] Nota 13, punto 61.

[31] Conclusioni dell'Avvocato Generale Michal Bobek, 19 dicembre 2018, causa C-40/17, *Fashion ID*, punto 38.

[32] Gli artt. 2(d) della DPD e 4(n.7) del GDPR sono allineate nel ritenere che il titolare del trattamento sia il soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

[33] Giova incidentalmente ricordare che il sistema degli obblighi e delle responsabilità in materia di protezione dei dati personali è ancorato alla qualificazione di un soggetto quale titolare, ovvero responsabile del trattamento. In assenza delle diverse forme di controllo sui dati connesse a tali qualifiche, l'ordinamento europeo non impone obblighi, né muove rimproveri. Ciò tuttavia non vuol dire che operazioni di trattamento (in senso atecnico) escluse dall'ambito da applicazione del Regolamento siano prive di tutela; semplicemente, troveranno applicazione le norme generali in materia di responsabilità (extra)contrattuale.

[34] Cfr. i commenti di De Gregorio, *Social network, contitolarità del trattamento e stabilimento: la dimensione costituzionale della tutela dei dati personali tra vecchie e prospettive passate e future* , in *Dir. inf. inform*., 2018, 462; Marcello, *Responsabilità e corresponsabilità nel trattamento dei dati personali*, in *Giustiziacivile.com*, 2018.

[35] Corte giust. Ue, 5 giugno 2018, causa C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, punto 36.

[36] Nota 13, punti 76-78.

[37] Per quanto concerne gli strumenti (o mezzi) del trattamento, la Corte spiega che «*la Fashion ID sembra aver inserito sul suo sito Internet il pulsante "Mi piace" di Facebook messo a*

disposizione dei gestori di siti internet da parte della Facebook Ireland, pur essendo consapevole del fatto che lo stesso serve da strumento di raccolta e di trasmissione di dati personali dei visitatori di tale sito, indipendentemente dal fatto che essi siano o meno iscritti al social network *Facebook*» (punto 77). Per quanto riguarda le finalità, la CGUE ritiene che «*l'inserimento da parte della Fashion ID del pulsante "Mi piace" di Facebook nel suo sito Internet le consenta di ottimizzare la pubblicità per i suoi prodotti rendendoli più visibili sul* social network *Facebook quando un visitatore del suo sito internet clicca su detto pulsante*»; dall'altro lato, Facebook «*ottiene come contropartita negoziale il fatto di poter disporre di tali dati ai propri fini commerciali*».

[38] Nota 13, punto 85.

[39] Lo spiega bene Globocnik, *op. cit*., 1037.

[40] Corte giust. Ue, 10 luglio 2018, causa C-25/17, *Tietosuojavaltuutettu v. Jehovan todistajat*, *cit*., punto 69.

[41] Il riferimento dell'AG è più raffinato, ricordando alla nt. 42 delle sue conclusioni che «*La responsabilità senza potere [è] la prerogativa dell'eunuco nei secoli*», citando Sir Humphrey Appleby (che a sua volta citava l'anonimo) in *Yes, Prime Minister*, Stagione 2, Episodio 7.

[42] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

[43] Nota 13, punto 90.

[44] Nel 2017 è stata resa nota la volontà delle istituzioni europee di procedere alla riforma della Direttiva e-Privacy da coordinarsi, in quanto *lex specialis*, con l'appena approvato GDPR. Il punto sicuramente centrale, che sta infatti rallentando i lavori, è la regolamentazione dei c.d. servizi *Over-the-Top* (OTTs). Ad oggi, la posizione del Consiglio è stata rigettata dal Coreper e nel 2020 la Commissione dovrà decidere se ritirare la proposta o rimaneggiarla radicalmente.

[45] L'AG Bobek riporta che vi è stato un ampio dibattito in udienza sul punto. Conclusioni dell'Avvocato Generale Michal Bobek, 19 dicembre 2018, C-40/17, *Fashion ID*, punto 115.

[46] L'art. 5(3) della Direttiva e-Prvacy, gli Stati membri devono assicurare «*l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la*

possibilità di rifiutare tale trattamento da parte del titolare del trattamento». Si tratta del noto «*consenso cookie*», trasposto il Italia dall'art. 122 del d.lgs. n. 196/2003 del 30 giugno 2003 (il «Codice privacy»). La scivolosa disciplina sui *cookies* è stata poi integrata dall'intervento chiarificatore del Garante con il Provv. Generale dell'8 maggio 2014 - *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l´uso dei cookie*.

[47] V. nt. 19 e 20.

[48] V. *ex plurimis* Solove, *Privacy Self-Management and the Consent Dilemma*, in 126 *Harv. L. Rev*. (2013).

[49] Espandendo quanto accennato in nt. 12, nella causa C-582/14, *Breyer* la Corte ha spiegato che in «*[U]n indirizzo di protocollo Internet (indirizzo IP) dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*» (punti. 44-49).

[50] Tene, *Privacy law's midlife crisis: a critical assessment of the second wave of global privacy laws*, in 74 *Ohio State Law J*, 1219.

[51] Cfr. sul panorama tedesco, Globocnik, *op. cit*., 1042.

[52] L'art. 26 del GDPR prevede in particolare che i contitolari «*determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti*».

[53] A mente dell'art. 82 del GDPR, «*[q]ualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato*».