L'identità digitale quale diritto del cittadino dell'Unione, fra tutela della privacy e concorrenza.*

Ruggiero Cafari Panico**

SOMMARIO: 1. Le iniziative del Parlamento europeo per il riconoscimento dell'identità digitale. – 2. La nozione di identità digitale. – 3. La protezione dei dati personali tra diritto alla privacy e concorrenza. – 4. Conclusioni.

1. Le iniziative del Parlamento europeo per il riconoscimento dell'identità digitale.

Fra gli ultimi atti del Parlamento europeo prima della interruzione delle attività in vista del suo rinnovo, con le elezioni del 26 maggio 2019, figura l'avvenuto deposito della proposta di risoluzione sul «riconoscimento dell'Identità Digitale Universale: un diritto fondamentale per tutti i cittadini Europei».[1]

Sarà il nuovo Parlamento a decidere se riprendere l'esame della proposta, ma sarebbe sorprendente se ciò non avvenisse dal momento che essa si colloca nel solco dell'azione da tempo intrapresa dalle istituzioni europee e, in particolare, dallo stesso Parlamento per giungere al pieno riconoscimento dell'identità digitale quale diritto fondamentale del cittadino dell'Unione, e prima ancora della persona.

Il 3 ottobre 2018 il Parlamento europeo ha approvato la risoluzione dal titolo «Tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione».[2] Nell'esaminare la tecnologia blockchain e in genere la tecnologia Distributed Ledger Technology (DLT) e le sue possibili applicazioni nei diversi settori del mercato interno, il documento evidenzia come tali tecnologie diano vita ad un vero e proprio ecosistema, fondato sulla auto-sovranità, identità e fiducia, dove può venir

* Il presente contributo è destinato agli "Scritti in onore di Claudia Morviducci", in corso di pubblicazione.

** Professore ordinario di Diritto dell'Unione europea presso l'Università degli Studi di Milano.

[1] La proposta di risoluzione è stata presentata a norma dell'art. 133 del regolamento del Parlamento europeo dal vicepresidente del Parlamento stesso F.M. Castaldo.

[2] P8_TA-PROV(2018)0373. Per l'avvio di un percorso volto alla definizione di un quadro normativo che possa favorire lo sviluppo di tecnologie *blockchain* e *distributed ledger*, vedi art. 8-ter della legge 11 febbraio 2019, n. 12, di conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, in GU n. 36 del 12 febbraio 2019.

meglio tutelata l'identità digitale delle persone, attraverso una gestione diretta dei dati personali[3] da parte del loro titolare[4].

Seppure inserita in un contesto in cui le DLT sono intese come strumento di sviluppo del mercato, non può non rilevarsi come ad emergere sia comunque il profilo della tutela della c.d. identità digitale, ancora però considerata come profilo a sé stante rispetto al novero delle posizioni giuridiche del soggetto titolare di tale identità. In altri termini, diviene sempre più evidente come l'attuazione della Agenda digitale europea nell'ambito della Strategia Europa 2020[5], cui sono riconducibili i diversi atti adottati nel tempo dalle Istituzioni dell'Unione, non possa più prescindere da una espressa affermazione da parte del Parlamento europeo della riconducibilità della identità digitale nell'ambito dei diritti fondamentali della persona, quali affermati in particolare dall'art. 8 («Protezione dei dati di carattere personale») della Carta dei diritti fondamentali dell'Unione europea e riconosciuti dall'art. 16 del Trattato sul funzionamento dell'Unione europea (TFUE), di cui gode il cittadino dell'Unione stessa.

La proposta cui si è fatto cenno all'inizio, fra l'altro, «riconosce il diritto all'identità digitale come diritto fondamentale della persona e assicura la tutela dello stesso e di tutti i diritti ad esso connessi» ed «esorta la Commissione a presentare un'iniziativa legislativa volta a riconoscere tale diritto, precisandone il contenuto, i limiti e le modalità di tutela».[6] Toccherà dunque alla Commissione, nel caso di approvazione della risoluzione, procedere ad adottare le necessarie misure idonee ad assicurare il pieno rispetto dei diritti una volta esattamente definiti, stabilendone, da un lato, il contenuto, alla luce anche degli strumenti

[3] Ovvero, secondo la definizione contenuta nel 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) (GDPR), in GUUE, L 119 del 4 maggio 2016, pp. 1-88, «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")» (art. 4). Il dato personale comprende dunque sia le informazioni oggettive sia quelle soggettive (valutazioni ed opinioni riconducibili ad un individuo; l'articolo continua infatti: «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», includendo quindi anche le informazioni più sensibili del soggetto preso in considerazione.

[4] Risoluzione «Tecnologie di registro distribuito e blockchain», cit., punto 28 ss.

[5] Un'agenda digitale europea è una delle sette iniziative faro della Strategia Europa 2020 lanciata dalla Commissione nel marzo 2010 (EUROPA 2020 – Una strategia per una crescita intelligente, sostenibile e inclusiva – COM(2010)2020 definitivo del 3 marzo 2010). I temi e gli obiettivi sviluppati a livello europeo con l'Agenda digitale europea sono declinati a livello italiano con l'Agenda digitale italiana che fa a sua volta da guida alle Agende digitali locali con le quali l'ente territoriale, Comune e Provincia, definisce il proprio impegno strategico per la promozione dell'economia digitale nel proprio territorio.

[6] Nella proposta di risoluzione viene parimenti auspicata «una revisione dei Trattati ed eventualmente della Carta dei diritti fondamentali dell'Unione europea che preveda una menzione esplicita del diritto all'identità digitale e la sua tutela»; sottolineata «l'importanza di ricomprendere tale diritto nell'alveo dei diritti fondamentali ai fini di qualunque azione dell'Unione, sul piano interno, esterno e delle negoziazioni con paesi terzi»; e, infine, richiesto «che tale diritto, riconosciuto come diritto fondamentale a livello dell'Unione, venga salvaguardato anche nell'ambito dei negoziati e nell'eventuale accordo finale di recesso del Regno Unito».

normativi già in vigore, e, dall'altro, l'ambito e i criteri di tutela, con riguardo, rispettivamente al contesto spaziale di esercizio e protezione e al loro bilanciamento con altri diritti.[7]

Si tratterebbe peraltro di proseguire e portare a conclusione il cammino avviato nel 2012 con la pubblicazione del Codice dei diritti online vigenti nell'UE, che costituiva all'epoca «una raccolta dei diritti e dei principi di base sanciti nel diritto dell'Unione a tutela dei cittadini che accedono online a reti e servizi e durante l'uso di tali reti e servizi». Seppur in una ottica limitata, era evidente lo sforzo dichiarato di individuare i diritti e principi che «sparsi in varie direttive, regolamenti e convenzioni nei settori delle comunicazioni elettroniche, del commercio elettronico e della protezione del consumatore» potrebbero trovare applicazione «nell'ambiente digitale». Fra tali diritti di cui deve poter godere «ciascun cittadino dell'Unione» comparivano «i diritti di accesso a internet», ovvero «a qualsiasi informazione e a distribuirla, nonché di gestire qualsiasi applicazione e servizio di sua scelta tramite le reti di comunicazione elettronica», il diritto di accesso senza discriminazioni «ai servizi forniti online» e quello alla «protezione dei propri dati personali», già sancito dal TFUE all'art. 16 e dalla Carta dei diritti fondamentali dell'Unione europea, all'art. 8.[8] Tale cammino è poi proseguito con i regolamenti GDPR[9] e eIDAS[10], in vigore

[7] In merito, per tutti, conclusioni avv. gen. Szpunar, 10 gennaio 2019, causa C-507/17, *Google LLC*, EU:C:2019:15, nonché Corte di giustizia, sentenza 14 febbraio 2019, causa C-345/17, EU:C:2019:122, con riguardo alla necessità «di conciliare due diritti fondamentali, vale a dire, da un lato, la tutela della vita privata e, dall'altra, le libertà di espressione» (punto 50), secondo un principio sancito anche dalla giurisprudenza della Corte europea dei diritti dell'uomo (punto 66). Per ampie considerazioni in merito al necessario bilanciamento fra il diritto alla riservatezza dei dati personali i principi di pubblicità e trasparenza che si "fronteggiano soprattutto nel nuovo scenario digitale: un ambito nel quale, da un lato, i diritti personali possono essere posti in pericolo dalla indiscriminata circolazione delle informazioni, e, dall'altro, proprio la più ampia circolazione dei dati può meglio consentire a ciascuno di informarsi e comunicare", vedi Corte cost., sentenza n. 20 del 21 febbraio 2019, punto 2.2 del *Considerato in diritto*.

[8] Per una precisa declinazione dei diritti alla vita privata, alla protezione dei dati personali e alla sicurezza, vedi, prima, Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche on riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in GUCE, L 281 del 23 novembre 1995, pp. 31-50), e, ora, il regolamento 2016/679. I diritti in questione si applicano anche nell'ambiente online, dove essi trovano ulteriore specificazione in base alla Direttiva 2002/58/CE del Parlamento europeo. Per quanto attiene alle iniziative del Consiglio d'Europa, con riguardo in particolare all'applicazione della c.d. Convenzione 108, così come modificata dal Protocollo CETS n. 223 (c.d. Convenzione 108+), vedi Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 gennaio 2017, T-PD(2017)01, nonché *Guidelines on artificial intelligence and data protection*, 25 gennaio 2019, T-PD(2019)01.

[9] Per la sua trasposizione nell'ordinamento italiano si veda Decreto legislativo 30 giugno 2003, n. 196 recante il «Codice in materia di protezione dei dati personali», integrato con le modifiche introdotte dal Decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)», in GU n. 205 del 4 settembre 2018.

[10] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, in GUUE, L 257 del 28 agosto 2014, pp. 73-114.

rispettivamente dal 25 maggio 2018 e dal 1° luglio 2016, giungendo con quest'ultimo all'introduzione di processi di identificazione digitale del cittadino per poter accedere ai servizi pubblici.[11]

Il passo compiuto dal Parlamento europeo verso l'estensione alla società cibernetica dei diritti tradizionali della persona già sanciti nella Carta dei diritti fondamentali dell'Unione è del tutto evidente. Altrettanto evidente è la sempre maggiore attenzione prestata dal diritto all'impatto delle tecnologie sulla vita delle persone.[12] Basti rileggere la Risoluzione del Parlamento europeo del 19 gennaio 2016 sul tema «Verso un atto sul mercato unico digitale»[13] per comprendere come il passaggio, da una visione in cui il cittadino era oggetto possibile della protezione che gli veniva accordata nell'ambiente digitale, ad una in cui l'identità e i relativi diritti assurgono a protagonisti attivi della nuova società cibernetica che si viene delineando, sia stato importante ma non completo. A mancare è ancora l'esplicito riconoscimento di quello che è stato definito anche come diritto di cittadinanza digitale, c.d. *e*-cittadinanza, che prescinda dagli usuali modelli basati sull'appartenenza ad un territorio materialmente inteso, ma abbia la propria ragione di esistere nelle connotazioni particolari dello spazio di Internet e la propria tutela nei diritti e delle libertà di cui gode ciascun cittadino dell'Unione europea nel mercato unico nella sua dimensione digitale. In altre parole, se finora il diritto all'identità digitale, nella misura in cui essa sia riassuntiva di numerose e a volte eterogenee situazioni soggettive riconducibili nella più ampia accezione di diritto all'identità personale così come si configura su Internet[14], è stato riconosciuto, proprio con riguardo al trattamento dei dati personali, principalmente come diritto a non essere rappresentati in maniera esatta, non deformante, si impone invece ora l'esigenza che l'identità, quale diritto ad essere se stessi, sia rispettata *tout court*, a prescindere dalla correttezza o meno della sua rappresentazione.

Ricondurre il diritto all'identità digitale, quale diritto fondamentale, nel novero di quelli attribuiti dalla cittadinanza europea[15] richiede tuttavia una rivisitazione del processo che ha condotto

---

[11] Lo SPID- Sistema Pubblico di Identità Digitale è la soluzione che consente ai cittadini di accedere ai servizi online della Pubblica Amministrazione. Con esso è stata avviata la possibilità per il cittadino di creare una identità digitale unica. Una volta concluso il percorso avviato con la notifica europea da parte dell'Agenzia per l'Italia Digitale, ai fini del mutuo riconoscimento dei mezzi di identificazione elettroni a adottati tra Stati membri, come previsto dall'art. 9 del regolamento eIDAS, SPID è destinato a diventare un'identità digitale europea. Un esempio di utilizzo avanzato di tale strumento è rappresentato dall'Estonia.

[12] Vedi M. ZANICHELLI, *Il diritto all'oblio tra privacy e identità digitale*, in *Informatica e diritto*, 2016, pp. 9-28, specie p. 9 dove si evidenzia al riguardo come il regolamento 2016/679 non a caso si riferisca non alla protezione dei dati, ma specificamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[13] P8_TA(2016)0009.

[14] Al riguardo, si veda Dichiarazione dei diritti in Internet approvata dalla Commissione di studio per i diritti e doveri relativi al mondo del *web*, pubblicata il 28 luglio 2015: M.F. COCUCCIO, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. fam. pers.*, 2016, pp. 949-968, spec. p. 962 s.

[15] Il legame indissolubile tra persona, cittadinanza e spazio di libertà, sicurezza e giustizia compare già nel Preambolo della Carta dei diritti fondamentali dell'Unione europea, i cui diritti sono riconosciuti per la maggior parte a tutte le persone indipendentemente dalla cittadinanza della persona in questione e, in particolare, dalla circostanza che essa abbia o meno la cittadinanza dell'Unione. Se dunque è vero che solo una minoranza sono riconosciuti in via esclusiva ai cittadini dell'Unione, lo è altrettanto che solo questi ultimi si possono avvalere degli strumenti che le libertà fondamentali pongono a loro disposizione perché siano esercitati nello spazio di libertà

all'affermazione stessa dell'esistenza di tale diritto come diritto della persona, prima, e come portato della cittadinanza dell'Unione europea, poi.

Nel mutato contesto economico e culturale rimane l'esigenza di fondo di stabilire che cosa si intenda per diritti e libertà fondamentali della persona, di quale sia la loro portata e la loro effettiva protezione, per lo meno alla luce dell'ordinamento dell'Unione e di quello dei suoi Stati membri, senza alcuna pretesa universalistica, bensì in una prospettiva diacronica di spazio e tempo, che affronti e risolva i problemi nello spazio cibernetico (world wide web) alla luce del dato normativo formatosi in epoca a noi più vicina.

2. La nozione di identità digitale.

Per delimitare l'oggetto delle nostre considerazioni giova ricordare quanto osservato in dottrina circa la nozione di identità personale e quella di identità digitale,[16] che assumono più valenze semantiche. Vero è infatti che il legislatore europeo ha adottato strumenti normativi in questo ambito, ricomprendendo il diritto all'identità personale fra i diritti fondamentali, ma non ha definito il concetto di «identità» né personale né tantomeno digitale.

Volendo ora risolvere il dubbio sul significato di tale nozione (identità personale), si può rilevare come, secondo l'insegnamento della Corte di giustizia, la determinazione dei termini per i quali il diritto dell'Unione non fornisce alcuna definizione deve avvenire sulla base del significato abituale del termine stesso nel linguaggio corrente, tenendo conto al contempo del contesto in cui esso è utilizzato e degli obiettivi perseguiti dalla normativa in cui è inserito.[17] Se così è, di sicuro, l'identità personale designa comunemente «il complesso delle risultanze anagrafiche, che servono ad identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati»[18]; ma da tale significato comune si evince anche che tale nozione costituisce per il singolo interessato una sorta di sintesi ideale della sua «biografia». Dal che deriva che, secondo un ormai risalente *dictum* della Corte costituzionale, il relativo diritto si configuri come «diritto ad essere se stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le convinzioni ideologiche, religiose, morali e sociali, che differenziano, ed al tempo

sicurezza e giustizia. In generale, N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Milano, 2018, p. 87 ss.

[16] G. RESTA, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 2017, pp. 511-531, spec. p. 512 ss. Il principale riferimento normativo alla tutela dell'identità digitale delle persone fisiche viene rinvenuto nell'art. 2 della Costituzione: S. LANDINI, *Identità digitale fra tutela della persona e proprietà intellettuale*, in *Riv. dir. civ.*, 2017, pp. 180-201, spec. p. 183.

[17] Corte di giustizia, sentenza 3 settembre 2014, C-201/13, *Deckmyn*, EU:C:2014:2132, punto 19 anche per ulteriori riferimenti.

[18] G. RESTA, *Identità*, cit., p. 18.

stesso qualificano, l'individuo»[19]; vale a dire, come appena osservato, che l'identità è intesa come formula riassuntiva di ciò che si è, declinata nei vari contesti di rilevanza giuridica per l'interessato.

Quanto in particolare all'identità digitale, il cui unico espresso riscontro normativo è rintracciabile nell'art. 640-*ter*[20], essa assumerebbe due diverse accezioni, indicando, per un verso, l'identità «"in rete" o "virtuale"», e, per un altro, l'insieme delle informazioni reperibili in rete nei riguardi del soggetto interessato[21]. Sul piano sostanziale le due nozioni sono riconducibili ad unità, o meglio i diritti riferibili alla identità digitale concorrono alla costruzione dell'identità personale che ne garantisce la tutela. In altri termini, il rapporto che intercorre tra identità personale e identità digitale non è dissimile da quello fra nome e identità personale[22], avendo come tratto caratteristico la riconducibilità di entrambe le nozioni alla identificabilità del singolo da parte dei terzi sulla base di determinati contrassegni, ma che si qualifica ulteriormente per la strumentalità della seconda rispetto alla prima, più generale e che ha già trovato da tempo un esplicito riconoscimento fra i diritti fondamentali.

A tale conclusione è possibile pervenire ripercorrendo la trasformazione intervenuta nel significato dell'identità personale a seguito dell'introduzione della legge n. 675 del 31 dicembre 1996[23] Con la nuova disciplina, poi trasposta nel Codice in materia di protezione dei dati personali (d.lgs. 196/2003), si assiste non solo ad una espressa «riconduzione della tutela dell'identità e della riservatezza all'interno del quadro dei diritti e delle libertà fondamentali»[24], ma anche una sua lettura in senso dinamico, correlato alla individuazione del patrimonio individuale nei diversi contesti in cui opera l'interessato, assumendo esso un contenuto che si configura a seconda delle condizioni sociali, economiche e giuridiche dello specifico contesto. In questa prospettiva, l'identità digitale risponde ad una possibile declinazione dell'identità personale nella nuova dimensione diacronica di Internet, divenendo tale identità variabile nello spazio e nel tempo, come dimostrano il diritto all'oblio[25] e la c.d. successione digitale[26].

---

[19] Corte cost., sentenza del 3 febbraio 1994, n. 13.

[20] Per tutti, F. CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, N. 93 (convertito con modificazioni dalla L. 15 ottobre 2013, N. 119)*, in *Cassazione penale*, 2014, pp. 1094-1105; e C. CRESCIOLI, *La tutela penale dell'identità digitale*, in *Diritto Penale Contemporaneo*, 2018, pp. 265-275, anche per ulteriori riferimenti.

[21] G. RESTA, *Identità*, cit., p.514s.

[22] G. PINO, *L'identità personale*, in S. RODOTÀ e P. ZATTI (dir.), *Trattato di biodiritto*, vol. I, *Ambito e fonti del biodiritto*, Milano, 2010, pp. 297-321, p. 306 s.

[23] Recante «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali», in GU n. 5 dell'8 gennaio 1997 - Suppl. Ordinario n. 3).

[24] *Ibid.*, p. 522.

[25] *Ex multis*, M.L. DAGA, *Diritto all'oblio: tra diritto alla riservatezza e diritto all'identità personale*, in *Danno e responsabilità*, 2014, pp. 274-278; e M. TAMPIERI, *Il diritto all'oblio e la tutela dei dati personali*, in *Responsabilità civile e previdenza*, 2017, pp. 1010-1031.

[26] M. CINQUE, *La successione nel "patrimonio digitale": prime considerazioni*, in *NGCC*, 2012, pp. 645-655; A. MAGNANI, *L'eredità digitale*, in *Notariato*, 2014, pp. 519-532; G. RESTA, *La 'morte digitale'*, in *Il diritto dell'informazione e dell'informatica*, 2014, 891-920; e G. MARINO, *La successione digitale*, in *Osservatorio del diritto civile e commerciale*, 2018, pp. 167-204.

Non espressamente previsto né dalla legislazione ordinaria né da quella costituzionale[27], il diritto all'oblio è stato dunque qualificato come una particolare declinazione della tutela dell'identità personale, ovvero come espressione del «giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata».[28] Al riguardo sono significative le osservazioni svolte dall'Avvocato generale Szpunar nella causa *Google LLC*.[29] Richiesto di precisare l'ambito di applicazione territoriale del diritto alla cancellazione, quale sancito dalla direttiva 95/46, applicabile al caso di specie *ratione temporis*,[30] l'Avvocato generale, richiamando il precedente rappresentato dalla sentenza *Google Spain*,[31] afferma come al centro della protezione accordata dalla normativa europea vi siano i diritti della persona i cui dati personali devono essere protetti,[32] che vengono così privilegiati. L'obiettivo della direttiva è infatti «garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali».[33] Proprio però dalla loro natura di diritti fondamentali deriva l'esigenza che il diritto all'oblio debba essere bilanciato con altri diritti fondamentali.[34] Valgono al riguardo le considerazioni svolte dalla Corte nel citato caso *Google Spain*, dove la Corte ha posto attribuito grande importanza alla necessità che i diritti alla protezione dei dati e alla vita privata siano bilanciati «con l'interesse legittimo del pubblico ad accedere all'informazione ricercata», che trae anch'esso origine dalla Carta (art. 11).[35] L'ulteriore osservazione è che i due ordini di diritti così contrapposti variano nel loro contenuto e nella corrispondente tutela a seconda del paese in cui operano, sicché, ove si ammettesse «una cancellazione a livello mondiale, le autorità dell'Unione non sarebbero in grado di definire e determinare un diritto a ricevere informazioni e, ancor meno, di bilanciarlo con gli altri diritti fondamentali alla protezione dei dati e alla vita privata».[36] A ciò si aggiungerebbe il rischio di dare l'avvio ad una sorta di «corsa al ribasso» a danno della libertà di espressione a livello mondiale, fornendo ai paesi terzi l'alibi per disporre analogamente una cancellazione in forza delle proprie leggi, precludendo «alle persone che si trovano in uno Stato membro dell'Unione

[27] A.L. VALVO, *Il diritto all'oblio nell'epoca dell'informazione "digitale"*, in *Studi sull'integrazione europea*, 2015, pp. 347-357, a p. 247.

[28] Così Cassazione civ., III sez., sentenza, 9 aprile 1998, n. 3679; vedi anche, *ex multis*, ID., 5 aprile 2012, n. 5525.

[29] Conclusioni del 10 gennaio 2019, causa C-507/17, EU:C:2019:15.

[30] *Ibid.*, punto 31.

[31] Sentenza del 13 maggio 2014, causa C-131/12, EU:C:2014:317.

[32] Conclusioni del 10 gennaio 2019, causa C-507/17, cit.

[33] *Ibid.*, punto 42.

[34] *Ibid.*, punto 57.

[35] *Ibid.*, punto 59.

[36] *Ibid.*, punto 60.

di accedere a un'informazione ricercata».[37] Di qui la conclusione che la protezione accordata dalle disposizioni della direttiva sia di regola circoscritta al territorio dell'Unione, ovvero al mercato interno.[38]

Lo stesso Avvocato generale è consapevole, da un lato, del fatto che il diritto dell'Unione conosce situazioni in cui sono ammessi gli effetti extraterritoriale delle sue norme e come, dall'altro, Internet sia «per sua natura mondiale e, in un certo qual senso, presente ovunque», ma proprio da ciò desume l'impossibilità di «trovare analogie e compiere raffronti», pur introducendo in via eccezionale la possibilità per l'Unione «di adottare misure a livello mondiale»[39], senza definirne le circostanze e i limiti. Ciò che emerge è la consapevolezza della impossibilità di risolvere a livello esclusivamente regionale una questione che investe la tutela di un diritto che solo in un contesto universale può per sua natura trovare adeguata protezione. Ma ancor più importante è che appaia ormai consolidato il riconoscimento dello *status* di diritto fondamentale di uno dei contenuti principali della costruenda identità digitale.

Indubbiamente per il legislatore nazionale ed europeo sono innumerevoli le sfide, di non facile soluzione, poste dall'avanzata della tecnologia e in questo contesto significativi sono gli sforzi compiuti in particolare dal legislatore europeo in materia di libero accesso al web, di neutralità della rete, di alfabetizzazione digitale e, più in generale, in materia di digitalizzazione della società, in un confronto sempre più serrato con i nuovi e complessi problemi che derivano dalla globalizzazione.

Le prospettive poste da Internet impongono dunque una rilettura degli schemi tradizionali che finisce per generare nuovi diritti e nuove forme di estrinsecazione delle libertà fondamentali dell'individuo che già sono tutelate dai Trattati e che ora divengono strumentali all'affermarsi di questi diritti della persona di ultima generazione, destinati ad essere esercitati dal cittadino dell'Unione nell'ecosistema che l'Unione si è impegnata a sviluppare, avvalendosi degli strumenti che le libertà fondamentali pongono a sua disposizione.

Strumento di identificazione del soggetto per la sua appartenenza al mondo di interne e dunque espressione dell'individualità della persona in tale ambito, l'identità digitale è stata oggetto negli anni più recenti di letture differenti, che hanno puntato di volta in volta su uno dei suoi molteplici aspetti.

Da mezzo dunque atto a designare, nella veste di identità informatica, l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un suo particolare utilizzatore, nel corso degli anni l'identità digitale si è progressivamente trasformato in oggetto di un diritto fondamentale dell'individuo a tutelare la propria identità come sintesi di quello che è nelle varie e innumerevoli attribuzioni che lo riguardano, che, grazie soprattutto all'intervenuto riconoscimento nei diversi ambiti da parte del diritto

---

[37] *Ibid.*, punto 61.

[38] *Ibid.*, punto 63.

[39] *Ibid.*, punto 62. Con riguardo infine alla necessità di ricorrere alla tecnica detta del «blocco geografico», a livello europeo, indipendentemente dal nome dell'utente di Internet che effettua la ricerca, vedi punto 64 ss. In generale, sulla portata extraterritoriale del regolamento n. 2016/679, vedi F. JAULT-SESEKE, *La portée extraterritoriale ou a-territoriale du RGPD*, in *R.A.E.*, 2018, pp. 43-51.

dell'Unione, può già ora ascriversi, pur in assenza di una formale affermazione, alla categoria dei diritti della personalità di cui godono i cittadini dell'Unione stessa.

Nel nostro ordinamento il dibattito sul concetto di identità digitale, sul suo fondamento e sulla sua utilità ha fatto costante riferimento al ben più tradizionale diritto al nome, al quale la giurisprudenza in specie penale.

Le analogie sono evidenti, ma le rispettive funzioni sono solo in parte sovrapponibili. Funzione dell'identità digitale non è infatti semplicemente quella di consentire di distinguere un individuo dagli altri, ma anche quella e soprattutto quella di costituire una identità che, costruita in termini di dati ed informazioni reperibili nella rete, l'individuo stesso potrà far valere nei confronti di chiunque tenti di incidere sull'utilizzo dei dati medesimi.

Questa funzione emerge con particolare chiarezza quando dalla ricostruzione statica del contenuto digitale, ovvero del trattamento dei dati su cui l'identità si fonda, si muove alla definizione dinamica degli strumenti di tutela dei diritti che a tali dati sono connessi in una prospettiva non già di loro sfruttamento nel mercato, ma di tutela di chi ne è titolare nei riguardi dell'uso che in detto mercato ne viene fatto. Il diritto all'oblio rappresenta un esempio dei diritti riconducibili all'identità digitale, ma la sua tutela come tradizionalmente intesa rimarrebbe inadeguata se non vi fosse a monte il riconoscimento del diritto pieno del titolare a disporne, essendo destinato quest'ultimo a prevalere nel difficile bilanciamento fra il diritto alla privacy e alla protezione dei dati e il diritto alla libertà di informazione.

3. La protezione dei dati personali tra diritto alla privacy e concorrenza.

La questione del trattamento dei dati personali è stata finora affrontata nell'ottica sia del ruolo, sopra accennato, del provider nel trattamento dei dati stessi, sia del diritto di accesso alla rete, di cui viene assunta la neutralità[40], sia in quella, non meno rilevante e su cui intendiamo soffermarci, del *public enforcement*, ovvero nella prospettiva della tutela offerta dalla azione svolta dalle autorità preposte alla vigilanza in tema di concorrenza e di privacy.[41] Sta di fatto che con l'avvento di Internet e dei nuovi modelli di business le imprese entrano in possesso di un numero sempre maggiore di dati personali relativi ai propri clienti che divengono così oggetto di una concorrenza sempre più dinamica in cui i tradizionali indicatori di stampo microeconomico da tempo non aiutano più le Authority; esse sono infatti chiamate

[40] A.L. VALVO, *Diritto di accesso e neutralità di internet nel diritto internazionale*, in *Percorsi costituzionali*, 2014, pp.97-114.

[41] R. CAFARI PANICO, *Protezione dei dati personali e concorrenza*, in AA. VV., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Santarcangelo di Romagna, 2013, pp. 159-168. Si veda anche J. CRÉMER, Y-A DE MONTJOYE, H. SCHWEITZER, *Competition policy for the digital era. Final Report*, 2019, reperibile al sito Internet http://ec.europa.eu/competition/publications.

a confrontarsi con un contesto di innovazione continua in cui il confronto e la concorrenza possono svolgersi addirittura prima della stessa nascita del mercato.

Inevitabilmente il profilo della protezione del diritto del consumatore alla riservatezza è destinato a sfumare di fronte all'esigenza di proteggere soprattutto il mercato da sempre più aggressive pratiche anticoncorrenziali. Al riguardo sono note le difficolta incontrate dalle diverse autorità di regolazione e controllo del mercato, preposte alla tutela della concorrenza e della privacy, già nel definire in via preliminare quale sia il rispettivo ambito di competenza, pur essendo possibile, anche se non agevole, individuare un *tradeoff* tra privacy e concorrenza. Quest'ultimo profilo risulta peraltro, come sottolineato dalla Autorità francese e da quella tedesca in un loro presa di posizione comune[42], «*privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which data serves as a main input of its products or services*», evidenziando così quella che è l'ipotesi più comune di illecito (l'abuso di posizione dominante), ma lasciando irrisolta la questione del possibile concorso fra le due normative.[43]

I profili di concorrenza con riguardo al mercato dei Big Data sono noti a tutti, come lo è l'ormai ricca prassi amministrativa formatasi in proposito. Meno approfondito è l'esame delle possibili forme di di interferenza fra i processi concorrenziali e quelli di protezione della privacy, con il rischio che essi finiscano inevitabilmente per sovrapporsi, e con l'ulteriore rischio che vi siano reciproche invasioni di campo, con ricorso a strumenti di tutela diversi per natura ed efficacia, o addirittura reciproche azioni di *self restraint* con un inevitabile vuoto di tutela.

Basti ricordare come nel 2016, in relazione alla controversa cessione dei dati *WhatsApp/Facebook*, si sia aperto in Italia un doppio fronte. Dopo infatti l'apertura dell'istruttoria del Garante per la protezione dei dati personali nel settembre, nel mese successivo anche l'Autorità garante della concorrenza e del mercato (AGCM) aveva avviato due procedimenti istruttori nei confronti della piattaforma di messaggistica istantanea. Contemporaneamente in Europa iniziative analoghe erano avviate dai Garanti della privacy dei vari Paesi.

Va peraltro rilevato come per lungo tempo, la Commissione, seguendo del resto la giurisprudenza della Corte di giustizia,[44] abbia ritenuto che le questioni relative alla violazione della privacy esulassero

[42] Autorité de la concurrence, Bundeskartellamt, *Competition Law and Data*, 10th May, 2016.

[43] *Ibid.*, p. 23 s.

[44] Corte di giustizia, sentenza 23 novembre 2006, causa C-238/05, *Asnef-Equifax*, EU:C:2006:734, dove è stato affermato che le questioni relative alla sensibilità dei dati personali non costituiscono, in quanto tali, questioni di diritto della concorrenza, ma possono essere risolte sulla base delle disposizioni pertinenti in materia di protezione dei dati.

dall'ambito di intervento in materia di concorrenza.[45] A partire dal caso *Google-DoubleClick*,[46] la privacy non ha dunque costituito un dato rilevante ai fini dello scrutinio antitrust. In quell'occasione infatti la Commissione, nel marzo 2008, ha approvato la fusione fra le due società basandosi esclusivamente su una valutazione ai sensi del regolamento concentrazioni, pur sottolineando che eventuali ulteriori rilievi sul versante della tutela della privacy sarebbero stati oggetto di ulteriore e distinta valutazione sulla base della legislazione vigente in materia. Tale orientamento ha trovato conferma nella decisione del 3 ottobre 2010 relativa alla fusione *Facebook/WhatsApp*, dove la Commissione si è limitata ad analizzare «*potential data concentration only to the extent that it is likely to strenghten Facebook's position in the online advertising market or in any sub-segments thereof*». Ciò in quanto «*[a]ny privacy related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*».[47]

L'atteggiamento sembra però essere mutato, almeno sul piano nazionale, con l'avvio da parte della Bundeskartellamt, nel 2016 di un'azione nei confronti di Facebook dove i profili di abuso di posizione dominante ex art. 102 TFUE e di tutela della privacy appaiono indissolubilmente connessi.[48] Tutto ciò mentre però, da parte loro, le autorità garanti della privacy, come già avvenuto nel 2013 nei confronti di Google, per iniziativa coordinata di sei paesi membri, tra cui l'Italia,[49] avviavano proprie azioni, autonome

---

[45] G. COLANGELO, M. MAGGIOLINO, *Data protection and antitrust in the wake of the Bundeskartellamt case against Facebook*, in *Rivista italiana di antitrust*, 2017, pp. 104-112, specie p. 107 ss.

[46] La decisione è reperibile al sito Internet http://europa.eu/rapid/press-release. Riguardo all'atteggiamento assunto dalle autorità statunitensi nel medesimo caso e quindi sul diverso modo di intendere il rapporto fra tutela della concorrenza, dei consumatori e della privacy, vedi R. CAFARI PANICO, *Concorrenza, benessere del consumatore e programmi di* compliance. *Nuove tendenze*, in *Scritti in onore di Giuseppe Tesauro*, vol. II, Napoli, 2014, pp. 1473-1503, specie p. 1495 ss., nonché, con riguardo al divario sempre crescente fra il sistema statunitense e quello europeo di protezione dei dati in connessione con i profili anticoncorrenziali, F.M. LANCIERI, *Digital Protectionism? Antitrust, data protection, and the EU/US transatlantic rift*, in *Journal of Antitrust Enforcement*, 2019, 7, pp. 27-53.

[47] Commissione europea, *Facebook/WhatsApp*, COMP/M.7217, par. 164.

[48] Bundeskartellamt, Press Release «Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules», 2 marzo 2016, reperibile al sito Internet www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html. L'autorità tedesca ha fatto dunque affidamento sul diritto alla tutela dei dati personali come parametro di riferimento per valutare se lo sfruttamento abusivo da parte dell'impresa dominante debba essere considerato un comportamento anticoncorrenziale. Quanto all'esito, vedi Press Release, «Bundeskartellamt prohibits Facebook from combining user data from different sources» del 7 febbraio 2019, relativo alla decisione del precedente 6 febbraio. In merito vedi anche Bundeskartellamt, Case Summary, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, 15 febbraio 2019 (I documenti sono reperibili ai siti Internet https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5 e https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3).

[49] Comunicato stampa del Garante della Privacy, 2 aprile 2013, reperibile al sito Internet http://www.garanteprivacy.it.

rispetto a quelle delle autorità sulla concorrenza e relative al trattamento dei dati, tanto in Germania[50] quanto in Italia,[51] nei confronti dello stesso soggetto (Facebook) verso il quale il trattamento dei Big Data era oggetto di valutazione ai fini concorrenziali. A livello europeo, come pure già ricordato, il Gruppo di lavoro «Articolo 29», che raccoglie i Garanti della privacy dei vari paesi europei, avviava il 27?ottobre2016 una propria indagine parallela sulle modalità di condivisione dei dati degli utenti di WhatsApp con la casa madre Facebook.[52]

È palese dunque il possibile sovrapporsi delle competenze di diverse autorità, ogniqualvolta il diritto alla riservatezza dei dati viene interessato, per il valore economico che essi assumono, da comportamenti con rilevanza concorrenziale. Ciò emerge con evidenza dalla recente iniziativa di indagine conoscitiva congiunta dell'AGCM e del Garante della privacy, del 30 maggio 2017,[53] riguardante l'individuazione di eventuali criticità connesse all'uso dei Big Data e la definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali, la concorrenza dei mercati dell'economia digitale, la tutela del consumatore, nonché i profili di promozione del pluralismo nell'ecosistema digitale. Scopo dell'indagine era perciò verificare se i Big Data possano tradursi in barriere all'ingresso nei mercati o favorire comportamenti restrittivi della concorrenza nonché ledere il diritto alla protezione dei dati delle persone coinvolte. Il possibile concorso dei diversi profili, tra loro complementari, non solo giustifica l'indagine congiunta, ma anche, come precisa l'AGCM nella decisione di avvio, la ricerca di forme di collaborazione fra le due Autorità, cogliendo appieno le possibili sinergie, in modo da consentire a ciascuna il più efficace perseguimento dei rispettivi fini istituzionali.[54]

A interessare in questa sede è l'ottica di tutela del consumatore in cui si muove l'AGCM con riguardo alla protezione delle persone fisiche in tema di trattamento dei dati, come dimostra la decisione dell'11 maggio 2017 dove, di fronte alla eccezione di possibili sovrapposizioni, nel caso che, come già ricordato, riguardava WhatsApp (acquisita nel 2014 dal gruppo Facebook), con le materie regolate dalla normativa sulla privacy, detta Autorità ha ritenuto che quella in oggetto costituisse una pratica

---

[50] The Hamburg Commissioner for Data Protection and Freedom of Information, Press release «Administrative order against the mass syncronisation of data between Facebook and Whatsapp», 27 settembre 2016, reperibile al sito Internet https://datenschutz-hamburg.de/pages/english-press.

[51] Garante per la protezione dei dati personali, Comunicato stampa «Il Garante privacy avvia istruttoria su Whatsapp», 27 settembre 2016, reperibile al sito Internet http://www.garanteprivacy.it.

[52] Si veda Press Release, 28 ottobre 2016, reperibile al sito Internet https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20161028_wp29_press_release_yahoo_whatsapp_enforcement_en.pdf.

[53] Comunicato stampa del Garante per la protezione dei dati personali, 1° giugno 2017, reperibile al sito Internet http://www.garanteprivacy.it.

[54] AGCM, Comunicato stampa – Primi risultati dell'indagine conoscitiva sui Big Data, 8 giugno 2018, reperibile al sito Internet www.agcm.it/media/comunicati-stampa/2018/6/alias-9334. Nello specifico lo studio congiunto si è soffermato su aspetti come la propensione degli utenti a consentire l'uso dei propri dati a fronte dell'erogazione di servizi, il grado della loro consapevolezza in relazione alla cessione e all'utilizzo dei propri dati e alla loro disponibilità a cederli come forma di pagamento dei servizi online.

commerciale scorretta di sua competenza ai sensi del Codice del Consumo,[55] quando invece in Germania la medesima questione è stata oggetto di distinta considerazione anche dal punto di vista della disciplina della protezione dei dati oltre che di quella concorrenziale.

Si realizza così, con soluzioni diverse nei vari paesi, un concorso tra gli strumenti di natura pubblicistica cui si affiancano, secondo forme anch'esse diverse, quelli di natura più prettamente privatistica, in un contesto che deve necessariamente tenere conto delle prospettive future create dalla entrata in vigore, nel 2018, del Regolamento n. 2016/79, relativo al trattamento dei dati personali nonché alla libera circolazione di tali dati, che ha abrogato la direttiva 95/46.

In quest'ultima direttiva già venivano disciplinati i meccanismi che possono essere attivati da ciascun interessato per far valere il proprio diritto al risarcimento del danno eventualmente subito. Sul punto si è così formata una ricca ed interessante giurisprudenza della Corte di giustizia. In particolare, giova prendere in considerazione il più recente episodio di quella che potremmo definire la saga Schrems, ovvero della lotta, perché tale è, ingaggiata da anni da tal Maximilian Schrems[56] nei confronti di Facebook, cui viene imputata la violazione dei suoi diritti alla riservatezza e alla protezione dei dati. La questione riguardava la possibilità che il ricorrente, che dopo aver utilizzato inizialmente Facebook per uso privato, per caricare ad esempio fotografie, pubblicare post e chattare utilizzando i servizi di messaggeria, si era successivamente servito anche di una pagina Facebook per attività quali la pubblicazione di libri, la tenuta di lezioni (anche remunerate), la creazione di siti web e la raccolta di donazioni, potesse continuare ad essere qualificato come consumatore. Il che gli avrebbe consentito di giovarsi dei meccanismi che il diritto dell'Unione ha introdotto sul piano giurisdizionale a tutela del consumatore, in quanto parte debole. Una seconda questione atteneva invece alla circostanza che il sig. Schrems si era fatto cedere da altri sette utenti Facebook i diritti a contestare violazioni identiche.

Questa non era dunque certo la prima delle battaglie intraprese dal sig. Schrems contro Facebook, tanto da rendere il caso in esame sicuramente curioso e al di fuori degli schemi, in quanto lo stesso

---

[55] AGCM, PS10601; si veda anche provvedimento AGCM, PS11112, 29 novembre 2018, con cui si è conclusa l'istruttoria avviata nei confronti di Facebook Ireland Ltd. e della sua controllata Facebook Inc. per violazioni anche in questo caso del Codice del consumo. In tal senso anche, in precedenza, anche, nel caso *Samsung*, AGCM, PS10207, 5 gennaio 2017.

[56] Si ricordi la nota sentenza sul c.d. safe harbour («approdo sicuro»), cioè la valutazione di adeguatezza della legislazione di un paese terzo, pronunciata in relazione ad una vicenda avviata da una denuncia dello stesso sig. Schrems, per il quale il diritto e la prassi statunitense non offrivano una tutela adeguata contro la sorveglianza svolta dalle autorità sui dati trasferiti verso quel paese (Corte di giustizia, sentenza 6 ottobre 2015, causa C-362/14, *Schrems/Data Protecion Commissioner*, EU:C:2015:650. Per un commento, vedi G. FINOCCHIARO, La giurisprudenza della Corte di giustizia in materia di dati personali da *Google Spain* a *Schrems*, in *Il diritto dell'informazione e dell'informatica*, 2015, pp. 779-799; e L. VALLE-L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Il diritto dell'informazione e dell'informatica*, 2017, pp. 169-224, anche con riguardo alla disciplina di cui alla Convenzione n. 108 del Consiglio d'Europa.

Schrems, come osserva l'Avvocato generale Bobek,[57] si era col tempo trasformato da consumatore coinvolto in misura crescente in controversie giuridiche in un vero e proprio professionista delle controversie in materia di consumatori con bersaglio privilegiato il colosso Facebook. In tali circostanze il sig. Schrems, che ha fatto della lotta a Facebook una ragione di lavoro se non di vita, può ancora essere considerato un consumatore speciale bisognoso di tutela? La risposta non è agevole in quanto non lo è la qualificazione di consumatore. Come rileva al riguardo l'Avvocato generale, nel caso di piattaforme di social media, come Facebook, tra l'universo sociale alimentato dal numero di like ricevuti e il numero di amici Facebook e la presentazione a fini commerciali di una grande impresa vi sono tutta una serie di sfumature. O meglio, tra i due estremi dell'uso marcatamente privato e l'altro chiaramente commerciale, osserva l'avvocato generale, «esistono cinquanta sfumature di blu (Facebook)».[58]

Nel caso dunque di uso promiscuo di account e pagine Facebook e più in generale dei social media non è possibile tracciare una netta separazione tra attività privata e professionale. La conclusione dell'Avvocato generale è che le attività di mera promozione, pur connesse alla sfera professionale dell'utente, non generando un ritorno economico immediato e non costituendo esse stesse attività commerciali economicamente rilevanti, non siano tali da incidere sulla qualificazione del rapporto intrattenuto sul piano contrattuale con il social media dal sig. Schrems, che deve pertanto essere considerato come consumatore anche per l'attività più professionale svolta sulla pagina Facebook.

Non meno interessanti, ma non altrettanto soddisfacenti per il consumatore, sono le considerazioni svolte dall'Avvocato generale in merito alla possibilità che il consumatore possa far valere oltre ai propri diritti anche quelli di altri consumatori che glieli hanno ceduti. In sostanza, si tratterebbe di una sorta di class action promossa dai consumatori. L'Avvocato generale su questo aspetto è categorico: la questione attiene alla autonomia procedurale di ciascuno Stato mentre non vi è alcun elemento che induca a ritenere che il diritto dell'Unione consenta l'esercizio di una azione collettiva in materia di contratti conclusi dai consumatori. Per quanto auspicabile possa essere l'adozione di strumenti di diritto dell'Unione in materia di azione collettiva, allo stato il tutto rimane a livello di proposte e per di più il problema non può essere certo risolto da un intervento del giudice europeo richiedendo la materia una disciplina organica che non può essere ottenuta in sede giurisdizionale.[59] La soluzione che esclude di fatto la cessione dei contratti dalle ipotesi di azione collettiva è in linea del resto con il dettato normativo dell'art. 140 *bis* del Codice del consumo che limita tali azioni alle ipotesi di mandato e non di cessione di contratto escludendo una assimilazione delle diverse ipotesi.

---

[57] Conclusioni del 14 novembre 2017, causa C-498/16, *Schrems*, ECLI:EU:2017:863.

[58] *Ibid.*, punto 46.

[59] Per un commento, G.M. RUOTOLO, *I dati non personali: l'emersione dei* big data *nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, pp. 97-116.

Da parte sua, la Corte di giustizia,[60] esprimendosi, anzitutto, sulla nozione di consumatore, dichiara che l'art. 15 del regolamento n. 44/2001 deve essere interpretato nel senso che un utilizzatore di un account Facebook privato non perde la qualità di «consumatore» ai sensi di detta disposizione allorché pubblica libri, tiene conferenze gestisce siti Internet, raccoglie donazioni e si fa cedere i diritti da altri consumatori al fine di far valere in giudizio tali diritti.[61] Cionondimeno, quanto alla possibilità che il consumatore possa giovarsi della regola di competenza speciale posta dall'art. 16, par. 1, di detto regolamento, a tutela della parte economicamente più debole, la Corte conclude che tale deroga deve essere oggetto di un'interpretazione restrittiva e che pertanto essa non si applica all'azione di un consumatore volta a far valere non soltanto diritti propri ma anche diritti ceduti da altri consumatori.[62]

Resta il fatto che la nozione di consumatore accolta dalla Corte può avere un impatto rilevante sulla disciplina dei contratti con i social media sul piano anche, ma non solo, giurisdizionale, per gli inevitabili riflessi che avrebbe in relazione al diritto applicabile al merito delle clausole contrattuale, specie tenendo conto del richiamo spesso previsto nei contratti alla giurisdizione inglese, destinato a divenire problematico nei riguardi dei paesi dell'Unione a seguito della imminente uscita del Regno Unito.

A testimonianza del continuo sforzo di adeguamento delle categorie del diritto ad una realtà – quella dei Big Data – difficilmente riconducibile sul piano tassonomico agli schemi usuali, va ricordata un'altra presa di posizione, del 24 ottobre 2017,[63] questa volta dell'Avvocato generale Bot, sul tema, in un certo senso complementare a quello precedente, di chi debba intendersi per responsabile del procedimento al fine di individuare quale sia l'autorità statale competente ad intervenire e quindi il diritto applicabile in relazione, questa volta, ad attività segnatamente commerciali. Si trattava nella specie di un provvedimento dell'autorità di vigilanza regionale per la protezione dei dati del Land Schleswig-Holdstein emesso nei confronti di una società tedesca cui era richiesto di disattivare una fanpage gestita sul sito di Facebook Ireland Ltd.

La violazione contestata riguardava l'utilizzo di *cookie* da parte di Facebook per realizzare statistiche sugli utenti al fine ultimo di diffondere pubblicità mirate.

La questione dell'individuazione del diritto nazionale applicabile e dell'autorità competente per l'intervento appare sicuramente complessa per l'intervento di più soggetti posti anche al di fuori dell'Unione. In un momento poi in cui le autorità di vigilanza di vari paesi sono intervenute ad infliggere

---

[60] Corte di giustizia, sentenza 25 gennaio 2018, causa C-498/16, *Schrems*, EU:C:2018:37.

[61] *Ibid.*, punto 41.

[62] *Ibid.*, punto 49. Sui problemi posti in tema di giurisdizione dalla nozione di «consumatore di servizi digitali» sviluppata a seguito della giurisprudenza *Schrems* e alla luce dell'opportunità di un coordinamento con le previsioni del regolamento (UE) 2018/302 sulla geolocalizzazione non giustificata, vedi S. DOMINELLI, *"Geolocalizzazione" e tutela dei "consumatori di servizi digitali": prime riflessioni di diritto internazionale privato e processuale uniforme*, in corso di pubblicazione.

[63] Conclusioni 24 ottobre 2017, causa C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2017:796.

sanzioni a Facebook per la violazione delle norme relative alla protezione dei dati dei suoi utenti, diviene essenziale definire la portata dei poteri di intervento delle singole autorità di vigilanza.

La società tedesca offriva servizi di formazione attraverso una fanpage gestita sul social network Facebook. Le fanpage sono account utenti che possono essere attivate su Facebook da singole persone imprese. Per farlo, il gestore della fanpage deve registrarsi presso Facebook e può così utilizzare la piattaforma da quest'ultimo amministrata per presentarsi agli utenti di detto social network e per diffondere comunicazioni di ogni tipo al fine in particolare di sviluppare un'attività commerciale. Non essendo stati gli utenti della fanpage informati che Facebook raccoglieva i loro dati personali servendosi di cookie e che sottoponeva tali dati ad un trattamento successivo, l'autorità di vigilanza aveva ordinato alla società gestore di disattivare la pagina che essa aveva creato su Facebook. Il gestore contestava la circostanza di poter essere considerata responsabile del trattamento dei dati compiuto da Facebook e dei cookie da quest'ultimo installati. Semmai l'azione avrebbe quindi dovuto essere avviata nei riguardi di Facebook e non certo in Germania. La questione viene rimessa dal giudice adito all'interpretazione della Corte di giustizia.

Quanto al primo profilo, l'Avvocato generale ritiene che per gli scopi della direttiva sulla protezione dei dati il gestore e Facebook avessero un controllo congiunto, seppure esso non fosse per il gestore completo, con la conseguenza che anche quest'ultimo poteva essere qualificato come responsabile dei trattamenti dei dati personali nell'ottica dell'elaborazione di statistiche sugli utenti della pagina Facebook, a fianco di Facebook Inc. e Facebook Ireland[64]

Stante il coinvolgimento non solo della società irlandese ma anche di Facebook Inc., che dagli Stati uniti fornisce servizi di social network nel territorio, la questione successiva era se l'autorità tedesca fosse competente ad adottare, in base alle proprie norme, provvedimenti anche nei confronti di soggetti, responsabili del trattamento, situati in altri paesi membri o addirittura in paesi terzi.[65] La risposta positiva si basa, secondo il ragionamento dell'avvocato generale, che si discosta in parte dalla precedente giurisprudenza, su due considerazioni: la prima è volta a stabilire la competenza della autorità tedesca a garantire il rispetto delle disposizioni in materia di protezione dei dati in ragione della presenza in Germania di uno stabilimento di Facebook Ireland che, pur non potendo essere considerata quale responsabile del trattamento, quale lo era invece Facebook Ireland, tuttavia svolgeva una attività inscindibilmente connessa a tale trattamento.[66] La seconda attiene alla individuazione del destinatario delle misure adottate dalla competente autorità di vigilanza. La conclusione è che competenza, così determinata, può esercitarsi nei confronti del responsabile del trattamento anche quando questo sia

[64] *Ibid.*, punto 58.
[65] *Ibid.*, punto 78.
[66] *Ibid.*, punto 121.

situato in un altro Stato membro o in un paese terzo[67], mirando a garantire che nel territorio tedesco il trattamento dei dati sia conforme a quel diritto, senza che vi sia bisogno di richiedere previamente all'autorità di vigilanza dello Stato membro in cui è situato il responsabile del trattamento (nella specie l'autorità irlandese) di esercitare i suoi poteri.[68] La conseguenza è che qualora il responsabile del trattamento disponga di stabilimenti in più Stati membri esso è soggetto al controllo di più autorità di vigilanza ogniqualvolta trovino applicazione le normative degli Stati di dette autorità.

Le considerazioni dell'Avvocato generale sono state fatte proprie dalla Grande Sezione della Corte di giustizia nella sentenza 5 giugno 2018.[69] Secondo la Corte il riconoscimento di una responsabilità congiunta del gestore del social network e dell'amministratore di una fanpage presente su tale network in relazione al trattamento dei dati personali dei visitatori di tale fanpage contribuisce a garantire una più completa tutela dei diritti di cui godono le persone che visitano una fanpage. L'esistenza di tale corresponsabilità non si traduce però necessariamente in un responsabilità equivalente dei diversi operatori nell'ambito di un trattamento di dati personali.[70] Quanto poi alla possibilità di esercizio dei poteri di controllo nei confronti di una impresa stabilita al di fuori dell'Unione che disponga di varie filiali in diversi Stati membri, la Corte accoglie anche su questo punto la soluzione estensiva suggerita dall'Avvocato generale,[71] affermando al contempo l'autonomia del potere di controllo esercitato da ciascuna autorità di uno Stato membro.[72]

I rischi di sovrapposizione di competenze e di possibili soluzioni confliggenti nei diversi paesi sono evidenti e ad essi ha inteso porre rimedio il meccanismo dello sportello unico introdotto dal regolamento 2016/679. Seppur in parte superate dalle norme del nuovo regolamento, che introducono il principio dello one-shop stop, attribuendo competenza alla autorità di controllo dello stabilimento principale che diviene autorità capofila per i trattamenti transfrontalieri e forme di collaborazione tra le varie autorità oltre ad un meccanismo di coerenza, i principi sanciti dalla Corte di giustizia e precedentemente affermati dall'Avvocato generale costituiscono un importante passo in avanti per la comprensione dei nuovi modelli di business in uno sforzo di adeguare la tutela del consumatore ad una realtà complessa e sempre più dinamica ed articolata.

Le conclusioni cui è pervenuta la Corte nella sentenza *Wirtschaftsakademie Schleswig-Holstein* con riguardo alla responsabilità congiunta sono state peraltro oggetto di riesame da parte dell'Avvocato

[67] *Ibid.*, punto 128.
[68] *Ibid.*, punto 136.
[69] Causa C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388.
[70] *Ibid.*, punto 42.
[71] *Ibid.*, punto 64.
[72] Ibid., punto 74.

generale Bobek nel caso *Fashion ID*[73], alla luce anche delle precisazioni fornite dalla stessa Corte nella sentenza *Jehovan todistajat*.[74]

L'Avvocato generale muove dalla constatazione di come alla luce di tale giurisprudenza anche la società Fashion ID, che aveva inserito un plugin nel suo sito Internet (ovvero, il pulsante «Like» di Facebook),[75] aveva agito come responsabile del trattamento ed era perciò corresponsabile, assieme a Facebook Ireland, del trattamento dei dati.[76] Ciò premesso, l'Avvocato generale si pone la domanda se effettivamente tale forma di attribuzione di (cor)responsabilità sia effettivamente idonea a rafforzare la protezione dei dati personali.[77] La risposta, che tiene anche conto del regime di responsabilità congiunta introdotto dal GDPR, non applicabile *ratione temporis* alle cause considerate, è che la responsabilità (congiunta) del responsabile del trattamento debba essere limitata alle operazioni «per le quali esso codecide effettivamente sugli strumenti e sulle finalità del trattamento dei dati personali»,[78] aprendo così un dibattito sulle finalità e sugli strumenti del trattamento dei dati personali, che, costituendo gli elementi essenziali della corresponsabilità,[79] devono essere oggetto di una valutazione tanto puntuale quanto non agevole, al fine di individuare una graduazione delle singole responsabilità alla luce di tutte le circostanze rilevanti del caso di specie, non sussistendo, come del resto già affermato dalla Corte di giustizia nel caso *Wirtschaftsakademie Schleswig-Holstein*, seppure senza ulteriori approfondimenti, una presunzione di responsabilità equivalente dei diversi operatori coinvolti.

4. Conclusioni.

In conclusione, la tutela del titolare dei dati nella sua veste di consumatore può trovare risposta nell'azione coordinata delle autorità preposte alla tutela della concorrenza e della privacy, ma anche negli strumenti giurisdizionali offerti dalla direttiva 2014/104,[80] sul *private enforcement*, per quanto riguarda la concorrenza, e prima dalla direttiva 95/46, e ora dal regolamento 2016/679, per quanto attiene alla

[73] Conclusioni 19 dicembre 2018, causa C-40/17, EU:C:2018:1039. A tale causa, allora pendente, aveva fatto riferimento l'avv. gen. Bot nelle Conclusioni del 24 ottobre 2017, causa C-210/16, cit., per affermare che non si può ravvisare «alcuna differenza essenziale tra la situazione di un gestore di fanpage e quella del gestore di un sito web che inserisce, all'interno dello stesso, il codice di un fornitore di servizi di *webtracking*» (punto 69).

[74] Sentenza 10 luglio 2018, C-25/17, EU:C:2018:551.

[75] Di conseguenza quando un utente entrava nel sito Internet della società le informazioni relative all'indirizzo IP e alla stringa del browser di tale utente erano trasferite a Facebook. Detto trasferimento avveniva automaticamente quando si apriva il sito Internet, indipendentemente dal fatto che l'utente avesse cliccato o meno il pulsante «Like» o avesse o meno un account Facebook.

[76] Conclusioni 19 dicembre 2018, causa C-40/17, cit., punto 66.

[77] *Ibid.*, punto 71 ss.

[78] *Ibid.*, punto 108.

[79] *Ibid.*, punto 101.

[80] Direttiva 2014/104/UE del Parlamento europeo e del Consiglio, del 26 novembre 2014, relativa a determinate norme che regolano le azioni per il risarcimento del danno ai sensi del diritto nazionale per violazioni delle disposizioni del diritto della concorrenza degli Stati membri e dell'Unione europea, in GUUE, L 349 del 5 dicembre 2014, pp. 1-19.

privacy, in un quadro normativo in cui sarebbero auspicabili non solo, da un lato, un pieno coordinamento dell'azione delle autorità preposte ai due settori in oggetto e, dall'altro, l'introduzione negli ordinamenti nazionali di strumenti analoghi per la tutela del titolare/consumatore in entrambi gli scenari. Basti ricordare in proposito quanto di recente dichiarato dalla Commissaria Vestager[81], che, proprio richiamando in tema di Big Data il concorso, nel caso *Microsoft/Linkedin*, dei profili sia concorrenziali sia di privacy, non solo rivendicava il fatto che la Commissione si era posta come obiettivo anche la tutela del diritto fondamentale del singolo ai propri dati personali, affermando così il ruolo centrale del profilo concorrenziale, ma auspicava anche che la Commissione potesse dotarsi di strumenti quali quelli previsti dal regolamento 2016/679, che consentono una uniformità di protezione a livello europeo. Le pur comprensibili osservazioni della Commissaria si scontrano peraltro con una realtà del tutto diversa, sbilanciata com'è, quanto alla effettività dei meccanismi di tutela, a favore della disciplina della concorrenza, la cui «scatola degli attrezzi» appare di per sé sufficientemente adeguata per fronteggiare le peculiarità del nuovo mercato digitale.[82] Ciò non toglie che anche la concorrenza possa beneficiare degli strumenti propri della tutela del consumatore e della protezione dei dati. Non a caso infatti l'AGCM non ha esitato a fare ricorso nei confronti di Facebook agli strumenti propri della tutela del consumatore, piuttosto che al diritto antitrust, approfittando del fatto che a gestirli sia la stessa autorità. Tuttavia proprio i continui cambiamenti tecnologici possono richiedere una risposta più articolata e flessibile che non può fare a meno di un coordinamento, finora solo abbozzato, con le istituzioni preposte alla protezione dei dati, che a loro volta, se lasciate sole, soffrono della minor «forza» degli strumenti di cui beneficiano.

Significative dell'attuale asimmetria regolamentare sono le proposte formulate nell'ottobre del 2016 dall'OCSE[83] che, esaminando il mercato dei Big Data, dopo aver dedicato il proprio studio quasi per intero ai profili concorrenziali, dedica un paragrafo anche alla tutela del diritto del consumatore alla riservatezza dei suoi dati personali, indicando come soluzione il ricorso a più efficaci strumenti contrattuali e a nuovi modelli di business, che possono consentire la creazione di un mercato virtuale in cui i consumatori negoziano la cessione contro corrispettivo dei propri dati personali alle imprese interessate.

Quello che si delinea è sicuramente un contesto sempre più complesso e sempre più diversificato di tutela multilivello sul piano sia amministrativo sia giurisdizionale, sia nazionale sia europeo, in cui dal

---

[81] M. VESTAGER, *What competition can do-and what it can't*, Chilling Competition Conference, 25 October 2017, reperibile al sito Internet https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements.

[82] A. PEZZOLI, "With a little help from my friends": *quale politica della concorrenza per l'economia digitale?*, in *Economia italiana*, 2019, pp. 20-37, specie p. 20 s.

[83] OCDE, *Big Data: bringing Competition Policy to the Digital Era*, DAF/COMP(2016)14, reperibile al sito Internet www.oecd.org/daf/competition.

punto di vista del titolare dei diritti assume un ruolo fondamentale il meccanismo dell'azione collettiva, unica idonea ad evitare che quella del singolo diventi la lotta di Davide contro Golia, in un mondo dove l'innovazione tecnologica segnerà il mutare continuo delle regole del gioco. È evidente che dal punto di vista del consumatore ad offrire maggiore tutela sia l'intervento della autorità sulla concorrenza, che si avvale di ben più sofisticati strumenti e di più matura esperienza. La collaborazione fra le autorità garanti della concorrenza, specie a seguito dell'adozione della direttiva n. 2019/1,[84] appare ben più incisiva della collaborazione nell'ambito del Gruppo di lavoro «Articolo 29», anche se il nuovo regolamento potrebbe dare ulteriore impulso alla collaborazione transnazionale. A far poi la differenza sono, da un lato, i meccanismi di collaborazione con le autorità giurisdizionali nazionali nonché con la stessa Commissione, e, dall'altro, per quanto concerne specificamente l'utente, i meccanismi di private enforcement introdotti dalla relativa direttiva, ben più incisivi di quelli di *private enforcement* previsti dal regolamento 2016/679, già peraltro più ampi rispetto a quanto previsto in precedenza nella direttiva 95/46.[85] L'auspicio non è quello di un assorbimento dei due ambiti di tutela, ma di certo un efficace coordinamento ed un progressivo avvicinamento degli strumenti di tutela del titolare dei dati sulla base dei due distinti ordini di norme sarebbero fortemente auspicabili.

[84] Direttiva (UE) 2019/1 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno, in GUUE, L 11 del 14 gennaio 2019, pp. 3-33.

[85] M. REQUEIRO ISIDRO, *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection*, in *MPILux Research Paper Series 2019 (3)*, reperibile al sito Internet www.mpi.lu.