IAIC MiBACT DGBIC CREDA

DIRITTO MERCATO TECNOLOGIA

NUMERO SPECIALE 2017

IL MERCATO UNICO DIGITALE

a cura di GIANLUCA CONTALDI

UNIVERSITÀ DI MACERATA
26 OTTOBRE 2016
ATTI DEL CONVEGNO

Nuova
Editrice
Universitaria

Diritto Mercato Tecnologia

Il convegno del 26 ottobre 2016 si inserisce nel Progetto Nazionale dei C.D.E Italiani dal titolo "Un Mercato Unico Digitale per l'Europa" promosso dalla Rappresentanza in Italia della Commissione Europea.

DIRITTO MERCATO TECNOLOGIA

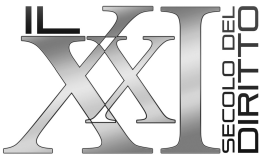
NUMERO SPECIALE 2017

IL MERCATO UNICO DIGITALE

A CURA DI GIANLUCA CONTALDI

UNIVERSITÀ DI MACERATA — 26 OTTOBRE 2016

ATTI DEL CONVEGNO



Via C. T. Masala, 42 – 00148 Roma
e-mail: nuovaeditriceunivers@libero.it

Finito di stampare nel mese di dicembre 2017
dalla Infocarcere s.c.r.l.
Via C. T. Masala, 42 – 00148 Roma

ISBN: 978-88-95155-71-5

DIRITTO MERCATO TECNOLOGIA

NUMERO SPECIALE 2017

IL MERCATO UNICO DIGITALE

SOMMARIO

Alberto Gambino
Università Europea di Roma

Dignità umana e mercato digitale

Sommario: 1. Introduzione – 2. Anonimato ed Internet – 3. Videogioco e dignità umana – 4. Protezione dei dati personali - 5. Negozio giuridico tra *blockchain* e *smart contracts* – 6. *Net neutrality* e *zero rating* – 7. Contratti relazionali – 8. Il nuovo ruolo dell'*influencer* – 9. Conclusioni

1. Introduzione

È indubbio che il termine Internet evochi un grande spazio di libertà, un luogo – come si è detto – dove dare forma all'esercizio dei propri diritti. Allo stesso tempo, tuttavia, è anche vero che la Rete ha inciso in modo netto sui concetti di diritto e libertà, sul loro significato, determinando delle modifiche non trascurabili. Questo saggio nasce proprio dal tentativo di esaminare e razionalizzare l'esperienza della *Digital Revolution*, che ha portato a mettere in discussione tradizionali punti di riferimento del ragionamento giuridico e ad affrontare lo sforzo di ricostruire nuove categorie e tecniche, con il fine ultimo di garantire un diritto persuasivo[1]. È in questo contesto che si inquadra questo breve scritto sulla buona fede ed i rapporti telematici.
È bene *in primis* sottolineare che di rapporti telematici, e non semplicemente di contratti telematici, dovrebbe discutersi. Ciò in quanto rispetto al passato, in cui ci si soffermava sui concetti di negoziazione a distanza ed esecuzione dei rapporti online, sembrano essersi inserite alcune devianze ed allo stesso tempo metamorfosi dei contenuti delle di-

[1] V. SCHULZE e STAUDENMAYER (a cura di), *Digital Revolution: Challenges for Contract Law in Practice*, Baden-Baden, 2016.

chiarazioni online che sembrano fuggire dal modello negoziale. *L'Idealtypus* non è più pertanto nell'autonomia negoziale e nel negozio giuridico.

Pare, piuttosto, che ad internet si possa conferire la qualificazione di formazione sociale[2], di cui presenta l'elemento materiale (ossia l'insieme dei soggetti), teleologico (lo scopo) e psicologico (la volontarietà di farne parte), a cui si aggiunge l'interesse particolare che disattende l'interesse dello Stato o quanto meno diventa peculiare rispetto all'interesse statuale. Una tale interpretazione andrebbe pienamente a disattivare il problema della giurisdizione, ossia il passaggio da princìpi generali astratti o globali alla statualità, invece, dei princìpi. Entreremmo, tipicamente, in una sfera in qualche modo impermeabile a quelli che sono princìpi di fonte normativa o, non può escludersi, di fonte transnazionale.

Certo è che una certa attenuazione fra una regolamentazione giuridica forte, *pleno iure*, statuale e l'assenza di normazione - che invece sembra talvolta essere percepita dagli utenti della rete - potrebbe, a questo punto, trovare un suo impianto sistematico in questa tesi. Si tratta dell'attribuzione, *sub specie iuris,* della *netiquette*, ossia di un insieme di regole di condotta il cui rispetto era richiesto agli utenti nel momento in cui accettavano, aderivano alla partecipazione sociale, comunicativa, informativa della rete.

---

[2] Su tutti, v. PASSAGLIA, *Le formazioni sociali e Internet*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 50. V. anche LEVI, *Le Formazioni Sociali*, Milano, 1999; BIANCA-GAMBINO-MESSINETTI (a cura di), *Libertà di Manifestazione del Pensiero e Diritti Fondamentali: Profili Applicativi nei Social Networks*, Milano, 2016; PIROZZOLI, *La libertà di riunione in Internet,* in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2004, pp. 595-627; PASSAGLIA, *Internet e pluralismo sociale*, in *Percorsi Costituzionali*, 1, 2014, pp. 75-96; ROSSI, *Le formazioni Sociali nella Costituzione Italiana*, Padova, 1989.

2. Anonimato ed Internet

A tal proposito, un tema particolarmente interessante da affrontare sarebbe quello della relazione tra anonimato ed individuazione delle responsabilità o imputazione, in merito ad esempio ad una dichiarazione[3]. La distinzione può certamente giocare un ruolo importante nella fase della giurisdizione. Tuttavia, nel campo delle formazioni sociali, tipicamente, l'anonimato può ampiamente sussistere. In sostanza, in assenza di una identificabilità strutturata del soggetto che agisce in rete, l'unico elemento o traccia è rappresentato da un indirizzo IP, un numero, un codice o un'identità alfanumerica. Il soggetto presente sullo sfondo potrebbe dunque rimanere occulto fintanto che non ci sia richiesta di un'autorità giudiziaria. Si potrebbe allora reinterpretare la rete come fenomeno di formazione sociale in cui le sanzioni vengono irrogate dagli operatori-attori della rete stessa. Quando il *troll* è un disturbatore viene disconnesso, ad esempio da parte di un moderatore, e questa reazione-sanzione si rivela efficace in quanto espelle dalla comunità il soggetto.

3. Videogioco e dignità umana

In tale quadro, sembra utile richiamare alcune fattispecie specifiche, comunque inerenti l'inquadramento dei rapporti telematici. Una prima

[3] Cfr. RESTA, *L'anonimato in Internet*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 66. V. anche MANETTI, *Libertà di pensiero e anonimato in rete*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2014, pp. 139-152; RICCIO, *Diritto all'anonimato e responsabilità civile del provider*, in *Internet e il diritto dei privati. Persona e proprietà intellettuale nelle reti telematiche*, a cura di Nivarra e Ricciuto, Torino, 2002; RODOTÀ, *Il Diritto di Avere Diritti*, Roma-Bari, 2012; VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2014, pp. 207-223; FINOCCHIARO, *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Trattato di Diritto Commerciale e di Diritto Pubblico dell'Economia*, diretto da Galgano, Padova, 2008; CUNIBERTI, *Democrazie, dissenso politico e tutela dell'anonimato*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2014, pp. 111-137.

fattispecie che merita attenzione concerne a mio avviso l'utilizzo di videogiochi di tipo *free-to-play* basati su realtà aumentata geo-localizzata con GPS. Tipico esempio, di tempi recenti, è rappresentato dal videogioco *Pokemon Go,* in cui il protagonista interagisce nell'ambiente reale attraverso il *device* (ossia lo smartphone) e nel cui contesto entrano in gioco persone reali. Nei fatti, il videogioco ha dato luogo a diverse questioni di natura giuridica, aventi ad oggetto ad esempio la tutela dell'ordine pubblico, il rispetto della proprietà privata, nonché la tutela della privacy o la protezione della dignità umana[4].

Proprio a tal riguardo, il coinvolgimento di persone fisiche, reali, che appaiono sulla scena involontariamente, ha portato la giurisprudenza a chiedersi se il contesto reale-virtuale in cui si svolge il videogioco non vada a ledere la loro dignità, a causa del disegno automatizzato della loro personalità inconsapevolmente offerta ai *players*[5]. In sostanza, nel

[4] Su tutti, v. PIZZETTI, *Il videogioco Pokemon Go e la tutela della dignità delle persone – uno spunto di riflessione sulla realtà aumentata alla luce del caso Omega*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 84. V. anche AZZONI, *Dignità dell'uomo e diritto privato*, in *Ragion Pratica*, 2012, pp. 75-97; CONTI, *La dignità umana dinanzi alla Corte di Giustizia,* in *Corriere Giuridico,* 2005, pp. 488-495; FLICK, *Elogio della Dignità*, Roma, 2015; RODOTÀ, *La Rivoluzione della Dignità*, Brescia, 2013; SCOGNAMIGLIO, *Dignità dell'uomo e tutela della personalità*, in *Giustizia Civile*, 2014, pp. 67-93; DI CIOMMO, *Dignità Umana e Stato Costituzionale*, Firenze, 2010.

[5] V. anche Corte giust. UE, Caso C-36/02 *Omega v Oberburgermeisterin* [2004] ECR I-9641. Nel caso, si discusse se lo sfruttamento commerciale del gioco costituiva una violazione della dignità umana. Come richiamato dalla Corte, 'il giudice del rinvio espone che la dignità umana è un principio costituzionale che può essere violato sia attraverso un trattamento degradante dell'avversario, cosa che non si verifica nel caso di specie, sia risvegliando o rafforzando nel giocatore un'attitudine che neghi il diritto fondamentale di ogni persona ad essere riconosciuta e rispettata, come la rappresentazione, nel caso di specie, di atti fittivi di violenza a scopo di gioco. Un valore costituzionale supremo quale la dignità umana non può essere soppresso nell'ambito di un gioco. I diritti fondamentali invocati dall'Omega non possono, nei confronti del diritto nazionale, modificare tale valutazione'. Per una analisi del caso *Omega*, v. PELLECCHIA, *Il caso Omega: la dignità umana e il delicato rapporto tra diritti fondamentali e libertà (economiche) fondamentali nel diritto comunitario*, in *Europa e Diritto Privato*, 2007, pp. 181-194.

videogioco, sembrerebbe esserci una sorta di ultra-attività rispetto a quelli che sono i soggetti di un rapporto telematico; persone reali ricevono nocumento per il fatto di ritrovarsi contestualmente in quell'ambito, anche se sono del tutto estranee alla competizione. È dunque legittimo richiamare le parole della Corte costituzionale del 1963 che, proprio con riferimento alle licenze di uso di apparecchi e congegni, affermava che è necessario impedire che la dignità umana riceva offesa dallo sterile impiego dell'autonomia individuale[6].

4. Protezione dei dati personali

Una seconda fattispecie attiene poi all'attività di profilazione ed al consenso al trattamento dei dati personali[7]. Come sostenuto dal Garante della Privacy, attraverso le linee guida, l'informativa deve essere chiara e completa e deve esservi un consenso ogni qualvolta la profilazione abbia finalità commerciali. In sostanza, l'interessato ha diritto a non essere oggetto di decisioni automatizzate ogniqualvolta siano fondate su elementi personali. L'utilizzo che si fa dei dati sembra assumere un ruolo centrale nell'analisi.

---

[6] Cfr. Corte cost., sentenza del 9 luglio 1963, n. 125.

[7] Sul tema, v. PIZZETTI e MONTUORI, *Il nuovo Regolamento Data Protection e le sfide dell'innovazione digitale*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 109; VANONI, *La protezione dei dati personali: privacy v. sicurezza nazionale*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 141; PIZZETTI, *Privacy ed il Diritto Europeo alla Protezione dei Dati Personali*, Torino, 2016; RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015, pp. 697-718; BASSINI, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni Costituzionali*, 3, 2016, pp. 587-590; FUMAGALLI e MERAVIGLIA, *Le nuove norme europee sulla protezione dei dati personali*, in *Il Diritto negli Scambi Internazionali*, 1, 2016, pp. 1-39; STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto Privato*, 4, 2016, pp. 1249-1264.

È recente l'intervento del Garante della Privacy che ha segnalato la necessità di informare le persone che osservano le pubblicità proiettate sui *totem*, presenti nelle principali stazioni ferroviarie italiane, sulla presenza di una telecamera che registra ed analizza le loro reazioni[8]. Sulla base dei dati acquisiti, concernenti ad esempio sesso ed età di un individuo, un'impresa ben potrebbe costruire una campagna pubblicitaria *ad hoc*. Nel suddetto contesto, le persone diventano inconsapevolmente oggetto di studio di algoritmi, contribuendo al profitto di chi utilizza quei dati. Quali i riflessi sulla dignità della persona, alla luce dei possibili rischi di tracciamento e monitoraggio?

5. Negozio giuridico tra *blockchain* e *smart contracts*

Proseguendo in questa breve trattazione, non si può di certo tralasciare il fenomeno della *blockchain*[9], ossia di quella tecnica o *disruptive technology* dove la verità non viene più accertata da un soggetto terzo certificatore, ma dalla maggioranza degli informatici, potremmo dire 'tecnocrati'. Fondamentalmente, una *blockchain* è un registro o database aperto e distribuito che può registrare le transazioni tra due parti in modo permanente, verificabile ed efficiente, sfruttando una rete *peer to peer* che si collega ad un protocollo per la convalida dei nuovi *blocks*. Pertanto, la *blockchain* permette di ottenere quelle garanzie di *trust*, fiducia ed affidabilità che nel passato erano necessariamente legate ad una figura terza, un notaio od avvocato.
All'interno della dimensione *blockchain,* in un rapporto di funzionalità,

[8] V. Garante per la Protezione dei Dati Personali, Provvedimento del 21 dicembre 2017, n. 7496252 (*Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria*).
[9] Sul significato del termine, v. Parlamento UE - DG European Parliamentary Research Service, Report del 20 Febbraio 2017 (*How blockchain technology could change our lives*). V. anche GAMBINO, *Blockchain e Assicurazione*, in *Convegno su Assicurazione e Nuove Tecnologie*, Firenze, 2018.

si collocano gli *smart contracts* o contratti intelligenti, ossia quei contratti che si eseguono automaticamente[10]. Lo *smart contract*, dando esecuzione immediata a una serie di clausole contenute nel programma negoziale, non consente alla parte di reagire, e, se una reazione tardiva si verifica, è probabile che dia luogo agli effetti di una eventuale penale. Uno *smart contract*, in breve, potrebbe essere interpretato come la traduzione o trasposizione in codice di un contratto (o insieme di input, dati, informazioni specifiche) al fine di verificare in automatico l'avverarsi di determinate condizioni e di eseguire in automatico determinate azioni nel momento in cui le condizioni negoziate tra le parti si verificano. Semplificando, se è vero che uno *smart contract* ha bisogno di un supporto legale per la sua stesura, è altrettanto vero che tale bisogno cessa per la sua verifica ed attivazione. Lo *smart contract* si avvale della *blockchain* per garantire che il codice che è alla sua base non possa essere modificato, che le fonti di dati che definiscono le condizioni di applicazione siano certificate ed affidabili, e che la lettura e controllo di queste fonti sia a sua volta certificata. Un esempio di *smart contracts* può rinvenirsi negli odierni contratti di assicurazione per autoveicoli, che, richiedendo l'utilizzo a bordo delle vetture di apparecchiature *Internet of Things* (*IoT*) per la trasmissione di dati sul comportamento del conducente, fanno si che determinate clausole e condizioni contrattuali si attivino o disattivino automaticamente. Si pensi al caso del frequente superamento del limite di velocità da parte del contraente; il dato, trasmesso dalle apparecchiature *IoT*, potrebbe essere interpretato dalla compagnia assicurativa come un elemento di rischio, e potrebbe di conseguenza determinare delle modifiche contrattuali alle condizioni applicate.

Ebbene, a fronte di tale quadro, non abbiamo più la certezza – intesa in senso tradizionale - della genesi del rapporto negoziale. O meglio, ciò che è mutato in maniera sostanziale è il modo per verificare la certezza

[10] Cfr. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Torino, 2016, p. 200.

giuridica di un fatto. È vero che l'input iniziale è comunque fornito dalla mente umana; nelle fasi successive, tuttavia, il controllo è affidato ad un sistema basato su algoritmi, che conseguentemente pone serie problematiche in tema di giurisdizione, di tracciabilità degli eventuali vizi dei vari atti, e di convenienza nel richiedere l'intervento dell'autorità giudiziaria.

6. *Net neutrality* e *zero rating*

Infine, il tema dei rapporti telematici e della loro evoluzione necessariamente richiama due ultime questioni. La prima attiene alla neutralità della rete, la cosiddetta *net neutrality*[11], ed il suo rapporto con lo *zero rating*[12]. La seconda - nell'ambito delle informazioni commerciali ed editoriali - verte sui contenuti e sull'impatto dei contratti relazionali, nonché sul ruolo degli *influencers*. Ma procediamo con ordine. Che cos'è lo *zero rating*? Si tratta di un meccanismo o pratica commerciale dove l'operatore della rete mobile fornisce all'utente l'accesso ad *Internet* senza costi, garantendo l'accesso gratuito a determinati siti web (e sovvenzionando il servizio, ad esempio, mediante pubblicità). In sostanza, l'utente non è più soggetto al *cap*, o limite di traffico dati, solitamente compreso nel pacchetto sottoscritto con gli operatori. Lo *zero rating* è, ad esempio, particolarmente gradito all'utente quando include accesso gratuito a quelle piattaforme (Facebook, Spotify, Twitter ecc)

[11] BELLI, *La neutralità della Rete tra diritti fondamentali, Internet generativa e minitelizzazione*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 161; D'ACUNTO, *Net (or not) neutrality?,* in *Foro nap.*, 22, 2017; MARSDEN, *Net Neutrality: Towards a Co-regulatory Solution*, Londra, 2010; BELLI e DE FILIPPI, *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*, New York, 2016.

[12] DONATI, *Net Neutrality E Zero Rating Nel Nuovo Assetto Delle Comunicazioni Elettroniche*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 185. V. anche SLUIJS, *Network Neutrality and Internal Market Fragmentation*, in *CMLR*, 2012, pp. 1647-1674.

che in genere determinano un rapido consumo del traffico dati previsto dal pacchetto acquisito.

Sebbene vi sia un apparente beneficio per il consumatore, si dovrebbe tuttavia riflettere su come riconciliare questa pratica commerciale con gli obiettivi della *net neutrality*, ossia quel principio secondo cui gli operatori devono gestire il traffico senza discriminazioni che danneggino concorrenza, innovazione, diritti degli utenti e delle aziende web. Invero, in un sistema di *zero rating*, sembra che la neutralità della rete non possa più essere garantita, alla luce dell'evidente trattamento discriminatorio (in termini di tariffe applicate) di determinate piattaforme e siti web.

Negli Stati Uniti, la tematica ha di recente acquisito maggiore centralità, a seguito della messa in discussione dell'*Open Internet Order*[13], che consentiva al regolatore (la *Federal Communications Commission*) di intervenire per garantire il rispetto della neutralità della rete. Nel caso di *zero rating*, ad esempio, l'approccio statunitense era quello di valutare caso per caso se fosse individuabile un comportamento anticompetitivo che penalizzasse concorrenti o favorisse determinati servizi a discapito di altri. Il nuovo orientamento che vuole l'abolizione della *net neutrality* ha già fatto insorgere diverse imprese ed associazioni, che hanno posto in evidenza i rischi che una tale scelta determinerebbe in termini di pregiudizio ai diritti di utenti ed aziende; diritti, è bene rievocare, che si trovano all'interno di rapporti telematici.

[13] Federal Communications Commission, Provvedimento del 26 Febbraio 2015, Docket n. 14-28 (*Open Internet Order*). L'atto si è ispirato ai principi del i) *no blocking* (divieto di bloccare dispositivi, contenuti e servizi legali); ii) *no throttling* (divieto di alterare o degradare il traffico internet); iii) *no paid prioritization* (divieto per gli operatori di rete di favorire parte del traffico internet e di dare priorità a servizi a pagamento). E' previsto inoltre il divieto per i fornitori di rete broadband di interferire con il libero accesso ad internet degli utenti.

7. Contratti relazionali

È poi opportuno soffermarsi sui cosiddetti contratti relazionali, contratti di lunga durata dove, in sostanza, vi sono clausole generali piuttosto evanescenti e dove, in realtà, si instaura un rapporto fiduciario tra due soggetti nel portare avanti i loro obiettivi, ad esempio in ambito commerciale o professionale. In tali tipologie di contratti, non è infrequente il verificarsi di fasi in cui il rapporto negoziale sembra essere squilibrato o non particolarmente conveniente per una delle parti. Nella rete, il ricorso a contratti relazionali sta dando luogo a un fenomeno alquanto drammatico, che mette in discussione le modalità con cui si fa informazione.

Il riferimento è all'utilizzo di 'derivati', ossia di *banner* che appaiono all'interno di un giornale e che forniscono l'impressione all'utente di essere articoli di corredo piuttosto che pubblicità redazionale, mancando spesso ogni avvertimento in tal senso. Il *banner*, va dunque ribadito, non è un articolo giornalistico, ma è una forma pubblicitaria e strategia di marketing; si rinvia, in sostanza, ad un altro sito che ha un carattere informativo collegato. In tale fattispecie, un ruolo centrale spetta al committente od all'azienda, dietro cui può celarsi una storia 'vendibile' di *expertise*, qualità umane e professionali, e che si fa promuovere – a fronte di un corrispettivo – dal giornale, all'interno del rapporto (e non mero contratto) telematico. In questo contesto, può risultare a volte arduo comprendere pienamente la natura di questo rapporto, l'aspetto patrimoniale ad esso connesso. Si potrebbe allora riflettere sul significato stesso del concetto di patrimonio all'interno della rete e dei rapporti telematici.

8. Il nuovo ruolo dell'*influencer*

Da ultimo, rimanendo nell'ambito dell'evoluzione dell'informazione commerciale, non può omettersi un riferimento alla figura dell'*influencer*, cioè di colui – il *testimonial* – che condivide alcune

campagne pubblicitarie evidenziando e risaltando le qualità di alcuni prodotti[14]. Nella prassi, l'*influencer marketing* consiste nella diffusione su blog o social network di foto commenti o video da parte di personaggi di riferimento del mondo online con un elevato numero di *followers*, che mostrano approvazione per determinati *brand*. Tutto questo genera un effetto pubblicitario, sebbene venga omessa ai consumatori la specifica finalità pubblicitaria della comunicazione[15]. Il fenomeno, dunque, prescinde dall'esistenza di un contratto di sponsorizzazione *ad hoc*, di *merchandising*.

L'Autorità Garante della Concorrenza e del Mercato si è di recente occupata delle modalità con cui si svolge *l'influencer marketing*, ed ha inviato lettere di *moral suasion* ad alcuni dei principali *influencer* ed alle società titolari dei marchi visualizzati senza l'indicazione evidente della possibile natura promozionale della comunicazione. In tali lettere, l'AGCM ha sollecitato la massima trasparenza sul contenuto pubblicitario dei post pubblicati, al fine di limitare fenomeni di pubblicità occulta, come previsto dal Codice del Consumo[16].

Anche in suddetto contesto, a ben vedere, risulta complicato comprendere se il consumatore sia o meno legittimato ad avere una protezione secondo la legge del contratto o, viceversa, solo all'interno della responsabilità civile di stampo risarcitorio; posto, comunque, che il consumatore potrebbe ben ritenere non conveniente od economico adire il giudice ordinario.

---

[14] Della tematica se ne è occupato, tra gli altri, GAMBARO, *Concorrenza e pluralismo nel mercato di Internet: la prospettiva economica*, in *Diritti e Libertà in Internet,* a cura di Pollicino-Frosini-Apa-Bassini, Milano, 2017, p. 267. V. anche WEBSTER, *The Marketplace for Attention: How Audience Takes Shape in a Digital Age*, Boston, 2014; e ATHEY-CALVANO-GANS, *The impact of targeting on advertising market and media competition,* in *American Economic Review*, 100-2, 2010, pp. 608-613.

[15] Del concetto di *influencer*, si è anche recentemente occupata la Corte giust. UE. V. Conclusioni dell'Avvocato Generale, Caso C-498/16 *Maximilian Schrems c Facebook Ireland,* ECLI:EU:C:2017:863, par. 49.

[16] V. D. Lgs. 6 settembre 2005, n. 206 (Codice del Consumo).

9. Conclusioni

In sintesi, da questo breve saggio, emerge in modo netto la necessità di valutare attentamente il rapporto tra la rete, l'individuo e i suoi diritti o libertà. A supporto di siffatta conclusione, basti pensare, solo per citare alcuni esempi, ai pericoli per la dignità umana derivanti dall'utilizzo di videogiochi basati su realtà aumentata; alla necessità di porre un limite ad un utilizzo delle tecnologie che invada oltremisura la sfera privata di un individuo; alle diverse difficoltà che possono sorgere dall'utilizzo di algoritmi nella definizione di rapporti telematici; alle conseguenze del trattamento di piattaforme e siti web in maniera discriminatoria; ed alla rivoluzione che la tecnologia ha portato nelle modalità di fare pubblicità, dal ruolo dei *banner* alla figura *dell'influencer*, con i rischi e pericoli che ne derivano per la posizione degli utenti.

Ebbene, le citate direttrici testimoniano l'emergere di evidenti problematiche nell'evoluzione del rapporto telematico, che difficilmente potranno essere risolte a livello giurisprudenziale tramite la mera applicazione di principi generali ed in mancanza di competenze tecniche specifiche e settoriali.

Ma forse tali ostacoli non sono poi così insormontabili. Per superarli, si potrebbe elevare la norma tecnica a norma giuridica, segnalando la strada dell'interprete ed evidenziando al tempo stesso l'esistenza di aporie. A questo si aggiunga l'opportunità, o piuttosto esigenza, di favorire un dialogo sui delicati temi inerenti il rapporto tra il diritto ed Internet quale spazio di libertà ma anche fonte di minaccia per il diritto stesso; un confronto, in particolare, tra la dottrina ed i futuri interpreti del diritto - gli studenti o i giovani ricercatori, nel contesto della formazione universitaria.

Ermanno Calzolaio
Università degli Studi di Macerata

Il Regolamento europeo sulla protezione dei dati personali: spunti introduttivi e profili problematici

Sommario: 1. Premessa – 2. La nozione di dato personale – 3. Dalla tutela riparatoria alla tutela preventiva – 4. L'ambito di applicazione territoriale – 5. Le effettive prospettive di armonizzazione della materia

1. Premessa

Il presente contributo intende raccogliere alcune brevi considerazioni sul nuovo Regolamento europeo sulla protezione dei dati personali, aventi carattere di semplice introduzione agli ampi saggi di seguito pubblicati, allo scopo di porre in luce l'interesse della nuova disciplina e di fornirne una iniziale chiave di lettura.

Entrato in vigore il 24 maggio 2016 e destinato a trovare applicazione diretta in tutti gli Stati membri dal 25 maggio 2018, il Regolamento UE 2016/679 interviene in materia di "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati", abrogando espressamente (art. 94) la direttiva n. 95/46/CE, che era stata emanata allo scopo di rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle liberà delle persone riguardo al trattamento dei dati personali, attraverso il ravvicinamento delle legislazioni nazionali[1].

[1] CGUE, 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito, Federación de Comercio Electrónico y Marketing Directo c. Administración del Estado*, cause riunite C-468/10 e 469/10, in specie par. 28.

Il modello alla base della direttiva si è prestato ad essere definito come facente perno sul binomio "circolazione e (vs) protezione" dei dati[2]. Infatti, il legislatore europeo del '95 muoveva dalla considerazione della inevitabilità del fenomeno della circolazione dei dati personali, identificando però una serie di contrappesi volti a tutelare la persona rispetto ad un loro uso distorto. A tal fine, il principio-guida della direttiva è che il trattamento dei dati personali può essere effettuato solo quando la persona interessata ha manifestato il proprio consenso in maniera inequivocabile oppure quando il trattamento è necessario per dare esecuzione a un contratto concluso con l'interessato, o per adempiere un obbligo giuridico da parte del titolare del trattamento, o per salvaguardare un interesse essenziale della persona interessata, o per svolgere una funzione di pubblico interesse, o, infine, per perseguire l'interesse legittimo del titolare del trattamento (art. 7 dir. N. 95/46/CE)[3]. Il consenso deve essere preceduto da idonea informativa concernente finalità, modalità e limiti del trattamento dei dati personali.

Il sistema di tutela previsto dalla direttiva 95/46/CE emerge da una serie di disposizioni che obbligano gli Stati membri a garantire ad ogni persona interessata il diritto di ottenere dal titolare del trattamento la conferma dell'esistenza o meno di trattamenti di dati che la riguardano e delle informazioni sulla loro origine, nonché il diritto di rettifica o cancellazione degli stessi, ove il loro trattamento non è conforme alle disposizione della direttiva, il diritto ad opporsi a decisioni individuali automatizzate, ad usi per finalità di *marketing*. In caso di violazione del diritto alla protezione dei dati a carattere personale, la direttiva impone agli Stati membri di apprestare mezzi di ricorso e sanzioni appropriate ed efficaci (artt. 22-24). Mette conto rammentare che la protezione dei

[2] Così S. Sica, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. Sica-V. D'Antonio-G. M. Riccio, *La nuova disciplina europea della privacy*, Padova, 2016, pp. 1 ss.

[3] Cfr. M. Fumagalli Meraviglia, *Le nuove normative europee sulla protezione dei dati personali*, in *Dir. Com. Sc. Int.*, 2016, pp. 1 ss.

dati di carattere personale trova un ulteriore e importante fondamento normativo nella Carta dei diritti fondamentali, in specie all'art. 8, ove appunto si sancisce che: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Il nuovo Regolamento, pur confermando l'impostazione seguita dalla direttiva e perseguendo l'obiettivo di una piena tutela dei dati personali, introduce alcune significative novità, anche tenendo conto del contributo offerto dalla Corte di giustizia rispetto ad alcune criticità emerse nel corso degli anni. Ne emerge un testo normativo particolarmente complesso e articolato, su cui sarebbe impossibile soffermarsi in questa sede anche solo per offrirne una descrizione sintetica. Si concentrerà dunque l'attenzione su tre profili che appaiono particolarmente significativi, per poi svolgere, in conclusione, alcune considerazioni sulla scelta del legislatore europeo di intervenire con un Regolamento e sulle prospettive di una effettiva armonizzazione dei diritti degli Stati membri in questa materia.

2. La nozione di dato personale

Un primo profilo attiene alla nozione di dato personale. Per l'art. 2 della direttiva è dato personale "qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".

L'art. 4 del Regolamento definisce ora il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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".

Con questa nuova definizione, come è stato evidenziato, l'idea di protezione del dato personale risulta essere piuttosto generica, ma tale da ricomprendere tutti i dati, anche quelli pseudonimi, che possano condurre all'identificazione di una persona fisica a seguito di combinazioni con altre informazioni[4].

3. Dalla tutela riparatoria alla tutela preventiva

Un secondo profilo attiene alla natura del sistema di tutele. Nello spirito della direttiva le tutele avevano essenzialmente carattere riparatorio. Il regolamento, invece, accoglie ora una impostazione fondata su una tutela preventiva. Il legislatore sembra così prendere atto che la "logica del consenso" si rivela insufficiente a fronte dell'evoluzione incessante del settore tecnologico, che consente un'invasione sempre più accentuata nella sfera privata delle persone. Basti pensare all'analisi ed elaborazione di dati relativi a utenti o clienti al fine di suddividere l'utenza in gruppi omogenei di comportamento (c.d. profilazione), all'insieme di metodologie che consentono l'estrazione e l'utilizzo di una conoscenza a partire da grandi quantità di dati attraverso metodi automatici o semi-automatici (c.d. *data mining*), alla sorveglianza delle attività di una persona attraverso l'uso di dati quali gli acquisti con car-

[4] S. Sica, *Verso l'unificazione ecc.*, cit., p. 5.

ta di credito, le chiamate telefoniche ecc. (c.d. *data veillance*)[5].

Del resto, è proprio su questi aspetti che la giurisprudenza della Corte di giustizia, nel vigore della direttiva 95/46 CE, ha fornito un contributo decisivo nell'ottica di una attuazione effettiva della protezione dei dati personali, in particolare affermando la prevalenza dei diritti della personalità rispetto agli interessi economici degli operatori[6].

Il Regolamento ricorre quindi a strumenti della valutazione di impatto sulla protezione dei dati personali e della protezione fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*)[7], muovendosi nella direzione di implementare meccanismi che consentano di anticipare la tutela ad un momento anteriore al trattamento dei dati personali, che fa leva su una serie di obblighi a carico dei titolari in sede di progettazione dei prodotti e dei servizi. L'obbligo di effettuare la valutazione di impatto grava sul titolare in via generale ogni qual volta il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35 Reg.).

In quest'ottica, assume particolare rilievo la novità costituita dalla creazione della figura del responsabile della protezione dei dati (artt. 37-39), destinata ad assumere un ruolo centrale nella disciplina per i compiti e le responsabilità, dai contorni per vero molto ampi, che gli sono affidati dal Regolamento.

4. L'ambito di applicazione territoriale

Un terzo profilo di interesse della nuova disciplina è costituito dal suo ambito di applicazione territoriale. L'art. 3 stabilisce la regola ge-

[5] M. G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa dir. priv.*, 2016, pp. 1249 ss.
[6] CGUE, 13 maggio 2014, *Google Spain SL/Google Inc, Agencia espanola de Proteccion de Datos*, *Mario Costeja Gonzales*, C-131/12.
[7] M. G. Stanzione, *Genesi ed ambito di applicazione*, in S. Sica-V. D'Antonio-G. M. Riccio, op. cit., p. 21.

nerale secondo cui le nuove regole trovano applicazione al trattamento di dati personali "effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione", ovvero al trattamento che venga effettuato da un titolare stabilito in un luogo soggetto al diritto di uno Stato membro in applicazione delle regole di diritto internazionale privato.

Già la giurisprudenza della Corte di giustizia aveva dato un contributo importante, in particolare con la sentenza *Schrems*, nella quale aveva affermato l'incompatibilità con la direttiva della presunzione di adeguatezza di tutela in favore degli operatori statunitensi che si fossero impegnati in modo esplicito al rispetto di regole generali (*Safe Harbour Privacy Principles*), poi recepite nella decisione della Commissione 2000/520, che potevano essere però derogati dalle organizzazioni statunitensi autocertificate che ricevevano dati personali dal territorio dell'Unione Europea laddove interferissero con esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia statunitensi. La Corte ha ritenuto inaccettabile la compressione dei diritti fondamentali dei soggetti interessati[8].

Con il Regolamento, si fa spazio una significativa evoluzione della nozione di stabilimento, secondo un approccio orientato ai destinatari del servizio, sicché le nuove norme possono trovare applicazione anche quando il titolare del trattamento non è stabilito nel territorio dell'Unione. I nuovi criteri in presenza dei quali si applica il Regolamento sono l'offerta di beni o la prestazione di servizi a persone interessate nell'Unione e il monitoraggio del comportamento di tali soggetti che avviene all'interno dell'Unione. A ciò si accompagna l'obbligo, previsto in capo al titolare o al responsabile del trattamento, di designare un rappresentante nell'Unione, con la funzione di interlocutore delle

[8] CGUE, 6 ottobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, C-362/14. In argomento cfr. *amplius* S. Sica-V. D'Antonio, *I Safe Habour Privacy Principles: genesi, contenuti, criticità*, in *Dir. inf.*, 2015, p. 803.

autorità di controllo e degli interessati sulle questioni relative al trattamento (art. 27 Reg.).

Per tal via, si giunge quindi ad una applicazione potenzialmente "universale" del Regolamento, in linea con il dichiarato obiettivo perseguito dal legislatore europeo "di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione" (considerando n. 10 del Regolamento)[9].

5. Le effettive prospettive di armonizzazione della materia

Così delineato un quadro sommario di alcuni tra i principali profili innovativi del Regolamento, appare utile svolgere, in conclusione, qualche considerazione su un aspetto di carattere più generale, relativo allo strumento che il legislatore europeo ha adottato per intervenire nella materia.

Invece di una nuova direttiva, si è fatto ricorso ad un regolamento, che, come è noto, è un atto avente "portata generale", "obbligatorio in tutti i suoi elementi" e "direttamente applicabile in ciascuno degli Stati membri", mentre la direttiva "vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi" (art. 288 TFUE).

La ragione di questa scelta sembra essere in qualche modo esplicitata in uno dei tanti (ben 173) considerando[10]: la direttiva 95/46/CE "non ha impedito la frammentazione dell'applicazione della protezione dei

[9] Cfr. ancora M. G. Stanzione, *Il regolamento europeo ecc.*, cit., p. 1252.

[10] Per un'ampia trattazione della prassi del legislatore europeo di ampliare, a volte in modo incontrollato, il numero e il contenuto dei "considerando" all'inizio di ogni testo normativo, nonché per una ricostruzione del loro valore a fini interpretativi, cfr. T. Klimas-J. Vaiciukaite, *The Law of Recitals in European Community Law*, in *Journal of Int. Comp. Law*, 2008, pp. 61 ss.

dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche" (considerando n. 9). Pertanto, le differenze che si riscontrano nelle discipline adottate dagli Stati membri in sede di attuazione della direttiva, possono "costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione" (ivi). Da ciò si intende che il legislatore europeo è voluto intervenire con una normativa unitaria, come tale idonea ad eliminare le divergenze di disciplina.

Senonché, basta leggere il considerando successivo per avvedersi che, in realtà, sono ampi gli spazi volutamente lasciati all'autonomia degli Stati membri, che godono di un "margine di manovra" per precisare le norme contenute nel Regolamento. Scorrendo il testo normativo vero e proprio, si incontrano in effetti numerose ipotesi in cui gli Stati possono introdurre discipline diverse: l'art. 8 consente agli Stati di fissare l'età del minore (che deve dare il consenso) in misura inferiore rispetto a quella di sedici anni prevista come regola generale (con il limite di tredici anni); l'art. 9 autorizza gli Stati membri a "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute"; l'art. 23 consente agli Stati membri di limitare per via legislativa la portata degli obblighi e dei diritti previsti dalla sezione seconda e che attengono la raccolta delle informazioni, la rettifica e la cancellazione, la portabilità dei dati, e via di seguito, ogni qual volta lo Stato intenda salvaguardare non solo la sicurezza nazionale, la difesa e la sicurezza pubblica, ma anche aspetti dai contorni molto più sfumati, quali la salvaguardia dell'indipendenza della magistratura, l'esecuzione delle azioni civili o, ancor più genericamente, la tutela dell'interessato o dei diritti e delle libertà altrui; l'art. 80 prevede che gli Stati membri possono prevedere che un organismo rappresentativo degli interessati sia autorizza-

to a proporre reclami all'autorità di controllo anche senza specifico mandato; l'art. 84 demanda agli Stati membri l'emanazione di norme volte a stabilire ulteriori sanzioni (che possono quindi divergere da Stato a Stato); l'art. 85 prevede che sia assicurata da ciascuno Stato membro l'armonizzazione tra le norme e i principi del Regolamento e "il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria"; l'art. 87 consente agli Stati membri di "precisare ulteriormente le condizioni specifiche per il trattamento di un numero di identificazione nazionale o di qualsiasi altro mezzo d'identificazione d'uso generale"; l'art. 88 consente l'adozione di norme più specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro "in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro"; l'art. 90 consente di estendere la portata degli obblighi di segretezza.

Questa pur rapida ed incompleta rassegna mostra con chiarezza quanto, in realtà, l'obiettivo di unificazione che si è inteso perseguire attraverso l'adozione di un Regolamento è destinato a scontarsi con una varietà di discipline negli Stati membri rispetto a profili centrali della materia. Il Regolamento, per vero, prevede degli strumenti al fine di implementare la cooperazione a livello istituzionale fra le Autorità di controllo nazionali (artt. 55 ss.). In proposito, assume rilievo il "meccanismo di coerenza" (art. 63) ed il ruolo assegnato al Comitato europeo per la protezione dei dati (artt. 68 ss.). Tuttavia, ciò non esclude che ci si potrà trovare in presenza di un conflitto fra gli indirizzi del Comitato e la normativa adottata dagli Stati sulla base dei "margini di manovra"

rimessi dal Regolamento alla loro autonomia normativa, in precedenza sommariamente descritti.

Si tratta di una nuova frontiera del processo di armonizzazione normativa ed interpretativa del diritto europeo della protezione e sicurezza dei dati personali, nella prospettiva dell'unità politica, economica e giuridica del *digital single market* europeo.

Il passaggio tra un'unificazione a livello legislativo e una reale armonizzazione potrà realizzarsi solo attraverso il contributo attivo e fattivo a livello legislativo, giurisprudenziale e applicativo, senza il quale è agevole prevedere il permanere, e forse il moltiplicarsi, di diversi livelli di tutela del cittadino europeo ai fini della protezione dei suoi dati personali[11].

[11] Sul significato e sulla rilevanza della cittadinanza europea, quale paradigma concettuale idoneo a sviluppare una nozione autentica di diritto europeo comune, cfr. gli ampi contributi di L. Moccia, *Dalla comparazione alla integrazione giuridica: la via della cittadinanza europea*, in *La cittadinanza europea*, 2015, pp. 5 ss.; nonché *Comparazione giuridica, diritto e giurista europeo: un punto di vista globale*, in *Riv. Trim. Dir. Proc. Civ.*, 2011, pp. 767 ss., ora raccolti, insieme ad altri saggi, in L. Moccia, *Comparazione giuridica e prospettive di studio del diritto*, Padova, 2016, cui si rinvia anche per ulteriori riferimenti.

Simone Calzolaio
Università degli Studi di Macerata

Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. UE 2016/679

Abstract: Il Reg. UE 2016/679 aggiorna le regole europee in materia di protezione dei dati personali all'avvento della società digitale, introducendo un modello di protezione dei dati personali fondato sulla rischiosità del trattamento, sulla responsabilità del Titolare del trattamento e sulla protezione dei dati sin dal momento della progettazione del trattamento e per impostazione predefinita. Il contributo intende analizzare gli istituti ed i principi che caratterizzano questa riforma.

The GDPR 2016/679 updates the European data protection rules after the advent of digital society by introducing a data protection model founded on the risk-based approach, the controller's accountability and privacy by design and privacy by default. The paper investigates these main novelties introduced by GDPR.

1. Obiettivo del contributo

Obiettivo di questo contributo è delineare le principali novità introdotte dal Reg. UE 2016/679 sotto il profilo dei principi e delle dinamiche del trattamento dei dati personali[1].

È stato osservato che il nuovo Regolamento europeo non abbandona l'approccio essenzialmente riparatorio della Dir. 95/46/CE, ma tenta di completarlo affiancandovi una tutela preventiva fondata sulla strutturale e dinamica responsabilizzazione della filiera soggettiva coinvolta nel trattamento dei dati personali[2]. Accentuando questa impostazione, si discute di un vero e proprio rovesciamento di prospettiva tra Direttiva e Regolamento, la prima incentrata prevalentemente sui diritti dell'interessato, il secondo invece basato sui doveri del Titolare e del Responsabile del trattamento[3].

L'analisi che segue intende focalizzare questo approccio, concentrandosi proprio sulle parti del testo del Regolamento europeo che introducono nozioni e principi che innovano la "gestione" del trattamento dei dati personali[4].

In primo luogo, si osserveranno le ragioni che – muovendo dai considerando del Regolamento europeo – hanno indotto ad approvare il nuovo Reg. in luogo della precedente Direttiva. Quindi, si procederà a descrivere alcune delle principali novità "lessicali" introdotte dal Reg., tentando di inquadrarle nell'ambito delle problematiche che provano ad affrontare. In terzo luogo, si fornirà una descrizione dei nuovi principi

[1] Per una disamina dell'evoluzione della protezione dei dati personali nell'ordinamento italiano ed europeo cfr. L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale scientifica, Napoli, 2016.

[2] M. G. Stanzione, *Genesi e ambito di applicazione*, in Sica - D'Antonio - Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, p. 21.

[3] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, pp. 153 ss.

[4] Per una introduzione generale al Reg. europeo in parola cfr. G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss.

cardine della protezione dei dati personali (*privacy by design* e *by default*). Infine, si cercherà di legare questi principi alla disciplina della valutazione di impatto e alla figura del *Data protection officer*.

In questo modo si intende fornire al lettore un quadro sintetico del modello attraverso il quale il legislatore europeo intende garantire i diritti (vecchi e nuovi)[5] afferenti alla protezione ed alla sicurezza dei dati personali e, contemporaneamente, gli interessi del vecchio continente nel panorama globale.

2. Le ragioni alla base del Reg. UE 2016/679

La lettura dei considerando del Regolamento lascia intravedere, con una certa chiarezza, gli obiettivi e le finalità principali che sono alla base del faticoso processo di elaborazione, durato circa un lustro[6].

Appare evidente che il fine del Regolamento è garantire il diritto fondamentale sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e ribadito dall'art. 16 TFUE, concernente la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale[7].

In questa prospettiva, l'esigenza primaria che ha suggerito l'adozione di un nuovo set di regole europee è strettamente legata alla

[5] Per una panoramica sui diritti tutelati dal Reg. cfr. i contributi di G. Di Genio, *Trasparenza e accesso ai dati personali*; P. Pacileo, *Profilazione e diritto di opposizione*; V. D'Antonio, *Oblio e cancellazione dei dati nel diritto europeo*; P. Pacileo, *Il diritto alla protabilità*, tutti in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, rispettivamente pp. 161 ss., pp. 177 ss., pp. 197 ss., pp. 221 ss.

[6] Cfr. S. Gutwirth-R. Leenes-P. de Hert (edited by), *Reforming European Data Protection Law*, *Law, Governance and Technology Series*, vol. 20, Springer 2015. Per i lavori preparatori del Reg. in parola, cfr. http://eur-lex.europa.eu/procedure/IT/2012_11.

[7] Cfr. F. Donati, *Art. 8. Protezione dei dati di carattere personale*, in R. Bifulco-M. Cartabia-A. Celotto, *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001, pp. 83 ss.

digitalizzazione della società e dell'economia europea (e globale). L'ambiente digitale è costituito dalla produzione, condivisione, elaborazione di un flusso incessante di dati: «*la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività*» e, contemporaneamente, «*sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano*» (cons. 6).

La circolazione di questa massa crescente di dati è un valore da custodire e promuovere, sia all'interno dell'Unione europea, sia nei rapporti con i «paesi terzi» e con le organizzazioni internazionali, ed appare tuttavia necessitare di nuove ed apposite regole europee volte alla garanzia di un elevato livello di protezione dei dati personali.

Attraverso la primaria esigenza di garantire il diritto individuale alla protezione dei dati personali segnatamente in ambiente digitale, le nuove regole europee perseguono altresì il fine di instaurare quel «*clima di fiducia*» e di certezza giuridica – fondato sulla consapevolezza delle persone fisiche di avere il controllo sui propri dati personali – necessario per lo «*sviluppo dell'economia digitale in tutto il mercato interno*» (cons. 7).

Società digitale, certezza giuridica, mercato unico[8]. Il perseguimento di questi obiettivi prioritari si lega strettamente con l'altra grande finalità (in qualche modo, strumentale ed operativa) del Reg. europeo: il superamento della frammentazione giuridica delle norme e delle prassi applicative in tema di protezione dei dati personali sul suolo

[8] Osserva puntualmente G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss. e spec. par. 3, che «in questo quadro, non si può non considerare il reg. 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". I due regolamenti, considerati in una prospettiva unitaria, indicano chiaramente l'intento del legislatore europeo di disegnare un mercato unico digitale, rimuovendo gli ostacoli giuridici costituiti dalla disomogeneità delle norme applicabili».

dell'Unione europea[9].

Si osserva infatti che «*sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche*». La coesistenza di diversi livelli di protezione a livello nazionale rappresenta un ostacolo alla libera circolazione dei dati personali all'interno dell'Unione, un freno all'esercizio delle attività economiche su scala dell'Unione, è in grado di falsare la concorrenza e di impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Si afferma con chiarezza che «*tale divario creatosi* (…) *è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE*» (cons. 9).

La conseguenza di tale osservazione è duplice e decisamente rilevante.

Non sarebbe stato sufficiente procedere ad un aggiornamento, magari radicale, delle regole europee in materia di protezione dei dati personali con una nuova direttiva. Si è reso necessario utilizzare una "nuova" fonte, il regolamento europeo, che è stato ritenuto l'unico strumento in grado di garantire «*un livello coerente di protezione delle persone fisiche*», certezza del diritto e trasparenza agli operatori economici e di «*prevenire disparità*» a livello nazionale (cons. 13), anche sotto il profilo sanzionatorio.

È opportuno almeno accennare al fatto che è stato il cammino della competenza europea in materia di protezione dei dati personali, culmi-

[9] Cfr. D. Erdos, *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps*, in *Legal Studies Research, Paper Series*, University of Cambridge, paper n. 30/2015, (attualmente in *Journal of Law and Society*, Dicembre 2016, pp. 534-564) il quale evidenzia la sussistenza di un divario rilevante all'interno dei singoli Stati nazionali europei nella protezione dei dati con specifico riferimento all'utilizzo delle nuove tecnologie.

nato con l'adozione dell'art. 16 del TFUE, che ha reso possibile l'adozione di un regolamento europeo in materia[10]: si tratta di un (raro, come noto, ma) evidente attestato di vitalità delle istituzioni europee, che hanno saputo decifrare il sorgere di un interesse strategico unitario europeo alla protezione dei dati personali e di disporre, conseguentemente, un peculiare titolo di competenza dell'Unione europea[11].

Pertanto, fra le ragioni che hanno condotto alla adozione delle nuove regole europee in materia di protezione dei dati personali delle persone fisiche va annoverata anche l'avvertita esigenza di sostituire la fonte regolamentare alla direttiva[12].

3. Rischio, profilazione, pseudonimizzazione. Il nuovo "dato personale"

Il Reg. contiene una disciplina molto articolata e una serie di definizioni ben più analitica rispetto alla precedente Dir. In questa sede, si vogliono trattare alcuni concetti e definizioni, che appaiono in grado di introdurre al nuovo modello di tutela europea.

Ci si vuole soffermare, pertanto, sui concetti di «*rischio*», «*profilazione*», «*pseudonimizzazione*».

---

[10] Cfr. sul tema H. Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Springer, 2016.

[11] Cfr. B. Cortese, *La protezione dei dati di carattere personale nell'Unione europea dopo il trattato di Lisbona*, in *Dir. Un. Eur*., n. 2 del 2013, pp. 313 ss.

[12] Deve comunque sottolinearsi che, da un lato, il Regolamento europeo appare la fonte del diritto più adeguata per far tesoro dell'ormai ampia elaborazione e dei ripetuti interventi della Corte di giustizia dell'Unione europea (cfr. in particolare, CGUE, 13 maggio 2014, causa C-131/12*, Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González*.; CGUE, 6 ottobre 2015, causa C-362/14, *Maximillian Schrems/Data Protection Commissioner*; CGUE, 8 aprile 2014, cause riunite n. C-293/12 e n. C-594/12) che avevano già interpretato in modo innovativo e perentorio il diritto dell'unione europea in materia di dati personali. D'altra parte, è opportuno segnalare che il Reg. UE 2016/679, lascia ampi margini di attuazione a livello statale (cfr., ad es., cons. 8, 10, e artt. 8, 9, 23, 80, 85, 87, 88, 90), seppure nell'ambito di stringenti meccanismi di cooperazione e coerenza (capo VII, artt. 60 ss.) volti ad uniformarne l'applicazione a livello europeo.

Si è detto che il Reg. viene adottato per aggiornare la disciplina della precedente Dir. all'avvento della società digitale. A livello scientifico, appare ormai scontato osservare che tra protezione dei dati personali e nuove tecnologie corra un difficile rapporto di compatibilità[13], in forza del quale sembra quasi ineluttabile che all'evolversi della società digitale debba corrispondere la progressiva estinzione delle istanze legate alla tutela della privacy, o in altre parole *the end of privacy*[14]. Questa osservazione sorge dalla analisi della realtà digitale: attualmente è possibile trarre informazioni strettamente personali su una o più persone fisiche semplicemente incrociando dati (né personali, né sensibili, sulla base della vigente normativa europea e italiana)[15] e, poi, altri dati personali. Ciò è agevolato dal fenomeno dei c.d. «*Big data*»[16]: una mole infinita di dati, che viene prodotta ogni giorno dalla vita digitale di persone, imprese, amministrazioni, cose[17], ed ogni giorno trattata e conservata (apparentemente) in quei non-luoghi chiamati *cloud*[18]. Un contesto c.d. *data intensive* in continua evoluzione. Questi dati, se corret-

[13] La dottrina su questo aspetto è ormai sterminata. Cfr., di recente, P. 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, n. 3/2016, http://www.giurcost.org/studi/passaglia7.pdf.

[14] ... così si intitolava un numero speciale della rivista *Science* (vol. n. 347 del 30 gennaio 2015, in http://science.sciencemag.org/content/347/6221/490). Cfr. A. Sarat (a cura di), *A World without Privacy. What Law Can and Should Do?*, Cambridge University Press, 2015.

[15] Cfr. A. Mantelero, *Data Protection, e-Ticketing, and Intelligent Systems for Public Transport*, in *International Data Privacy Law*, 2015, pp. 309 ss.

[16] Per introdursi alla complessità del fenomeno cfr. G. D'Acquisto - M. Naldi, *Big data e privacy by design*, Giappichelli, 2017.

[17] Cfr. U. Pagallo-M. Durante-S. Monteleone, *What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT*, in R. Leenes-R. Van Brakel-S. Gutwirth-P. DeHert (a cura di), *Data Protection and Privacy: (In)visibilities and Infrastructures*, *Law, Governance and Technology Series,* vol. 36, Springer, 2017, pp. 59 ss.

[18] Cfr. M. M. Winkler-J. Mosca, *Cloud computing e protezione dei dati personali*, in M. Fumagalli Meraviglia (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Editoriale Scientifica, Napoli, 2015, pp. 121 ss.

tamente interrogati, sono una fonte di conoscenza smisurata, e di una utilità ed un valore inedito nella storia dell'uomo: ne è nato un nuovo e fiorente settore di ricerca ed industriale, la «*big data analytics*». Quel che interessa in questa sede puntualizzare è che attualmente per trarre informazioni analitiche su singole persone non è più necessario trattare dati personali o sensibili. È sufficiente essere in grado di interrogare correttamente i *big data* e incrociare (*data inference* e *re-identification*) dati non personali per ottenere informazioni personali analitiche, costanti, complete, intime, riservate[19].

Le conseguenze sul piano giuridico sono molteplici[20] e ancora non del tutto intelligibili[21].

Proprio per questo, su un punto si può osservare una certa chiarezza: una volta che un dato (e, quindi, anche un dato personale) è inserito nel circuito digitale, non si può evitare che circoli, che possa essere utilizzato e riutilizzato, comunicato e diffuso, incrociato con altri dati anche di natura completamente diversa, per finalità imprevedibili rispetto alla ragione per cui il dato era stato originariamente prodotto, richiesto, trattato[22].

---

[19] Per una spiegazione del fenomeno dei Big data e della possibilità tecnica – molto contestata nel dibattito internazionale – di farlo convivere con gli strumenti a tutela della protezione dei dati cfr. G. D'Acquisto-J. Domingo-Ferrer-P. Kikiras-V. Torra-Y. A. de Montjoye-A. Bourka, *Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data analytics*, European Union Agency for network and information security, december 2015, in http://www.enisa.europa.eu.

[20] Cfr. F. Di Porto (a cura di), *Big data e concorrenza*, in *Concorrenza e mercato*, numero speciale 23/16, e, in tale volume, in particolare, V. Zeno-Zencovich - G. Giannone Codiglione, *Ten Legal Perspectives on the "Big Data Revolution"*, pp. 29 ss.; per una prima indagine sul rapporto e sui risvolti fra digitalizzazione pubblica e «Big Data» sia consentito rinviare a S. Calzolaio, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, n. 31/2016, pp. 185 ss.

[21] Cfr. A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss.

[22] Cfr. D. Klitou, *Privacy-Invading Tecnologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, *Information Technology and Law Series,* vol. 25, Asser press – Springer, 2014.

In termini sintetici, la produzione di un dato in ambiente digitale coincide di norma con l'accettazione di un rischio da parte del soggetto interessato, un rischio che abbraccia il trattamento nel cui ambito quel dato è richiesto e tutti i potenziali trattamenti c.d. secondari.

L'insieme delle disposizioni del Reg. europeo appare trovare le sue fondamenta concettuali su questa osservazione del rischio e della rischiosità della circolazione in rete di dati (e di dati personali), a partire dalla quale si può comprendere quel cambiamento di impostazione rispetto alla dir. ed, almeno in parte, alla normativa vigente in Italia[23]: è vero che il Reg. si concentra prevalentemente nell'imporre obblighi al Titolare ed al Responsabile del trattamento e con questo, in parte, muta o almeno allarga la strategia normativa della precedente Dir., che faceva di alcuni obblighi – in particolare del modello informativa-consenso – un precipitato della disciplina dei diritti dell'interessato; ma ciò avviene nell'ambito di un ardito tentativo di fornire una protezione effettiva dell'interessato, di fronte a "rischi certi" per la protezione dei dati personali in ambiente digitale.

Non a caso, il termine "rischio" (o "rischi") ricorre appena 8 volte nella Dir. e oltre 100 nel Reg., quasi a segnare il passaggio ad una prospettiva improntata al principio di precauzione nella protezione dei dati personali[24].

Ne consegue che, come è stato osservato, elemento caratteristico del Reg. consiste nella strutturale necessità di una valutazione sistematica da parte del Titolare/Responsabile del trattamento dei rischi attuali e

[23] Come osserva A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss., «è il profilo inerente la responsabilità degli autori del trattamento, in quanto collegata alla gestione del rischio, a rappresentare il nucleo centrale del nuovo quadro di tutela dei dati personali definito dall'Unione europea. In questa prospettiva, istituti centrali sono la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva».

[24] Cfr. M.G. Stanzione, *Genesi ed ambito di applicazione*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, pp. 21 ss.; sul principio di precauzione cfr. F. De Leonardis, *Il principio di precauzione nell'amministrazione di rischio*, Giuffré, Milano, 2005.

potenziali del trattamento, sia in riferimento alla protezione dei diritti dell'interessato sia in riferimento specifico alla sicurezza dei dati. La ponderazione della rischiosità si lega strettamente con i profili inerenti la responsabilità giuridica per il trattamento e con l'operatività di altri istituti introdotti dal Reg., come la valutazione di impatto[25].

A questo riguardo, il Reg. cerca anche di qualificare il livello del rischio, distinguendo fra rischio generico e rischio elevato. Nelle pieghe del Reg. sembra anche osservarsi l'ipotesi di un rischio basso per i diritti dell'interessato [cons. 80, art. 27, c. 2, lett. *a)*].

Il parametro di valutazione del rischio prende in considerazione la probabilità e gravità di una violazione dei diritti e delle libertà degli interessati a causa o nell'ambito del trattamento[26] e non è rimesso alla mera sensibilità del Titolare del trattamento, ma trova una oggettivazione (dinamica) nella conformità della valutazione ai codici di condotta approvati e/o alle certificazioni approvate e/o linee guida fornite dal comitato europeo per la protezione dei dati e/o indicazioni fornite da un responsabile della protezione dei dati[27].

In particolare, sembrerebbe potersi ritenere che vi sia una sorta di presunzione di elevata rischiosità per i trattamenti che comportano l'utilizzo di nuove tecnologie (cfr. cons. n. 89 e art. 35, c. 1, i quali per-

[25] Cfr. G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, pp. 55 ss.

[26] Il cons. 76 afferma che la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Il cons. 77 afferma che per dimostrare la conformità da parte del titolare del trattamento/responsabile del trattamento è necessario attenersi ai codici di condotta approvati e/o alle certificazioni approvate e/o linee guida fornite dal comitato e/o indicazioni fornite da un responsabile della protezione dei dati.

[27] Il cons. 83 specifica che per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare/responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura.

tanto normalmente dovrebbero essere sottoposti a valutazione di impatto sulla protezione dei dati). Allo stesso modo, almeno per quanto concerne i trattamenti oggetto di valutazione preventiva, la rischiosità può variare nel corso del trattamento e spetta ancora una volta al Titolare procedere ad un riesame (quindi ad una rivalutazione) del rischio (art. 35, u.c.; più in generale, artt. 24, c. 1, e 25, c. 1).

Inoltre, viene specificamente preso in considerazione il rischio per la sicurezza del trattamento, in riferimento al quale viene individuata la "cifratura" quale tecnica idonea a limitare il rischio[28]. Sotto questo profilo, va sottolineato che le misure di garanzia di un adeguato livello di sicurezza del trattamento sono individuate «*tenuto conto dello stato*

[28] Il considerando n. 51 individua, in modo puntuale, i singoli aspetti che devono essere considerati nella valutazione del rischio: «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o dell'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; se sono trattati i dati genetici o biometrici per identificare in modo univoco una persona o se sono trattati i dati relativi alla salute o i dati relativi alla vita sessuale e all'orientamento sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi e la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori o se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*».

Il cons. n. 52 specifica che «*La probabilità e la gravità del rischio dovrebbero essere determinate con riferimento alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se il trattamento di dati comporta un rischio elevato. Un rischio elevato è un particolare rischio di pregiudizio dei diritti e delle libertà degli interessati*».

dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere»: si stabilisce pertanto un nesso di proporzionalità fra rischi del trattamento, evoluzione tecnologica e costi di attuazione.

Le molteplici sfumature in cui si dipana il problema del rischio ne fanno, attualmente, un oggetto di indagine ancora allo stato magmatico, sotto il profilo della sua piena operatività[29].

Tuttavia, il Reg. traccia una linea che consente, in sede interpretativa, di introdursi alla tipologia di trattamento che appare integrare pienamente gli estremi di una rilevante e persistente rischiosità nella nuova disciplina europea.

Si tratta della ormai famosa «*profilazione*», ovvero di «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica*» (così l'art. 4, n. 4).

In linea generale, si può osservare che la profilazione è una nuova forma di conoscenza conseguente alla correlazione di dati contenuti in uno o più database volta alla definizione di un profilo di un individuo o di un gruppo. Attraverso la profilazione si conoscono aspetti, elementi, correlazioni del soggetto profilato che non sarebbe possibile trarre attraverso le modalità di analisi classiche. La profilazione pertanto non produce solo nuove o buone informazioni, ma genera un nuovo stadio di conoscenza, attraverso il quale è possibile osservare e prevedere analiticamente (cioè, profilare) comportamenti, attitudini, preferenze. La profilazione si rivela un mezzo funzionale alla assunzione di una decisione rilevante per l'individuo o per il gruppo profilato, proprio in quanto adeguato a valutare e *prevedere* analiticamente il comportamento presente e futuro del soggetto profilato[30].

[29] Ciò emerge anche dal contributo di A. Mantelero, *Il Consiglio d'Europa adotta le prime linee guida internazionali su Big Data e tutela dei dati personali*, in *questa Rivista*, 2017, e, più approfonditamente, ID., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss.

[30] Su questo tema è molto utile approfondire attraverso la ricerca di F. Bosco-N.

Come si può intuire, se si volesse individuare un fenomeno che plasticamente rappresenta l'endiadi fra società digitale e *big data* ci si può agevolmente riferire al rilievo assunto dalla attività di profilazione: non a caso, pertanto, il Reg. vi fa costantemente riferimento[31].

Specifica attenzione è riservata alla attività di profilazione quando è volta a «*analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*» (così, ancora, la definizione di cui all'art. 4, n. 4), in modo particolare quando si inserisce in un «*processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*». In merito, l'art. 22 afferma che, in via generale, «*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*». Correlativamente, si specifica che l'interessato, nei casi in cui i suoi dati personali sono sottoposti a trattamento automatizzato (compresa la profilazione), è titolare di un di un diritto di opposizione (art. 21, c. 1[32]) e di un "*right of explanation*" in merito alla logica utilizzata, nonché

Creemers-V. Ferraris-D. Guagnin-B.J. Koops, *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth-R. Leenes-P. de Hert (edited by), *Reforming European Data Protection Law*, Law, Governance and Technology Series, vol. 20, Springer, 2015, pp. 3 ss.

[31] Cfr., in particolare, cons. n. 24 (in merito al trattamento effettuato da Titolare/Responsabile non stabilito nell'UE, quando è riferito al monitoraggio del comportamento di un interessato); art. 47, c. 2, lett. *e)* (in merito alle norme vincolanti d'impresa stabilite dalla competente autorità di controllo); cons. nn. 60, 63, 70 e artt. 13, c. 2, lett. *f)*, 14, c. 2, lett. *g)*, 15, c. 1, lett. *h)*, 21, c. 1 e 2 (in merito ai diritti dell'interessato rispetto alla profilazione); cons. n. 71 e art. 22 (in merito al trattamento automatizzato); cons. 91 e art. 35 (in merito alla valutazione di impatto); cons. 72 e art. 70, c. 1, lett. *f)* (in merito ai poteri di orientamento del Comitato europeo per la protezione dei dati); cons. 73 e art.23 (in merito alle limitazioni).

[32] Cfr. quanto puntualmente esposto da P. Pacileo, *Profilazione e diritto di opposizione*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, rispettivamente pp. 194 ss.

all'importanza e alle conseguenze previste di tale trattamento[33]. Ciò significa che in qualche modo si intende riconoscere un diritto di conoscenza (e, quindi, di controllo) dell'interessato sulle «*procedure matematiche o statistiche*» utilizzate dal Titolare del trattamento «*per la profilazione*», le quali devono essere «*appropriate*» (cons. 71).

In termini sintetici, il legislatore europeo individua la profilazione ed il connesso trattamento automatizzato dei dati come un rischio specifico (e generalizzato) del trattamento dei dati personali, in base al quale l'(ignaro) interessato può trovarsi di fronte ad una decisione rilevante per la sua sfera giuridica (cfr. cons. n. 58) che è frutto di un trattamento di dati personali (e non personali) da parte di un sistema automatizzato governato da uno o più algoritmi, al fine di servire gli interessi "economico-sociali" che li ha prodotti[34], per ora, attraverso l'incidente atti-

[33] Cfr. artt. 13, 14, 15 del Reg., indicate nella nota precedente, e B. Goodman-S. Flaxman, *European Union regulations on algorithmic decision-making and a 'right to explanation'* (31 agosto 2016), in http://arxiv.org/abs/1606.08813; Wachter-B. Mittelstadt-L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation* (28 dicembre 2016), in *International Data Privacy Law*, forthcoming and now available at SSRN: https://ssrn.com/abstract=2903469.

[34] In tal senso, pur non potendo sviluppare in questa sede il tema, non appare casuale che la qualificazione più puntuale delle dinamiche della profilazione sia contenuta in un considerando che si occupa del trattamento ad opera di un titolare/responsabile non stabilito nell'Unione europea. Nel cons. 24 si afferma che «È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al *monitoraggio del comportamento* di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al *controllo del comportamento dell'interessato*, è opportuno verificare se le persone fisiche sono *tracciate* su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella *profilazione della persona fisica*, in particolare per *adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*» (nostri i corsivi). Per una introduzione al problema cfr. R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. Cost.*, n. 1/2016, pp. 289 ss.

vità di altri esseri umani[35].

Per affrontare in modo sistematico questi rischi e, comunque, per minimizzare l'impatto sulla sfera personale dei trattamenti, ivi compresi quelli automatizzati e secondari, il Reg. individua un rimedio generale, nella «pseudonimizzazione», cioè nel «*trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*» (art. 4, n. 5).

È interessante osservare che, secondo la definizione appena riportata, la pseudonimizzazione si qualifica come misura tecnica (un'operazione in forza della quale i dati personali non possono essere riferiti ad un interessato senza l'utilizzo di informazioni aggiuntive), ma anche come misura organizzativa: la misura tecnica è suscettibile di generare, ai sensi del Reg., una psuedonimizzazione dei dati personali solo se le informazioni necessarie per risalire agli originari dati personali sono conservate separatamente rispetto a questi e comunque se sono soggette ad ulteriori misure di garanzia dell'irriferibilità dei dati personali pseudonimi ad una persona fisica. Misure tecniche e modelli organizzativi improntati alla sicurezza (della infrastruttura del Titolare/Responsabile) devono muoversi in sincronia: quella che si delinea con la nozione di pseudonimizzazione appare una delle chiavi di volta della nuova disciplina europea, che sembra attuare l'osservazione secondo cui «l'unico modo efficace di affrontare il problema della sicurezza dell'informazione è quello che ne comporta una visione integrata: informatica, giuridica e organizzativa»[36].

Altro profilo notevole è che la pseudonimizzazione non sottrae i dati

[35] Cfr. Information commissioner's office, *Big data, artificial intelligence, machine learning and data protection*, Version 2.0 del 1.3.2017, in *https://ico.org.uk/*.
[36] Cfr. G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss.

trattati dalla sfera di applicazione del Reg., poiché essi non sono assimilabili ai dati anonimizzati e continuano ad essere considerati come «*informazioni su una persona fisica identificabile*» (cons. 26)[37]. Tuttavia si tratta di una misura fortemente incentivata[38], poiché considerata in grado di minimizzare il rischio per gli interessati coinvolti nel trattamento (cons. 28-29) e di aumentarne sensibilmente la sicurezza [art. 32, c. 1, lett. *a)*]. Inoltre, la pseudonimizzazione, insieme alla "cifratura", appare una garanzia di protezione ritenuta rilevante in sede di trattamenti c.d. secondari [art. 6, c. 4, lett. *e)*], laddove cioè il Titolare intenda svolgere un trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti[39].

L'interrelazione fra i concetti sin qui analizzati di rischio, profilazione e

[37] Cfr. È stato recentemente puntualizzato che «la tutela introdotta con la pseudonimizzazione è volta a garantire la confidenzialità del dato, non più immediatamente intelligibile, ma anche, come avviene nel caso dell'applicazione di tecniche crittografiche, a garantirne l'integrità contro manipolazioni anche accidentali. Nel caso dell'anonimizzazione la tutela è invece volta a impedire, a meno di dover ricorrere a mezzi irragionevolmente utilizzabili, la riferibilità del dato a una persona». Per questo, si afferma che i dati anonimizzati sono una misura di tutela della privacy, mentre i dati pseudonimi sono una misura di sicurezza, così G. D'Acquisto-M. Naldi, *Big data e privacy by design*, Giappichelli, 2017, p. 39; cfr. anche Gruppo di lavoro art. 29 per la protezione dei dati personali, *Parere 05/2014 sulle tecniche di anonimizzazione* (10 aprile 2014), in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf*, spec. pp. 21 ss. Tuttavia, anche la distinzione fra dati pseudonimizzati e dati anonimi (e poi fra dati anonimi e dati personali) si rivela di carattere giuridico-stipulativo, o comunque una distinzione fondata su una valutazione del livello del rischio di disvelazione di dati personali, poiché «*anonymized data can always become personal data again depending upon the evolution of the data environment*», cfr. S. Stalla-Bourdillon-A. Knight, *Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data* (6 Marzo 2017), in *Wisconsin International Law Journal*, 2017, disponibile presso *https://ssrn.com/abstract=2927945*.

[38] Cfr. oltre alle disposizioni citate di seguito nel testo, i cons. 75, 78, 85, 156 (quest'ultimo, insieme all'art. 89, c. 1, riferito al trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici) e gli artt. 25, c. 1; 40, c. 2, lett. *d)* (in riferimento alla elaborazione di codici di condotta).

[39] Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 253.

pseudonimizzazione appare in grado di giustificare la innovazione introdotta dal Reg. nella basilare definizione di «*dato personale*» (art. 4, n. 1), la quale, come è stato rilevato, si estende ormai «all'insieme di informazioni relative ad una persona fisica, avendo riguardo per gli identificativi prodotti da dispositivi on line (indirizzo IP, cookies, ecc.) o di quei dati che, nonostante la pseudonimizzazione, possono essere oggetto di combinazione con ulteriori informazioni in modo da rendere possibile, direttamente o indirettamente, l'identificazione dell'interessato»[40].

Si tratta, per l'appunto, della qualificazione del concetto di «*dato personale*» al tempo del "rischio digitale".

4. La nozione di *privacy by design* (e di *privacy by default*) nel Reg. europeo

Il Reg. fa una scelta di campo netta in merito al soggetto cui addebitare l'intera responsabilità (intesa nel duplice senso di responsabilità giuridica e di connesso vincolo alla cura "amministrativa" e organizzativa) della gestione della composita filiera del trattamento dei dati personali. Il protagonista ed anche il *pivot* della nuova architettura giuridica europea è il Titolare del trattamento.

Ai sensi dell'art. 24, spetta al Titolare tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. Ciò significa, in primo luogo, essere in grado di determinare e delineare puntualmente i caratteri del trattamento, aspetto che può dimostrarsi di difficile realizzazione pratica nella società digitale[41].

---

[40] Cfr. G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, cit. p. 64.

[41] Come osserva A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss., spec. par. 5, nel contesto dei Big Data «le finalità "specifiche" del trattamento dati possono essere assai difficilmente descritte al momento della raccolta delle informazioni, stante la natura mutevole dell'utilizzo dei dati posto in essere dai titolari del trattamento che im-

Sulla base di questa iniziale valutazione, spetta al Titolare procedere a ponderare i rischi del trattamento sia sul versante della *probabilità* del verificarsi dei medesimi, sia sul versante della *gravità* della lesione dei diritti e delle libertà delle persone fisiche in caso di realizzazione delle ipotesi di rischio contemplate[42].

In ragione di questi due livelli di valutazione, il titolare del trattamento decide quali misure tecniche e organizzative sono adeguate per garantire che il trattamento sia effettuato conformemente alle disposizioni del Reg. e le mette in atto.

Si deve precisare che queste tre distinte attività non si esauriscono nella fase prodromica al trattamento, ma si estendono per tutta la sua durata: il Titolare deve monitorare i caratteri del trattamento (natura, ambito, contesto, finalità) ed i rischi connessi (probabilità e gravità) per l'intera durata del trattamento e su tale base, se necessario, è tenuto a procedere al riesame ed all'aggiornamento delle misure adottate.

Il Titolare, infine, deve essere in grado di dimostrare – in sostanza –

---

piegano soluzioni di Big Data analytics».

[42] Il cons. 75 elenca una molteplicità di ipotesi rischiose: «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*».

lo svolgimento di tutte le attività appena descritte[43].

Sorge spontaneo il quesito sulle modalità concrete con cui il Titolare debba adempiere ad un così articolato schema normativo.

Su questo versante, si ritiene che il Reg. abbia adottato, allo stato, un indirizzo generico sul piano normativo, ma realistico sul versante applicativo.

In primo luogo, l'art. 24, c. 2, specifica che le misure tecniche ed organizzative «*includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento*», se ciò è proporzionato rispetto ai caratteri del trattamento. È forse opportuno segnalare che, in realtà, tutta l'attività di valutazione preventiva del trattamento, testé delineata, rappresenta già una politica di trattamento dei dati personali che prelude alla individuazione e messa in atto delle misure tecniche (e non viceversa). In questa prospettiva, quel che forse più rileva è il riferimento al principio di proporzionalità, col quale si vuole evidentemente sottolineare che non tutti i trattamenti presentano profili di rischiosità tali da necessitare di una particolare strategia (o politica) di prevenzione.

L'ultima parte dell'art. 24 indirizza il titolare verso una modalità di comprensione analitica di cosa effettivamente sia tenuto a fare, per rispettare i dettami normativi europei. Non si individuano direttamente condotte, ma si prelude ad un intenso lavorio di concreta specificazione di pratiche e modelli attuativi delle disposizioni regolamentari: «*l'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*».

Si potrebbe sintetizzare che c'è molta *privacy by design* – o, se si preferisce, protezione dei dati fin dalla progettazione – nel principio di *accountabilty*[44] delineato dall'art. 24: una volta posta in capo al Titolare

[43] Si ricorda che il cons. 81, cui si rinvia, specifica una articolata serie di doveri e cautele del Titolare nel caso in cui designi un Responsabile del trattamento.

[44] Sul rilievo e sul significato del principio di *accountability* cfr. G. Finocchiaro,

– ovviamente, peraltro – la responsabilità del trattamento, si delinea una procedura costante di valutazione dei caratteri e dei rischi del trattamento, che va svolta "agganciando" l'organizzazione e la struttura aziendale alle condotte ritenute idonee sulla base degli appositi codici o delle buone pratiche connesse con i meccanismi di certificazione. All'esito di questa procedura il Titolare è credibilmente in grado di valutare, determinare e, se del caso, aggiornare in corso d'opera le misure tecniche e organizzative adeguate al trattamento.

In questa prospettiva, l'art. 25, c. 1, del Reg. si rivela utile perché arricchisce e specifica – sempre in modo sostanzialmente generale – i caratteri della progettazione del trattamento.

In primo luogo, si precisa che quanto richiesto al Titolare deve essere ragionevole e proporzionato, poiché nel determinare le «*adeguate*» misure tecniche e organizzative si tiene conto dello «*stato dell'arte*» e dei «*costi di attuazione*» delle medesime, in comparazione con i caratteri strutturali del trattamento e con la valutazione dei rischi.

In secondo luogo, si offrono precisazioni sulle misure tecniche e organizzative ritenute – di *default* – adeguate, come la pseudonimizzazione, e sui principi di architettura del modello europeo di protezione dei dati, quale il principio generale di minimizzazione dei dati [art. 5, c. 1, lett. *c)*], in forza del quale «*i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*».

I due aspetti appaiono legati ancora una volta alle dinamiche della società digitale: tanto più il trattamento appare suscettibile di comportare il rischio di una circolazione di dati personali in ambiente digitale, quanto più si fanno stringenti le esigenze strutturali di minimizzazione e di pseudonimizzazione dei dati trattati fin dalla progettazione del trattamento. Diversamente, sulla base dei principi di ragionevolezza e proporzionalità, potranno apparire prevalenti, allo stato dell'arte, misure diverse e meno costose a livello organizzativo ed economico. In en-

---

Introduzione al regolamento europeo sulla protezione dei dati, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss., spec. par. 5.1.

trambi i casi è comunque necessaria una valutazione di questi aspetti in sede di progettazione del trattamento ed il Titolare deve essere in grado di giustificare le misure adottate (e quelle non adottate), sulla base di una «istruttoria» interna che si snoda dalla progettazione sino alla conclusione – fase, come noto, delicatissima – del trattamento.

In questa prospettiva, il successivo principio della protezione dei dati personali per impostazione predefinita (o *privacy by default*, cfr. art. 25, c. 2) appare principalmente una (opportuna) specificazione del principio generale di minimizzazione dei dati[45].

Il Titolare deve garantire, in primo luogo, che la infrastruttura tecnica di cui si avvale consenta di svolgere il trattamento utilizzando «*solo i dati personali necessari per ogni specifica finalità del trattamento*». Si instaura, in tal modo, una stretta correlazione fra «*ogni specifica finalità del trattamento*», così come emerge attraverso le informazioni che normalmente il Titolare rende all'interessato, acquisendone il consenso, e «*quantità dei dati personali raccolti*», «*portata del trattamento*», «*periodo di conservazione*» e, soprattutto, «*accessibilità*» dei dati personali trattati. Come più volte emerso in precedenza, quel che veramente si vuole evitare, attraverso i *default settings*, è che «*siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*» (art. 25, c. 2; l'u.c. dell'art. 25 specifica, ancora una volta, che un "elemento" che può essere utilizzato dal Titolare per dimostrare la conformità ai requisiti della *privacy by design* e *by default* è costituito da un meccanismo di certificazione riconosciuto ai sensi dell'art. 42).

Come anticipato, il Reg. affida interamente la protezione dei dati fin dalla progettazione e per impostazione predefinita al Titolare del trattamento. È superfluo osservarlo, ma ciò significa che – nella prospettiva del legislatore europeo – la *privacy by design* è riferita alla progettazione del trattamento.

---

[45] Cfr. G. D'Orazio, *Protezione dei dati by default e by design*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, pp. 79 ss.

Ci si deve domandare se ciò corrisponda pienamente alla natura ed alla logica del principio in parola.

La domanda sorge leggendo il cons. n. 78, ove – in riferimento alle misure tecniche e organizzative – l'attenzione non è rivolta esclusivamente al Titolare del trattamento, ma prende in specifica considerazione «*i produttori dei prodotti, dei servizi e delle applicazioni*», i quali «*in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni (...) dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati*».

Come è evidente, lo stesso Reg. riconosce che non v'è perfetta analogia fra la protezione dei dati fin dalla progettazione del trattamento, da parte del Titolare, e la protezione dei dati fin dalla progettazione da parte del produttore di prodotti, servizi e applicazioni. Più precisamente – seppure in modo implicito – è lo stesso Reg. che lascia giustamente intendere che, in assenza della *privacy by design* dei – si passi la sintesi – sistemi *hardware* e *software*, il Titolare potrebbe non essere in grado di adempiere agli obblighi di protezione «*fin dalla progettazione*» (del trattamento) su di lui gravanti.

In effetti, è stato rilevato che la protezione dei dati fin dalla progettazione è un principio che ha come primario termine di riferimento la progettazione di applicazioni, servizi, prodotti[46], poiché è funzionale

[46] Cfr. D. Klitou, *Privacy-Invading Tecnologies and Privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, *Informtaion Technology and Law Series*, vol. 25, Asser press – Springer, 2014: «PBD simply seeks to ensure that privacy is taken into consideration or built-in at the earliest stage of the device or system's lifecycle, i.e. when the device or system is being designed and manufactured, as opposed to "glued on" or "bolted on" after the device or system has already been developed. In essence, PBD is meant to serve not as a barrier to technology, but rather as a guided and prudent driver of technological development».

all'integrazione all'interno di un prodotto o sistema o applicazione di un modello adeguato di protezione dei dati personali, secondo i 7 famosi principi della *privacy by design*[47]. Il principio pertanto appare rivolgersi innanzitutto ai produttori ed agli ideatori di *information and communications technology* (ICT)[48] e potrebbe in tale prospettiva declinarsi, per chiarezza, in termini di *privacy by research*.

Nella prospettiva disciplinata dal Reg., invece, il principio è tutto declinato – almeno in prima battuta – sul Titolare, e solo indirettamente, per suo tramite, nei confronti di chi architetta e gestisce i sistemi informatici[49].

Il nodo fattuale è che il Titolare può trovarsi ad operare con prodotti e sistemi già predefiniti (*ex ante*) in assenza di un orientamento di *privacy by design*. A quel punto, in sostanza, la protezione dei dati fin dalla progettazione del trattamento finirebbe per risolversi con l'applicazione "ortopedica" (*ex post*) di *privacy enhancing technologies* (ovvero tecnologie di protezione della privacy) su prodotti e sistemi non pensati, all'origine, per integrare strutturalmente la protezione dei dati personali.

D'altra parte, almeno in prospettiva, tale esigenza del Titolare – di tutti i Titolari – non potrà che scaricarsi come istanza ai fornitori ed ai consulenti (a loro volta, in ipotesi, Titolari di trattamenti) e, quindi, progressivamente la *privacy by design* dovrebbe disseminarsi fra «*i*

[47] A. Cavoukian, *7 Foundational Principles of Privacy by Design*, Office of the Information & Privacy Commissioner of Ontario, 2010.

[48] Cfr. A. Principato, *Verso nuovi approcci alla tutela della* privacy*: privacy by design e privacy by default settings*, in *Contratto e impresa. Europa*, 1/2015, pp. 199 ss.

[49] Cfr. The European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Data Protection Reform Package*, 7 marzo 2012, ove si afferma che «182. The principles of data protection by design and by default are not presently addressed to advisers, developers and producers of hardware or software. However, they will be relevant for them from the start, as controllers are bound by them and accountable for compliance. In other words, obligations for controllers (and for processors, as mentioned above) are likely to create some incentives for the market of relevant goods and services».

produttori di applicazioni, servizi, prodotti» in riferimento al loro ambito di attività[50].

Una spinta analoga alla disseminazione delle pratiche della *privacy by design* dovrebbe arrivare dai meccanismi di certificazione di cui i Titolari possono dotarsi, i quali plausibilmente li orienteranno a richiedere l'adozione di sistemi e prodotti orientati alla protezione dei dati personali fin dalla progettazione e per impostazione predefinita.

Appare tuttavia evidente che il legislatore europeo non ha voluto spingersi al di là del mero incoraggiamento dei produttori a tener conto della protezione dei dati personali in sede di sviluppo e progetto dei prodotti (cons. 78), poiché ciò avrebbe comportato una marcata differenziazione normativa di questa categoria di soggetti che, allo stato, deve essere apparsa prematura, non proporzionata e forse un disincentivo all'innovazione ed agli investimenti in ICT[51].

5. Un cenno ad alcuni istituti e figure della *privacy by design*

È opportuno volgere un rapido sguardo ad alcuni istituti che completano il quadro sistematico del trattamento dei dati personali nel nuovo Reg.

Si è già accennato (*supra*, par. 3) alla valutazione di impatto sulla protezione dei dati (art. 35), riferita all'ipotesi di trattamento che possa presentare un rischio elevato.

Il Reg. individua – in modo abbastanza generico – tre tipologie di

[50] Nella prospettiva di un efficace coordinamento fra protezione dei dati personali e *big data*, attraverso l'implementazione della *privacy by design* cfr. A. Cavoukian, *Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism*, in S. Gutwirth-R. Leenes-P. de Hert (edited by), *Reforming European Data Protection Law*, *Law,Governance and Technology Series*, vol. 20, Springer, 2015, pp. 293 ss.

[51] Sull'impatto economico della regolazione europea in materia di protezione dei dati personali, cfr. H. Lee-Makiyama, *The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs*, in L. Floridi (a cura di), *Protection of Information and the Right to Privacy - A New Equilibrium?*, *Law, Governance and Technology Series*, vol. 17, Springer, 2014, pp. 85 ss.

trattamento che richiedono una valutazione preventiva di impatto[52]. Il novero dei trattamenti necessariamente soggetti a valutazione si completa con un elenco redatto dalla autorità nazionale di controllo, la quale può anche predisporre un elenco di trattamenti per cui non è richiesta la valutazione (art. 35, c. 3, 4, 5).

Il Titolare è tenuto a consultare preventivamente l'autorità di controllo se dalla valutazione di impatto emerge l'esistenza di un rischio elevato in assenza di misure di attenuazione del rischio (art. 36, c. 1).

Quel che interessa sottolineare[53] è che l'inserimento dei principi della *privacy by design* e *by default* ha reso ragionevole superare la previsione della Dir. dell'obbligo generale, in riferimento ad alcuni trattamenti, di notifica alla autorità di controllo (cons. 89), rendendo – almeno astrattamente – residuali le ipotesi in cui è obbligatorio ricorrere alla comunicazione preventiva, la quale – in ogni caso – è successiva ad una "fase istruttoria" sviluppata autonomamente dal Titolare del trattamento (la valutazione di impatto)[54].

Il Reg. prevede che, nel momento in cui svolge la valutazione di impatto il Titolare del trattamento consulta il responsabile della protezione dei dati «*qualora ne sia designato uno*» [art. 35, c. 2 e correlativamente art. 39, c. 1, lett. *c)*].

Ciò ci consente di osservare una delle principali novità del Reg.: il

---

[52] L'art. 35, c. 3, dispone che: «*3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*».

[53] Per un approfondimento della valutazione di impatto sulla protezione dei dati e della comunicazione preventiva si rinvia a G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, cit. pp. 68 ss.

[54] Cfr. art. 18 (e 20), Dir. e artt. 17 e 37, D.Lgs. 196/03.

c.d. *data protection officer* (DPO).

In questa sede non interessa analizzare nello specifico le funzioni ed i caratteri del responsabile della protezione dei dati[55], mentre rileva invece inquadrarlo nella prospettiva di un trattamento che fin dalla progettazione incorpora l'esigenza della protezione dei dati personali. Forse non a caso, pertanto, si tratta di una figura che è già disciplinata in diversi Stati membri e che oggi il Reg. vuole introdurre in via generale a livello europeo[56].

La designazione di un DPO da parte del Titolare (art. 37, c. 1) è obbligatoria solo in casi specifici: in generale, i soggetti pubblici («*autorità pubblica*», «*organismo pubblico*») devono sistematicamente nominare un DPO, ad eccezione delle autorità giurisdizionali quando esercitano la funzione giurisdizionale; per tutti gli altri soggetti, la designazione è obbligatoria quando le «*attività principali del Titolare*», considerati i caratteri del trattamento, «*richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*» oppure quando consistono nel trattamento, su larga scala, di categorie particolari di dati, di cui all'art. 9[57], o di dati relativi a condanne penali e reati di cui all'art. 10.

---

[55] Cfr. comunque cons. n. 77 (in merito agli orientamenti per la individuazione del rischio da parte del Titolare) e artt. 13, c. 1, lett. *b)*; 14, c. 1, lett. *b)* (in merito ai diritti dell'interessato di conoscere i dati di contatto del DPO); 30, c. 1, lett. *a)* e c. 2, lett. *a)* (in merito alla indicazione nei registri da parte del Titolare/Responsabile del nome e dati di contatto del DPO); 33, c. 3, lett. *b)* (in merito al contenuto del nome e dati di contatto del DPO nella notifica in caso di violazione dei dati personali); 35, c. 2; il capo IV , sez. 4, artt. 37-39 (dedicati proprio alla figura del DPO); gli artt. 47, c. 2, lett. *h)*; 57, c. 3. Per chiari dettagli sulla nomina, la posizione e i compiti del DPO, cfr. Gruppo di lavoro Articolo 29, *Linee-guida sul responsabile della protezione dei dati (RPD)*, (versione emendata del 5 aprile 2017), in *http://www.garanteprivacy.it/*.

[56] Cfr., per più specifiche indicazioni, G. M. Riccio, *Data protection officer e altre figure*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, cit., pp. 33 ss., spec. PP. 49 ss.

[57] … quali i «*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale», ovvero i «dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*» (art. 9, c. 1).

Il DPO è designato in funzione delle qualità professionali ed è tenuto ad una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati; può essere un dipendente del Titolare o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi; i dati di contatto del DPO devono essere comunicati al Garante dal Titolare/Responsabile del trattamento (art. 37, c. 5-7).

I compiti del DPO si dipanano essenzialmente su due fronti: nei confronti del Titolare/Responsabile del trattamento, poiché spetta al DPO fornire consulenza e sorvegliare la corretta applicazione della normativa in materia di protezione dei dati, contribuire ad informare e formare il personale, oltre che, se richiesto, fornire un parere e sorvegliare lo svolgimento della valutazione di impatto; nei confronti dell'Autorità di controllo, con cui il DPO è chiamato a collaborare e a fungere da «*punto di contatto*» (in particolare in caso di comunicazione preventiva). Ovviamente, non si può escludere che il DPO possa avere una funzione anche nei confronti degli interessati al trattamento, i quali hanno diritto di ottenerne i dati di contatto da parte del Titolare (cfr. artt. 13 e 14).

Il compito principale del DPO si rinviene incrociando la qualificazione professionale che lo caratterizza, con il ruolo di collegamento operativo fra Titolare/Responsabile del trattamento ed il livello istituzionale della protezione dei dati personali. In altri termini, il vero ruolo che il DPO assume è quello di importare, nell'organizzazione del Titolare del trattamento, l'esperienza maturata ed aggiornata in merito alle migliori pratiche attuative ed alle politiche della *privacy by design* e *by default*[58].

Se è giusto sottolineare che – nella normativa europea – il principio della *privacy by design* significa integrare la protezione dei dati fin dalla progettazione del trattamento, è bene osservare che questa strategia – per buona parte dei trattamenti su larga scala (e per i trattamenti dei

[58] Come osserva F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Il Regolamento europeo 2016/679*, Torino, 2017, p. 109, «il DPO opera a livello per così dire "micro". Esso, infatti, costituisce una figura di raccordo tra gli interessi e le finalità dei titolari dei trattamenti, la tutela proattiva degli interessati, l'attuazione coerente della nuova normativa e l'attività di consulenza e controllo delle Autorità».

soggetti pubblici) – trova compimento attraverso l'inserimento, nella organizzazione aziendale, di una figura specializzata, che ha esattamente questa vocazione professionale e questo compito.

In tal modo, il legislatore europeo tenta – per i trattamenti più rischiosi – di colmare l'inesorabile *gap* fra norme vigenti e relativa applicazione, inserendo – se si passa la sintesi – perizia e «prassi» applicativa all'interno del tessuto organizzativo del Titolare del trattamento. Con ogni evidenza, grazie all'introduzione sistematica del DPO nell'organizzazione dei soggetti pubblici Titolari del trattamento, il Reg. ha ritenuto di far leva sul vasto e ramificato settore pubblico europeo per raggiungere questo fine.

Va osservato, infine, che attraverso la figura professionale del DPO, si ottiene anche un legame – non solo, come talvolta si osserva, formale e burocratico – fra meccanismi di certificazione o processi di formazione nel settore della protezione dei dati personali e figure professionali interne o al servizio dell'organizzazione del Titolare del trattamento.

In conclusione, pertanto, è possibile osservare che l'istituto della valutazione di impatto induce il Titolare alla formalizzazione della visione e delle politiche del trattamento che presenti elevati rischi, mentre la figura del DPO è volta ad integrare nell'organizzazione del Titolare quell'insieme di competenze e di collegamenti necessari per strutturare quella visione e quelle politiche di protezione dei dati: entrambi gli aspetti vanno colti ed osservati come istituti che completano la strategia europea per una organica protezione dei dati, anticipata rispetto all'insieme dei trattamenti, sistematica e costante per tutta la loro durata.

6. Già e non ancora: il Reg. europeo fra rilievo globale ed esigenze di attuazione

Si vuole concludere il presente contributo con tre osservazioni finali.

Si sono passate in rassegna diverse disposizioni della pur vastissima e complessa trama del Reg. europeo (173 cons. e 99 artt.). Non si può

evitare di rilevare che il Reg. introduce molteplici novità, ma con una chiara coscienza della necessità di una attuazione progressiva dei nuovi principi e dei nuovi istituti. Ne sono un segno evidente non solo i diversi rinvii alla integrazione da parte degli Stati membri (cons. 8) contenuti nell'articolato, ma anche il ruolo riconosciuto alla c.d. *soft law* (codici di condotta, linee guida, elenchi, ecc.), agli atti delegati della Commissione europea (art. 92), ai meccanismi per garantire una applicazione uniforme delle regole introdotte dal Reg. e di quelle che grazie al Reg. prenderanno forma (ci si riferisce, in particolare, alle disposizioni contenute nel capo VII «*Cooperazione e coerenza*» del Reg., e in particolare al meccanismo di coerenza). Non meno rilevanti le innovazioni sul piano istituzionale e delle relazioni e competenze delle istituzioni nazionali ed europee.

È facile pertanto osservare che il Reg. ha mosso un passo importante verso la *privacy by design*, ma che questo passo è il primo di un cammino che si prospetta lungo e volto ad affrontare non solo un'epoca di cambiamenti, ma un cambiamento d'epoca[59], indotto – per quanto qui interessa – dalla evoluzione digitale.

Ciò consente di introdursi ad una seconda osservazione. La società digitale è un fenomeno globale in grado di comportare – di *default* – l'avvento di una sorveglianza di massa, che non ha riguardo a confini e limiti, che può arrivare a prevedere i comportamenti e prima ancora le aspirazioni ed i desideri e, prevedendoli, può influenzarne il divenire ed il libero progredire. Il tutto attraverso processi automatici, progressivamente gestiti (guidati?) da forme di intelligenza artificiale al servizio di intelligenze umane e dei loro interessi. Si tratta di un contesto c.d. virale, che si diffonde attraverso l'espandersi e la fruizione dei servizi e delle utilità digitali da parte delle persone e delle collettività.

[59] Cfr. quanto acutamente osservato da Papa Francesco, *Discorso del Santo Padre*, V Convegno nazionale della Chiesa italiana, Firenze, 10 novembre 2015, in *http://w2.vatican.va/content/francesco/it/speeches/2015/november/documents/papa-francesco_20151110_firenze-convegno-chiesa-italiana.html*.

In questo contesto, l'Unione europea non è una realtà neutrale nel panorama mondiale. Infatti, se in altre parti del mondo si concentra la produzione di *devices* e l'ideazione e produzione di ICT, non è difficile osservare che il vecchio continente (cioè l'Unione europea) è principalmente un grande consumatore di ICT e produttore di dati (anche personali).

L'esigenza di tutelare i propri «prodotti» è alla base della familiarità dell'ordinamento europeo con la protezione dei dati personali, sia in una visione di tutela della persona, sia nella prospettiva di tutela di un vero e proprio interesse pubblico europeo (cfr., *supra*, par. 2). Per questo, pur non essendo nata su suolo europeo[60], la *privacy by design* si è fatta strada proprio nell'Unione europea. Si tratta di un principio olistico, che attraverso la tutela della autodeterminazione informativa della persona si presta a garantire anche la protezione di gruppi, territori, Stati: esigenza particolarmente avvertita, nel continente europeo, al tempo dei *big data*, della profilazione e della sorveglianza di massa[61].

A ben vedere si tratta di una esigenza che inizia ad essere avvertita anche al di là dei confini dell'Unione europea, su cui vale la pena spendere l'ultima considerazione. Non ci si può nascondere che il Reg. e prima ancora le istituzioni europee hanno l'ambizione di fare della disciplina europea un punto di riferimento nel panorama internazionale. Sotto questo profilo, il fine del Reg. è di rappresentare uno «standard globale» di tutela[62], capace di diffondersi viralmente grazie alla ragionevolezza ed utilità dell'approccio di tutela in esso contenuto, così co-

[60] Cfr. A. Cavoukian, *Privacy by Design: Leadership, Methods, and Results*, in S. Gutwirth-R. Leenes-P. de Hert-Y. Poullet (a cura di), *European Data Protection: Coming of Age*, Springer, 2013, p. 175.

[61] Cfr. quanto segnalato da R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. Cost.*, n. 1/2016, pp. 289 ss.

[62] Cfr. L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale scientifica, Napoli, 2016, p. 70, la quale puntualmente ricorda che con il motto "*one continent, one law*", che ha accompagnato nelle istituzioni europee l'iter formativo del Regolamento, la allora Vicepresidente della Commissione Viviane Reding dichiarava chiaramente di ambire a creare proprio un "global standard".

me si diffondono grazie alla loro semplicità ed utilità le tecnologie digitali[63]. *Vaste programme*, potrebbe chiosare qualcuno[64]. Tuttavia, il Reg. vigente ha la naturale vocazione a estendere la propria influenza al di là dei confini dell'Unione europea, se non altro nei confronti di chi ha interesse a trattare dati (e non solo dati) europei e di chi ritiene che la *privacy by design*, magari declinata in modo autonomo ed originale, non sia un'idea da scartare. Forse, infatti, è proprio la *privacy by design*, più che la sua versione europea, ad essere suscettibile di divenire uno standard globale. Già, e non ancora.

[63] Cfr. G. Buttarelli, *The EU GDPR as a clarion call for a new global digital gold standard*, in *International Data Privacy Law* 2/2016, pp. 77-78.

[64] Cfr. B.J. KROOPS, *The Trouble with European data protection law*, in *International Data Privacy Law*, 2014, Vol. 4, no. 4, p. 250: "The trouble with the law, as with Hitchcock's Harry, is that is dead. What the statues describe and how the courts interpret this has usually only a marginal effect on data-processing practices. Data protection law is a dead letter; current ideas what to do with the body are not leading anywhere except that they offer entertainment to spectators. With the current reform, the letter of data protection law will remain stone-dead".

Marco Bolognese
Università degli Studi di Macerata

La tutela dei dati personali nel Regolamento UE 2016/679

Sommario: 1. La base giuridica – 2. Alcuni profili di illegittimità rispetto al Trattato di Lisbona – 3. La definizione dei dati – 4. I soggetti destinatari – 5. Ambito di applicazione territoriale – 6. I principi generali ed i diritti del proprietario dei dati – 7. Gli obblighi dei tenutari dei dati – 8. Le autorità di controllo – 9. Considerazioni conclusive

La tutela del trattamento dei dati personali e la loro libera circolazione verrà disciplinata, a far data dal 25 maggio 2018, dal regolamento 2016/679[1]. Il nuovo "*approccio globale alla protezione nell'Unione europea*"[2] si sostituisce alla direttiva 95/46/CE[3], divenuta oramai inidonea a causa degli incalzanti sviluppi tecnologici, che hanno accresciuto esponenzialmente la condivisone e la raccolta dei dati da parte delle imprese private e delle pubbliche autorità nello svolgimento delle loro attività. L'intento del legislatore europeo, pertanto, è quello di restaurare un clima di fiducia negli ambienti *on line*, con conseguenti benefici

[1] Regolamento (UE) 2016/79 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 95/45 CE (regolamento generale sulla protezione dei dati), in GUUE del 4.5.2016. L. 119/3. Tale strumento è affiancato dalla Direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati. D'ora in avanti nelle note gli articoli del regolamento verranno indicati come "art".

[2] Proposta della Commissione europea del 25.1.2012, COM(2012) 11 *final*, in *http://www.eur-lex.europa.eu*.

[3] Direttiva 95/46/CE in *Gazzetta ufficiale* n. L 281 del 23/11/1995, pag. 0031 – 0050, d'ora in avanti indicata in nota come "direttiva".

per la crescita dell'economia digitale nel mercato interno. La mancanza di fiducia, infatti, frenando i consumatori sia negli acquisti *on line* sia nell'utilizzo di nuovi servizi, rafforza il rischio di rallentare lo sviluppo di applicazioni tecnologiche innovative.

L'ambizioso progetto di una tutela globale appare in realtà tutt'altro che esaustivo. Da un lato, infatti, il Regolamento non trova applicazione nel trattamento dei dati effettuato: dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione; dalle istituzioni dell'U.E.[4]; in caso di repressione e di accertamento dei reati. Dall'altro lato, non si rinviene un ben definito e chiaro coordinamento con la legislazione degli Stati Membri, sia essa preesistente o futura. Invero, il tratto comune del Regolamento è la costante possibilità di deroga al trattamento dei dati per consentire l'esercizio di altri diritti fondamentali o la tutela di interessi dello Stato. A questa delicata operazione di bilanciamento si affiancano possibili profili di non conformità con i trattati istitutivi dell'Unione europea e l'esistenza a livello internazionale di una convenzione tra gli Stati membri che già disciplinava alcuni aspetti del trattamento dei dati.

Senza sottacere, poi, la complessità del testo normativo con i suoi n. 99 articoli e 173 considerando. Quest'ultimi a volte – ad esempio nel caso del trattamento dei dati sensibili[5] – oltrepassano la loro funzione di

[4] Regolamento CE n. 45/2001, in *http://www.eur-lex.europa.eu*.

[5] L'art. 9 in materia di dati sensibili pone una deroga al loro divieto di trattamento giustificata da motivi di interesse pubblico nei settori della sanità pubblica. Il considerando n. 54 aggiunge che, in tale ambito, il trattamento è lecito senza il consenso dell'interessato mentre esso non è consentito per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito. Analogamente l'art. 3 stabilisce in modo scarno che il regolamento si applica ai dati trattati da un titolare del trattamento non stabilito nell'Unione europea, quando l'attività di trattamento è connessa all'offerta di beni o servizi. A fronte di tale sintetica disposizione, il considerando 27 sembra aggiungere una fattispecie normativa ulteriore, riferita alla semplice intenzione di offrire: "*Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito*

motivare "in modo conciso le norme essenziali dell'articolato", contenendo enunciati a carattere normativo, contrariamente all'accordo interistituzionale sulla qualità redazionale degli atti[6] e alla giurisprudenza interpretativa del medesimo[7].

1. La base giuridica

La protezione dei dati personali, prima del Trattato di Lisbona trovava la sua fonte in due convenzioni internazionali

L'art. 6 dell'allora TUE richiamava la CEDU come fonte da cui desumere i principi fondamentali. Non a caso l'art. 1 della direttiva 95/46/CE ricalcava a grandi linee l'art. 8 della CEDU nella interpretazione fornitane dalla Corte di Strasburgo[8], cosicché il trattamento dei dati personali veniva considerato un aspetto del diritto alla vita privata.

Lo sviluppo tecnologico degli anni '60 ha portato[9] nel 1981 alla speci-

---

web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione".

[6] Il 22 dicembre 1998 il Parlamento europeo, il Consiglio e la Commissione hanno concluso un accordo interistituzionale sugli orientamenti comuni relativi alla qualità redazionale della legislazione comunitaria, in GU 1999, C 73, pag. 1. Gli orientamenti non sono giuridicamente vincolanti. Tra i principi ivi contenuti si annoverano i seguenti: "10. I 'considerando' motivano in modo conciso le norme essenziali dell'articolato (…). Non contengono enunciati di carattere normativo (…)".

[7] CGUE, 12 luglio 2005, cause riunite C-154/04 e C-155/04, *Alliance for Natural Health*, in *Racc. 2005*, pag. I-6451, punto 92.

[8] CEDU, 2 agosto 1984, ricorso n. 8691/79, *Malone c. Regno Unito;* 3 aprile 2007, ricorso n. 62617/00, *Copland c. Regno Unito*, in *www.echr.coe.int*.

[9] Committee of Ministers (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals *vis-a-vis E*lectronic Data Banks in the Private Sector, 26 September 1973; Committee of Ministers (1974), Resolution (74) 29 on the Protection

fica protezione dei dati personali, attraverso la stipula dalla Convenzione n. 108[10] da parte degli Stati facenti parte del Consiglio d'Europa, ratificata poi da tutti gli Stati dell'Unione europea, ed aperta alla firma di Paesi terzi. L'esistenza di tale strumento pone qualche ragionevole dubbio sul rispetto del principio di proporzionalità da parte del Regolamento. Infatti la Convenzione contiene in larga parte elementi comuni al regolamento[11]. Senza sottacere che nel 1999[12] fu modificata per permettervi l'adesione dell'Unione europea. Infine nel 2001[13] fu adottato un protocollo addizionale riguardante i flussi transazionali di dati verso Paesi non contraenti e la creazione obbligatoria dell'Autorità di controllo per la protezione dei dati personali.

Infine, con il Trattato di Lisbona del 2009, la protezione dei dati personali divine un diritto fondamentale sancito nell'art. 8 della Carta

---

of the Privacy of Individuals *vis-a-vis* Electronic Data Banks in the Public Sector, 20 September 1974, in *www.coe.int*.

[10] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108 del 28 gennaio 1981, in *https://www.coe.int*.

[11] La Convenzione si applica a tutti i trattamenti di dati effettuati sia nel settore privato sia in quello pubblico, come ad esempio l'elaborazione dei dati da parte delle autorità di polizia e giudiziarie. La raccolta e il trattamento dei dati personali sono governati dai principi di equità e di legittimità: i dati elaborati automaticamente sono registrati per scopi legittimi specifici e non possono essere utilizzati per fini incompatibili con tali scopi; né conservati per più di quanto è necessario. Sono vietati, in assenza di adeguate garanzie giuridiche, l'elaborazione di dati sensibili quali quelli relativi alla razza, ideologie politiche, salute, religione, vita sessuale di una persona. La Convenzione sancisce anche il diritto dell'individuo di conoscere le modalità del trattamento ed il diritto alla rettifica. Le restrizioni alla tutela, stabilita dalla Convenzione, sono ammesse per garantire superiori interessi, come ad esempio la sicurezza o la difesa dello Stato contraente. La libera circolazione dei dati personali tra i Paesi aderenti subisce anche alcune limitazioni verso quegli Stati in cui la legislazione non fornisce una protezione equivalente.

[12] Amendments to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) Allowing the European Communities to Accede, Adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999, in *www.coe.int*; art. 23.2 della Convenzione n. 108.

[13] Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, CETS No. 181, 2001, in *www.coe.int*.

di Nizza[14]; mentre l'art. 16 del TFUE (già 286 TCE), unitamente all'art. 4.1 TFUE, ne affidano la tutela alla competenza concorrente tra gli Stati membri e l'Unione europea. I due rifermenti normativi costituiscono il fondamento giuridico del Regolamento[15].

Va subito precisato che la protezione dei dati, sebbene assurga a diritto fondamentale dell'Unione, non è una prerogativa assoluta, potendo subire delle deroghe, per permettere l'esercizio di altri diritti fondamentali o proteggere particolari interessi dello Stato[16]. È pur vero che l'art. 8 della Carta di Nizza, contrariamente al "gemello" della CEDU, non contiene al suo interno alcuna limitazione. Tuttavia le restrizioni, in primo luogo, erano già state imposte dalla Corte di giustizia secondo cui la disposizione *de qua* deve essere letta tenendo presente la sua funzione nella società[17]. Secondariamente l'art. 52 della Carta prevede delle limitazioni a condizione che siano imposte dalla "dalla legge", "siano necessarie", "rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui". Tali vincoli corrispondono in buona sostanza a quelli di cui all'art. 8.2 della CEDU[18]. Pertanto

---

[14] Carta dei diritti fondamentali dell'Unione europea, in *http://eur-lex.europa.eu*. L. S. Rossi, *"stesso valore giuridico dei Trattati"? Rango, primato ed effetti della Carta dei diritti fondamentali dell'Unione europea*, in *Il diritto dell'Unione europea*, 2016, p. 329.

[15] Considerando 1.

[16] P. De Sena, *Proportionality and Human Rights in International Law: Some... «Utilitarian Reflection»*, in *Rivista di diritto internazionale*, 2016, p. 1009.

[17] CGUE, 9 Novembre 2010, cause riunite C-92/09 e C-93/09, *Volker e Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, in *Racc*. 2010, punto 48.

[18] Art. 8 comma 2 CEDU "Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Sul legittimo scopo perseguito v. CEDU, 28 gennaio 2003, ricorso n. 44647/98, *Peck c. Regno Unito,* § 85. Sulla necessità per la sicurezza sociale v. CEDU, 26 marzo1987, ricorso n. 9248/87, *Leander c. Svezia*, §§ 58-67; 18 ottobre 2011, ricorso n. 16188/07, *Khelili c. Svizzera.* Sul concetto di legge v. CEDU, 16 febbraio 2000, ricorso n. 27798/95, *Amann c. Svizzera*, § 50; 25 marzo 1988, ricorso n. 23224/94, *Kopp c. Svizzera*, § 55; 10 febbraio 2009, ricorso n. 25198/02, *Iordachi and*

atteso il contenuto quasi identico delle due disposizioni, sulla base dell'art. 52.3 della Carta, le restrizioni dovranno essere interpretate alla luce della giurisprudenza della Corte Edu. I giudici di Strasburgo, in particolare, hanno circoscritto la tutela dei dati per garantire l'esercizio di altri diritti quali la libertà di stampa, di espressione[19], la libertà di scienza e di arte[20]. Conformemente a tale giurisprudenza, il Regolamento dispone espressamente delle deroghe al diritto sul trattamento dei dati per garantire le stesse libertà[21]. Inoltre, il riferimento alla giurisprudenza della Corte di Strasburgo diverrà una operazione ermeneutica necessaria, in considerazione della possibilità degli Stati di derogare alle disposizioni del Regolamento.

La necessità di tale richiamo è testimoniata dallo stesso strumento derivato, che recepisce le restrizioni di cui all'art. 52 della Carta al fine di limitare i diritti e gli obblighi connessi al trattamento, per la salvaguardia di beni superiori come un interesse economico o finanziario dell'Unione o dello Stato membro[22].

2. Alcuni profili di illegittimità rispetto al Trattato di Lisbona

Nonostante la chiarezza della base giuridica, il continuo bilanciamento del diritto al trattamento dei dati con altri interessi, quindi la sua limitazione anche e soprattutto da parte degli Stati membri, pone un dubbio più che legittimo sul rispetto del principio di sussidiarietà da

---

Others c. Moldavia, § 50; 7 febbraio 2012, ricorso n. 39954/08, *Axel Springer AG c. Germania*, §§ 90-91; 7 febbraio 2012, ricorsi nn. 40660/08 e 60641/08, *Von Hannover c. Germania* (N. 2)*,* §§ 118 e 124, tutte in *www.echr.coe.i*nt.

[19] CEDU, ricorso n. 39954/08 *Axel Springer AG c. Germana,* cit., § 90 e 91; ricorsi 40660/08 e 60641/08, *Von Hannover c. Germany* (N. 2*),* cit., §§ 118 e 124, in *www.echr.coe.int*.

[20] CEDU, 24 maggio 1988, ricorso n. 10737/84, *Müller e altri c. Svizzera*; 25 gennaio 2007, ricorso n. 68345/01, *Vereinigung bildender Künstler c. Austria*, §§ 26 e 34, in *www.echr.coe.int*.

[21] Artt. 85 e 89.

[22] Art. 23.

parte della normativa derivata[23].

Tale violazione si individuerebbe, ad esempio, in riferimento alle ipotesi che determinano la liceità del consenso. Tra esse si annoverano il trattamento dei dati necessario o per adempiere ad un obbligo legale (cui è sottoposto il titolare del trattamento) oppure per eseguire un compito connesso all'esercizio di pubblici poteri (cui è investito il titolare del trattamento). In entrambi i casi gli Stati membri rimangono sovrani di stabilire la base giuridica da cui deriva l'obbligo del trattamento: non si richiede nemmeno l'adozione di un atto legislativo da parte del parlamento nazionale, fatte salve le prescrizioni dell'ordinamento costituzionale interessato. In aggiunta il Regolamento prevede che gli Stati membri possono mantenere (o introdurre) disposizioni specifiche sulle modalità del predetto trattamento[24].

La normativa domestica può addirittura derogare alla quasi totalità delle disposizioni del Regolamento – riguardanti i capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) – qualora sia necessario per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione. Deroghe o limitazioni sono consentite anche al diritto di acceso (art. 15) di rettifica (art. 16) di cancellazione (art. 17) per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[25]. La normativa statale può, altresì, conservare limitazioni già disposte o introdurne di nuove riferite al trattamento di dati genetici e biometrici[26].

Appare evidente, dunque, come l'azione dell'Unione non sia affatto

[23] Art. 5.3 TUE.
[24] Considerando 41; art. 6 par. 2.
[25] Considerando 41; art. 6 par. 2. Considerando 156; art. 6 par. 3; art. 85 e art. 89.
[26] Art. 9.

necessaria, stante il mantenimento di una legislazione preesistente[27] in aggiunta alla possibilità, per i parlamenti nazionali, di derogare al regolamento. Anzi la possibilità dell'intervento statale finisce proprio per mantenere quella frammentazione della protezione dei dati, che il Regolamento si prefigge di eliminare nel territorio dell'Unione[28].

Per altro verso, il Regolamento violerebbe anche il "principio di attribuzione" delle competenze, perché più che regolare la competenza "concorrente" tra gli Stati e l'Unione[29], finisce per trasformarla in competenza "esclusiva". Infatti, una volta che l'Unione europea ha disciplinato la materia con il Regolamento in esame, il medesimo, come visto, conferisce agli Stati la possibilità di introdurre norme soprattutto di carattere derogatorio. I Paesi membri, vale a dire, possono adottare autonomamente atti giuridici vincolanti perché sono stati autorizzati dall'Unione, al pari di quanto avviene nelle competenze esclusive[30]. Mentre nella competenza concorrente, come quella in esame, gli Stati devono intervenire nella "*misura in cui l'Unione non ha esercitato la propria*"[31]; non possono, cioè, legiferare sugli elementi disciplinati nell'atto adottato[32].

Si violerebbe, poi, il precetto costituzionale europeo del divieto di discriminazione sulla base del patrimonio[33]. Infatti il Regolamento, a certe condizioni, non impone alle imprese con meno di 250 dipendenti la tenuta dei registri in cui annotare il trattamento dei dati[34]. Tuttavia tale l'obbligo, per di più soggetto a sanzione pecuniaria amministrati-

[27] Emblematico il considerando 52 che, in riferimento alla tutela dei dati sensibili, afferma che le deroga al divieto del loro trattamento dovrebbe essere consentita anche quando è prevista dal diritto degli Stati membri.
[28] Considerando 9.
[29] M. E. Bartoloni, *Competenze puramente Statali e diritto dell'Unione europea*, in *Il diritto dell'Unione europea*, 2015, p. 339.
[30] Art. 2.1 TUE.
[31] Art. 2.2 TUE.
[32] Protocollo n. 25.
[33] Art. 21 Carta dei diritti fondamentali dell'Unione europea, cit.
[34] Art. 30.5.

va[35], permane per la persona fisica professionista la cui prestazione è prevalentemente di natura personale, caratterizzata cioè dalla quasi assenza di impiego di capitali e lavoro altrui, e che per tale fatto, *a fortiori*, si avvicina all'impresa con meno di 250 dipendenti. Quindi, fermo il dato politico di individuare l'esenzione per le piccole e medie imprese, nessuna giustificazione si rinviene per mantenere tale obbligo in capo al professionista. Si trattano, così, in modo diverso situazioni patrimoniali analoghe.

Sembrerebbero violati, anche, i presupposti stabiliti dai trattati[36] per il conferimento della delega alla Commissione, per l'adozione di atti giuridici vincolanti. Infatti, in tema dei diritti dell'interessato, tra cui rientrano soprattutto le informazioni e comunicazioni che il titolare deve fornire nel rispetto del principio di trasparenza, l'art. 29 del regolamento conferisce alla Commissione il potere di adottare atti delegati "*al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate*". La parola "stabilire" va intesa come precisare e dunque è sinonimo di "integrare" l'atto legislativo di base[37]. Ciò posto si osserva che la delega sembra riguardare gli atti essenziali del regolamento, poiché la Commissione può incidere non solo sulle informazioni che costituiscono lo "zoccolo duro" dei di-

[35] Art. 83.4 lett. *a)*.
[36] Art. 290 TFUE.
[37] La Corte dopo aver tracciato la distinzione tra "*La delega di un potere di «integrare» un atto legislativo,* [che] *infatti, consiste semplicemente nell'autorizzare la Commissione ad attuare tale atto. Qualora essa eserciti un tale potere, il suo mandato è limitato allo sviluppo in dettaglio, nel rispetto dell'integralità dell'atto legislativo adottato dal legislatore, degli elementi non essenziali della specifica normativa che il legislatore non ha definito*" (41) e "*La delega di un potere di «modificare» un atto legislativo* [che]*, invece, consiste nell'autorizzare la Commissione a emendare o abrogare elementi non essenziali previsti in tale atto dal legislatore. Qualora la Commissione eserciti un tale potere, essa non è ovviamente tenuta ad agire nel rispetto degli elementi che il mandato accordatole mira a «modificare»*" (42), ritiene che il verbo specificare sia sinonimo di integrare (punto 47)*,* cfr. CGUE, 17 marzo 2016, causa C-286/14, *Parlamento europeo c. Commissione*, punto 41*,* in *ECLI: ECLI:EU:C:2016:183.*

ritti della persona fisica ma anche sulle modalità di comunicazione che sono reputate altrettanto fondamentali in quanto permeate dal principio di trasparenza.

3. La definizione dei dati

In merito al concetto di "dati personali", la portata "globale" della tutela si percepisce non tanto nella nozione di dato personale, definita, al pari della direttiva[38], come le informazioni riguardanti una persona fisica che concorrono ad identificarla, quanto nell'aumento degli elementi che conducono all'identificazione, quali il nome, i dati relativi all'ubicazione, gli elementi genetici, e un identificativo *on line*[39]. Quest'ultimo a sottolineare l'adeguamento della normativa al progresso tecnologico.

Specifica tutela viene riservata ai dati c.d. sensibili[40] il cui novero si arricchisce rispetto alla direttiva. Ai dati relativi alla vita sessuale si affianco quelli relativi all'orientamento sessuale. Si specifica, caso mai ce

[38] Art. 83.4 lett. *a)*.

[39] Considerando 29: indirizzi IP, marcatori temporanei (*cookies*), identificativi di altro tipo, come i tag di identificazione a radiofrequenza. CGUE, 19 ottobre 2016, causa C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland***,** in *ECLI:EU:C:2016:779*, secondo cui l'indirizzo IP dinamico (ossia quello, provvisorio, assegnato ad ogni connessione a Internet e sostituito in caso di successive connessioni, e non indirizzi IP «statici», che sono invariabili e consentono l'identificazione permanente del dispositivo connesso alla rete) va considerato come dato personale poiché consente l'identificabilità dell'utente (intestatario del contratto di accesso) tramite l'incrocio con i dati raccolti dal *provider*. Di conseguenza, gli operatori di un sito *web* sono ammessi a trattare i dati personali per i loro interessi legittimi, che nel caso esaminato dalla Corte erano costituiti dalla protezione della rete e del sito *web*, in particolare per ricercare i responsabili di attacchi informatici. Trattamento che per tali fini può avvenire anche senza il consenso. Mentre la raccolta degli IP non è ammessa per fini diversi, quali ad esempio il contrasto alle violazioni del *copyright*, poiché esso non rientra negli interessi legittimi dei gestori del sito.

[40] Tale qualificazione, assente nell'art. 9, si rinviene nel considerando 51.

ne fosse bisogno, che il dato «origine razziale» non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte[41]. Fanno il loro ingresso i dati biometrici ottenuti cioè da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali, quali l'immagine facciale o i dati dattiloscopici. Mentre non sono più considerati sensibili e nemmeno rientranti nell'ambito di applicazione del regolamento quelli relativi alle condanne penali e ai reati, il cui trattamento e l'eventuale registro delle condanne vengono affidati all'autorità di pubblica sicurezza[42]. Essi invece sono considerati tali dalla Convenzione n. 108.

Si amplia, inoltre, l'elenco della categoria dei dati medici: i dati relativi alla salute, presenti nella direttiva senza indicazione alcuna, vengono ora definiti come quelli concernenti la salute fisica e mentale comprese le prestazioni di assistenza sanitaria che rilevino tali informazioni[43]. Essi si differenziano dai dati genetici perché quest'ultimi risultano dall'analisi di un campione biologico della persona: esempio il DNA.

I dati sensibili sono sottoposti a diversi livelli di protezione. In primo luogo viene sancito un divieto generale di trattamento, suscettibile di essere derogato per soddisfare diverse garanzie, in parte già presenti nella direttiva[44] quali la difesa in giudizio di un diritto o un interesse vitale dell'interessato; altre nuove come l'esercizio di diritti e obblighi del titolare del trattamento in materia di diritti del lavoro e della sicurezza sociale.

Viene riconfermata la tutela più stringente[45] nel momento in cui essi

[41] Considerando 51.
[42] Considerando 19; Art. 10, già art. 8.5 direttiva.
[43] Per alcune esemplificazioni v. considerando n. 35.
[44] Considerando 25, 34, 51-54; art. 9. Art. 8 direttiva.
[45] Tutela serrata già confermata dalla Corte di Strasburgo. La vicenda riguardava un cittadino inglese affetto da HIV, che aveva commesso una serie di reati sessuali. Successivamente veniva anche condannato per omicidio colposo poiché aveva deliberatamente esposto le sue vittime al rischio di infezione da HIV. Con tale sen-

siano collegati ad attività della sanità pubblica[46]. Il trattamento, in tale ambito, è ammesso per motivi di interesse pubblico (quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici), purché i dati siano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale[47]. Allo stesso modo il trattamento è ammesso per finalità di medicina preventiva o di medicina del lavoro, di diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari, che si fondano anche su un contratto con un professionista della sanità il quale deve essere sottoposto al segreto professionale. In tali ipotesi la persona fisica non può pretendere la cancellazione dei suoi dati[48].

Preme evidenziare come la tutela dei dati relativi alla salute, approntata dal Regolamento in ambito sanitario, violerebbe il principio di attribuzione delle competenze. Il sistema sanitario, nella definizione del legislatore sovranazionale è composto anche dalle risorse destinate all'assistenza sanitaria, dalle prestazioni di assistenza sanitaria, dalle di modalità di accesso[49]. Il sistema così inteso è finalizzato alla tutela e al miglioramento della salute della persona. Quest'ultimi obiettivi tuttavia

---

tenza il giudice aveva imposto che i nominativi del condannato ed i documenti del processo dovevano rimanere riservati per 10 anni, nonostante il condannato avesse chiesto un periodo di secretazione più lungo. La Corte Edu ha ritenuto che il decennio era breve e violava l'art. 8 della CEDU, poiché la protezione dei dati medici è di fondamentale importanza per il godimento del diritto al rispetto della vita privata e familiare, in particolare quando si tratta di informazioni su infezioni da HIV, a causa della stigmatizzazione derivante da questa condizione in molte società, v. CEDU, 25 febbraio 1997, ricorso n. 22009/93, *Z. c. Finlandia*, §§ 94 e 112. Sentenze 27 agosto 1997, ricorso n. 20837/92, *M. S. c. Svezia;* 10 ottobre 2006, ricorso n. 7508/02, *L. L. c. Francia*; 17 luglio 2008, ricorso n. 20511/03, *I. c. Finlandia*; 28 aprile 2009, ricorso n. 32881/04, *K. H. E altri c. Slovacchia*; 2 giugno 2009, ricorso n. 36936/05, *Szuluk c. Regno Unito*, tutte in *www.echr.coe.int*.

[46] Per la nozione ampia di sanità pubblica v. considerando 54.

[47] CEDU, 25 novembre 2008, ricorso n. 23373/03, *Biriuk c. Lituania*, in *www.echr.coe.int*.

[48] Art. 20.

[49] Considerando 54.

rientrano nella competenza di coordinamento[50], con la conseguenza di attirare nella loro orbita gravitazionale anche la tutela dei dati alla salute, poiché, come detto, essi sono definiti espressamente come connessi alle prestazioni di assistenza sanitaria. In sintesi: poiché i dati sulla salute, per definizione legislativa, sono connessi alle prestazioni sanitarie e le medesime a loro volta sono misure finalizzate al miglioramento della salute; miglioramento che è ricompreso nelle competenze di coordinamento, anche i dati sulla salute vi dovrebbero far parte. Si ricordi che in tale tipologia di competenza l'Unione interviene per "completare" l'azione degli Stati membri non per consentire loro, come stabilito nel Regolamento, di introdurre ulteriori condizioni, comprese le limitazioni.

4. I soggetti destinatari

Il Regolamento designa due categorie di soggetti contrapposti: i primi beneficiari del diritto alla protezione dei dati personali, i secondi destinatari degli obblighi di protezione.

I beneficiari definiti anche come gli interessati[51], sono unicamente le persone fisiche viventi[52], che si trovano nell'Unione[53], a prescindere dalla loro nazionalità o dalla loro residenza[54]. Riprova del valore "uomo"[55] della tutela viene evidenziata in riferimento modalità del consenso al trattamento dei propri dati espresso dal minore (di età compresa tra i 13 ed i 16 anni), nella ipotesi in cui egli sia parte di un contratto. In particolare quando il minore richieda ad una società un servizio erogato a pagamento[56], il consenso al trattamento dei dati è sempre necessario a

[50] Art. 6.1 TFUE.
[51] Art. 3 comma 2.
[52] Art. 1, considerando 14 e 27.
[53] Art. 3 comma 2.
[54] Considerando 2 e 14.
[55] Considerando 4.
[56] Servizio erogato a distanza (fornito senza la presenza simultanea delle parti), per

prescindere dal fatto che la minore età sia una causa di invalidità del negozio sulla base della normativa degli Stati membri[57].

Non sono annoverate, invece, le persone giuridiche. Tuttavia la loro non inclusione nei destinatari del diritto al trattamento non significa che siano sfornite di garanzia europea nella materia *de qua*. La Corte di giustizia nella causa *Volker*[58], riferendosi alla pubblicazione di dati personali relativi ai beneficiari di aiuti agricoli, ha considerato che "*le persone giuridiche possono invocare la tutela degli artt. 7 e 8 della Carta nei confronti di una simile identificazione solamente qualora la ragione sociale della persona giuridica identifichi una o più persone fisiche.* […Il] *rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta,* [è] *riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile […]*". In riferimento ai professionisti i giudici del Lussemburgo nella predetta vicenda hanno stabilito che «*[…] è irrilevante la circostanza che i dati pubblicati attengano ad attività professionali […]. La Corte europea dei diritti dell'uomo ha dichiarato, a tale proposito, con riguardo all'interpretazione dell'art. 8 della CEDU, che l'espressione "vita privata" non deve essere interpretata in modo restrittivo e che "nessun motivo di principio consente di escludere le attività professionali [...] dalla nozione di "vita privata"*».

La Convenzione n. 108, poi, facoltizza le Parti contraenti ad estendere la tutela prevista per le persone fisiche anche alle persone giuridiche.

Per ciò che riguarda il lato passivo, ossia i soggetti obbligati, si individuano due macro aree. Le autorità pubbliche ove vi sono sacche di parziale immunità dal Regolamento, come l'autorità giudiziaria

via elettronica (inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento e di memorizzazione di dati), e mediante trasmissione di dati su richiesta individuale.

[57] Considerando 38; art. 6 comma 1 lett. *a)*; art. 8; art. 4 n. 25.

[58] CGUE, 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, in *Racc.* 2010, I-11063, punti 53, 55 e 59.

nell'esercizio delle proprie funzioni giurisdizionali. L'altra categoria viene individuata nei professionisti[59] e nelle società – siano esse di persone o di capitali – anche se aggregate in gruppi societari costituiti da una controllante e da controllate.

Tutti gli obbligati dal regolamento hanno in comune tre elementi. Innanzitutto il "trattamento", definibile, in generale, come la raccolta, la conservazione e la diffusone dei dati. Esso può essere automatizzato (completamente o parzialmente) oppure manuale[60]. Si noti che rispetto alla direttiva il trattamento comprende attività ulteriori. Viene introdotto, ad esempio, il concetto di "profilazione" cioè l'utilizzo di dati per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute l'ubicazione o la salute della persona. Compare poi la "pseudonimizzazione": i dati personali non possono più essere attribuiti ad una persona specifica senza l'utilizzo di informazione aggiuntive che vengono custodite separatamente. Scompare il termine "congelazione" del dato, sintomatico di perpetuità del trattamento, surrogato dal suo opposto: il diritto alla cancellazione del dato (c.d. diritto all'oblio).

Il secondo elemento è la figura del "titolare del trattamento" ossia il soggetto che stabilisce le finalità ed i mezzi del trattamento dei dati, che nella direttiva veniva definito "responsabile del trattamento". Inoltre esso sarà individuato anche dal diritto dell'Unione o degli Stati membri qualora le finalità ed i mezzi sono stabiliti dal diritto dell'UE o degli Stati membri.

Il terzo elemento è il "responsabile del trattamento" cioè il soggetto munito di competenze tecniche, professionali e organizzative che effettua il trattamento dei dati per conto del titolare del trattamento, sulla base di un contratto, e con possibilità di delega del trattamento se autorizzato[61].

[59] Considerando 18; art. 14 in riferimento al segreto professionale; art. 23 in riferimento alla deontologia.
[60] Considerando 15 e Art. 4.
[61] Artt. 4 e 28.

Sia il titolare che il responsabile del trattamento designano il responsabile della protezione dei dati (*data protection officer*) scelto tra i loro dipendenti o su base di un contratto di servizi, che sarà coinvolto in tutte le attività di trattamento, fornendo a tal fine consulenza ed interfacciandosi con l'autorità pubblica di controllo[62].

5. Ambito di applicazione territoriale

La descrizione delle due categorie di soggetti antagoniste è utile per comprendere l'ambito di applicazione materiale del Regolamento. Occorre ricordare, a tal fine, che i dati personali sono connessi con i beni prodotti/scambiati dall'impresa, con i servizi erogati sia da professionisti sia dalle pubbliche autorità nell'ambito dei loro doveri istituzionali.

Il Regolamento quindi troverà applicazione quando almeno uno dei due protagonisti sia fisicamente presente nel territorio dell'Unione. Evenienza che si può verificare quando il titolare o il responsabile del trattamento sono stabiliti a titolo principale o secondario all'interno dell'Unione europea, indipendentemente dal fatto che il trattamento sia effettuato in territorio *extra* UE. L'altra ipotesi di applicazione si verificherà quando le persone fisiche sono nel territorio dell'UE e sono destinatari di beni o servizi, forniti dal responsabile o dal titolare non stabiliti[63]; come pure quando l'interessato tenga un comportamento monitorato da tali soggetti non presenti. Quest'ultimi designeranno per iscritto un loro rappresentante stabilito nell'UE che avrà il compito di interagire con gli interessati e le autorità nazionali preposte al controllo sul coretto trattamento dei dati[64].

[62] Artt. 37-39.
[63] Considerando 22, 23, 24; art. 3.
[64] Art. 27.

6. I principi generali ed i diritti del proprietario dei dati

Un breve accenno meritano i principi generali stabiliti dal Regolamento, in parte già previsti in parte dalla direttiva. La regola generale è caratterizzata dal fatto che il trattamento dei dati è consentito solo per finalità previste dalla legge statale o europea, e deve essere basato sul consenso espresso generalmente per ciascuna di tali finalità. Tuttavia si ammette il trattamento per una finalità diversa da quella per la quale i dati personali sono stati inizialmente raccolti e non basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, a condizione che il responsabile del trattamento valuti l'esistenza di alcuni indici fissati dal Regolamento[65].

Merita, poi, di essere menzionata la precisazione del principio di minimizzazione dei dati: si richiede che essi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

La liceità del trattamento poggia anch'essa sui medesimi criteri già previsti dalla direttiva[66]. Al riguardo la novità di rilievo è la definizione di "consenso inequivocabile", inteso come manifestazione dell'assenso fornita mediante dichiarazione o azione positiva inequivocabile[67]. Si prevede, inoltre, che qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato lo ha prestato. Se il consenso è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Altrimenti nessuna parte di una tale dichiarazione, in quanto resa in violazione del Regolamento, è vincolante. L'interessato, poi, ha il diritto di revocare il proprio consenso in qualsiasi momento: la revoca opera per il futuro non pregiudicando la

[65] Artt. 5 e 6; art. 6 direttiva.
[66] Art. 6; art. 7 direttiva.
[67] Considerando 32, art. 4 n. 11.

liceità del trattamento basata sul consenso conferito prima della stessa. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto[68]. Si precisa poi che il responsabile del trattamento non è obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del presente regolamento[69].

7. Gli obblighi dei tenutari dei dati

I diritti degli interessati vanno letti anche come corrispondenti obblighi in capo al titolare e/o responsabile del trattamento, poiché questi ultimi hanno una responsabilità generale in merito al rispetto di tali prerogative (*accountability*). Agli obblighi, ricavabili da questa lettura speculare, si devono aggiungere anche quelli specificamente imposti dal Regolamento. Innanzitutto, in ossequio al principio di trasparenza, la persona fisica ha diritto alle informazioni e alle comunicazioni relative al trattamento (in particolare alle finalità e ai soggetti tenuti al trattamento). Notizie che devono essere fornite, per iscritto, dal titolare del trattamento al momento della raccolta; devono poi essere facilmente accessibili e comprensibili, redatte con un linguaggio semplice e chiaro[70]. Rispetto alla direttiva si amplia il novero delle informazioni da fornire sia quando i dati siano raccolti presso la persona fisica[71] sia quando la raccolta non avvenga presso la medesima[72]. Viene potenziato anche il contenuto del diritto

[68] Art. 7.
[69] Art. 10.
[70] Considerando 39, artt. 12, 13 e 14.
[71] Art. 13; art. 10 direttiva.
[72] Art. 14; art. 11 direttiva.

di accesso ai propri dati[73]; si rafforza il diritto di riceve su supporti anche informatici una copia dei propri dati se il trattamento si basava sul consenso; si prevede la possibilità di comandare al titolare il trasferimento di dati direttamente ad altri soggetti (c.d. portabilità)[74]. Vengono introdotti nuovi istituti come il diritto alla rettifica dei dati se inesatti o il diritto di integrarli se incompleti[75]. Si disciplina il nuovo istituto della cancellazione dei dati[76] di origine pretoria.

Per quanto riguarda le misure di protezione, specificamente previste, il Regolamento impone anche al titolare e/o responsabile del trattamento l'adozione di sistemi volti a scongiurare la violazione o i rischi di violazione del trattamento dei dati. Tali soggetti sono tenuti a dare la prova di aver posto in essere concretamente gli strumenti idonei: *onus probandi* alleggerito dall'adesione a codici di condotta o dall'ottenimento di certificazioni rilasciate da apposite autorità[77].

In particolare tra le prescrizioni imposte dal Regolamento, oltre alla tenuta di registri in cui annotare le attività di trattamento[78], si segnala la progettazione di servizi, ossia di misure tecniche e organizzative, per garantire la protezione dei dati sin dal momento del loro trattamento (c.d. *privacy by design*)[79]. L'intento è quello di prevenire una lesione dei dati come illustrata esemplificativamente nel caso *I. c. Finlandia*[80]. La vicenda riguardava una ricorrente che, nel processo interno, non era stata in grado di dimostrare che altri dipendenti dell'ospedale presso cui era impiegata, avevano avuto accesso alle sue cartelle cliniche sanitarie in modo illecito. La violazione del proprio diritto alla protezione dei dati, asserita dalla ricorrente, era stata pertanto respinta dai giudici nazionali. La

[73] Art. 15.
[74] Art. 20.
[75] Art. 16.
[76] Art. 17.
[77] Vedi Capo IV del Regolamento.
[78] Art. 30.
[79] Art. 25.
[80] CCEDU, ricorso n. 20511/03, *I. c. Finlandia*, cit.

Corte EDU, per contro, ha concluso che vi era stata una violazione dell'articolo 8 della CEDU, poiché il sistema dei registri dell'ospedale per la gestione delle cartelle cliniche non consentiva di chiarire retroattivamente quale uso fosse stato fatto dei registri dei pazienti. Infatti il sistema indicava solamente le ultime cinque consultazioni più recenti, le quali venivano cancellate subito dopo il ritorno delle cartelle negli archivi. La Corte EDU ha ritenuto decisivo il fatto che il sistema dei registri, in uso nell'ospedale, fosse stato chiaramente in contrasto con gli obblighi legali previsti dalla normativa nazionale; aspetto che non aveva ricevuto la debita considerazione da parte dei giudici nazionali.

8. Le autorità di controllo

L'osservanza dei diritti (conferiti alle persone) e degli obblighi (imposti alle imprese e pubbliche amministrazioni) si sviluppa su un duplice livello: sul piano domestico viene affidata alle singole autorità di controllo nazionali, alla cui vigilanza si sottraggono le autorità giurisdizionali. Sul territorio dell'intera Unione viene conferita alle autorità di controllo nazionali che cooperano eventualmente con la Commissione attraverso il meccanismo di coerenza.

Per quanto riguarda la vigilanza in ambito nazionale, le autorità (designate e rette dal diritto interno) godono di indipendenza da ogni potere. In caso in cui il titolare del trattamento operi in più Stati membri l'autorità di controllo sarà quella in cui il titolare ha l'amministrazione centrale, cioè lo stabilimento principale (c.d. autorità capofila). Tale autorità collaborerà e coopererà con quelle istituite nei diversi Stati, in cui il titolare ha altri stabilimenti (c.d. autorità interessate), ma sarà l'unica ad emettere una decisione nei confronti del soggetto vigilato e l'unica a cui la persona fisica può presentare un reclamo. Qualora invece la trattazione dei dati è circoscritta in un solo degli Stati membri, l'autorità interessata può emettere la relativa decisione, previa informazione

all'autorità capofila ed a condizione che quest'ultima non decida di avocare a sé la questione (c.d. Meccanismo dello sportello unico). Possibili conflitti tra tali autorità, riguardanti l'adozione di una decisione nei confronti del soggetto vigilato, verranno composti all'interno del "meccanismo di coerenza", ferma *medio tempore* la possibilità dell'autorità interessata di adottare misure d'urgenza, circoscritte al proprio ambito nazionale per la tutela delle persone fisiche[81].

I compiti delle autorità possono essere classificati in informativi, con cui favorisce la consapevolezza in capo agli interessati e ai titolari circa i rispettivi diritti e obblighi; propositivi con cui si agevola l'adozione di codici di condotta ed i meccanismi di certificazione; normativi in senso ampio fornendo consulenza agli Stati per l'adozione di misure legislative in tema di trattamento, adottando le norme vincolanti d'impresa e clausole contrattuali (cioè gli strumenti per trasferire i dati verso organizzazioni internazionali o Paesi terzi), e decidendo sui reclami presentati dall'interessato[82].

Le suddette prerogative vengono realizzate tramite tre tipologie di poteri. In primo luogo con i poteri di indagine che si spingono fino all'accesso nei luoghi del titolare del trattamento ivi inclusi i sistemi di tenuta dei dati. Poteri correttivi che partono dalla diffida all'afflizione di sanzioni amministrative, oltre la possibilità di agire in giudizio per far rispettare il Regolamento. Infine poteri autorizzativi e consultivi come l'accreditamento degli organismi di certificazione e l'approvazione dei codici di condotta. Gli Stati possono ampliare il novero dei poteri delle autorità. Poteri il cui corretto esercizio è sempre garantito dal ricorso giurisdizionale[83].

Le autorità di vigilanza, inoltre, cooperano tra loro scambiandosi informazioni ed esercitando congiuntamente i poteri di cui sono munite, con possibilità di delegare le operazioni all'autorità di vigilanza interessata. Lo Stato membro è tenuto a risarcire i danni causati, nel proprio

[81] Art. 60.
[82] Art. 57.
[83] Art. 58.

territorio, sia dalla sua autorità di vigilanza sia dal personale dell'autorità di controllo ospitato, salvo in quest'ultimo caso il rimborso da parte dello Stato di riferimento.

Al fine di applicare in modo coerente il Regolamento in tutto il territorio dell'Unione è istituito in meccanismo di coerenza per la cooperazione tra le autorità di controllo.

Il meccanismo, tendenzialmente, opera quando il trattamento dei dati riguarda un numero significativo di interessati in vari Stati membri. Infatti tra i suoi compiti rientrano quelli di emettere parerei[84] e comporre le controversie[85]. In un caso il parere viene reso se richiesto della Commissione o da qualsiasi autorità di controllo, quando sia dubbio che una autorità di vigilanza non abbia rispettato gli obblighi relativi all'assistenza reciproca o alle operazioni congiunte. Nell'altro caso il parere, di natura preventiva obbligatoria, viene fornito qualora l'autorità di controllo adotti una misura intesa a produrre effetti giuridici, come nel caso di adozione del codice di condotta indirizzato ad attività in vari Stati membri. In entrambe le evenienze se l'autorità comunica di non uniformarsi al parere si apre la fase di composizione in cui il "meccanismo" deve rendere una decisione vincolante, entro un termine. La decisione vincolante viene resa, come detto, anche in caso di conflitti tra l'autorità capofila e quella interessata.

Il meccanismo opera in concreto tramite il Comitato europeo per la protezione dei dati[86]. Si tratta di un organismo dell'Unione, qualificato come indipendente[87], munito di autonomia statutaria[88], e dotato di personalità giuridica. Per quanto riguardo la sua struttura è composto da un presidente che lo rappresenta. Ne fanno parte anche il Garante europeo della protezione dei dati e la figura di vertice dell'autorità di controllo

[84] Art. 64.
[85] Art. 65.
[86] Sostituisce il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito con direttiva.
[87] Art. 69.
[88] Art. 72.

di ciascuno Stato membro. La Commissione partecipa alle attività del Comitato senza diritto di voto. Il Comitato è assistito da un segretariato messo a disposizione dal Garante europeo della protezione dei dati. Il personale del Garante europeo, impegnato nell'assolvimento dei compiti attribuiti al Comitato, è sottoposto esclusivamente alle istruzioni del presidente del Comitato e deve riferire solo a quest'ultimo.

Il meccanismo di coerenza lungi dall'essere un sistema di regolamentazione di competenze sul controllo, sembra quasi assurgere ad una sorta di nuova istituzione dell'Unione, dotata di ampia discrezionalità valutativa e di azione in riferimento a compiti dai confini piuttosto estesi. Sebbene esso non sia previsto nei Trattati, possiede caratteristiche che lo accomunano con le istituzioni europee. La Corte di giustizia ha avuto modo di precisare[89] che il termine istituzione comprende anche quegli organismi che sebbene non elencati nei Trattati hanno il compito di contribuire alla realizzazione degli scopi dell'Unione con conseguente loro responsabilità extracontrattuale. Il meccanismo soddisfa le statuizioni della Corte, in quanto avendo il compito di applicare in modo coerente il Regolamento in tutto il territorio dell'Unione, ne persegue i fini, vale a dire contribuire alla realizzazione di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche. Inoltre la personalità giuridica di cui è munito lo rende tenuto a risarcire i danni che ha causato nell'adempimento delle competenze eserciate.

La connotazione di istituzione emerge anche dai poteri normativi "in senso lato" in grado di incidere in modo diretto sulla sfera giuridica dei soggetti vigilati. L'assunto trova conforto nella definizione di istituzione che può trarsi dal caso *Van Gend an Loos*[90]. Si è poc'anzi osservato

[89] CGUE, 3 marzo 1988, causa C-85/86, *Commissione c. BEI*, in *Racc.* 1998, p. 01281; 2 dicembre 1992, causa C-370/89, *SGEEM e Etroy c. BEI*, in *Racc*. 1992, p. I-006211.

[90] CGUE, 5 febbraio 1963, causa C- 26/62, *Van Gend en Loos / Administratie der Belastingen* in *Racc*. 1963, p. 0003 "... organi investiti istituzionalmente di poteri

che nel caso di adozione, da parte di una autorità di vigilanza, del codice di condotta che si riferisca ad attività in vari Stati membri, l'autorità deve preventivamente richiedere un parere al Comitato. Questi se ritine il progetto del codice conforme al regolamento trasmette tale parere alla Commissione la quale con atti di esecuzione (procedura d'esame) può conferire al codice validità generale all'interno dell'Unione[91]. Al di là del dato formale dell'atto di esecuzione della Commissione, la valenza normativa del codice risiede a monte nel parere, senza il quale la Commissione non potrebbe attivarsi.

La potestà normativa emerge più chiaramente ponendo mente ai compiti attribuiti al Comitato. Infatti deve emettere un parere – obbligatorio nella richiesta e vincolante nel risultato – sulle norme giuridiche, adottate dall'autorità di controllo nazionale, che disciplinano in modo standardizzato il vincolo tra il titolare ed il responsabile del trattamento[92]. Il potere normativo sembrerebbe conferito anche nel compito di pubblicare le linee guida, le raccomandazioni e le migliori prassi per promuovere l'applicazione coerente del Regolamento[93]: il contenuto di tali strumenti costituirà ragionevolmente l'oggetto della consulenza fornita alla Commissione per le eventuali proposte di modifica del Regolamento[94].

Su un piano più generale, il meccanismo di coerenza, conferma la tendenza del legislatore europeo di avocare a se la regolamentazione di alcune competenze che, in quanto affidate agli Stati membri, generano una tutela frammentata che inficia il corretto funzionamento del mercato. L'intervento legislativo dell'Unione però non esautora completamente i Paesi membri, poiché a causa della complessità della materia, l'Unione non riuscirebbe a verificarne la completa osservanza. A tal fi-

---

sovrani da esercitarsi nei confronti sia degli Stati membri sia dei loro cittadini".
[91] Art. 40.
[92] Art. 28.
[93] Art. 70.1 lett. *e)*.
[94] Art. 70.1 lett. *b)*.

ne il legislatore sovranazionale crea meccanismi caratterizzati non solo da un controllo ripartito tra una autorità centrale europea e le autorità nazionali, ma anche muniti di poteri normativi e di composizione di conflitti insorti tra le stesse[95].

9. Considerazioni conclusive

Dall'analisi delle disposizioni, l'interrogativo se i dati personali risultino maggiormente tutelati, rispetto alla direttiva, non riceve una risposta agevole. Non c'è dubbio che vi sia un aumento delle garanzie, le quali però nel concreto devono essere fornite dall'impresa o dalla pubblica amministrazione. È plausibile, pertanto, che gli obbligati alla protezione dovranno supportare costi per adempiere al Regolamento: la realizzazione di strutture e sistemi interni, l'ottenimento di certificazioni, come pure prestazioni rese da soggetti esterni (es. *data protection officer*). È inoltre ragionevole supporre che le imprese si accolleranno oneri assicurativi per garantirsi da eventuali inadempimenti della normativa europea, forieri di danni. Costi che inevitabilmente verranno scaricati sulla stessa persona fisica in termini di aumento: *i)* dei prezzi dei beni/servizi acquistati (in caso di imprese); *ii)* della tassazione in generale per gli oneri delle pubbliche amministrazioni.

[95] Il riferimento è al Meccanismo unico di vigilanza bancaria. L'Unione europea, infatti, ha trasferito in capo alla BCE, i compiti esclusivi di vigilanza sulla solvibilità e sulla solidità delle banche ed imprese d'investimento significative, ubicate negli Stati della zona euro. L'istituzione europea, a far data dal 4 novembre 2014, esercita tale supervisione, assistita dalle autorità di controllo nazionali (costituite generalmente dalle banche centrali nazionali). La sinergia si svolge all'interno del Meccanismo unico di vigilanza, istituito dal Regolamento UE 1024/2013, e completato dal Regolamento della BCE 468/2014. La supervisione degli enti meno significativi rimane affidata, invece, alla vigilanza delle Autorità nazionali le quali però subiscono diversi gradi interferenza da parte della BCE: dal costante e reciproco scambio di informazioni fino all'assunzione in capo alla stessa della vigilanza, esautorando le Autorità nazionali.

Ad opacizzare il quadro concorre, poi, la possibilità per gli Stati non solo di derogare la disposizione europea, ma anche di fissare l'obbligo giuridico del trattamento.

Il dubbio sul reale effetto utile della normativa e quindi sul rispetto del principio di sussidiarietà, si aggrava, altresì, ponendo mente alla regolamentazione dei trasferimenti dei dati in Paesi *extra* UE, attraverso lo strumento della decisione di adeguatezza[96], in cui l'azione della Commissione rivela, ad oggi, tutta la sua inefficacia. Il riferimento è alle recenti vicende sul trasferimento dei dati negli Stati Uniti. La Corte di giustizia nel 2015[97] aveva annullato il c.d. "*Safe Harbor*", cioè la decisione della Commissione, adottata sulla base della direttiva 95/46, che aveva consentito il trasferimento dei dati negli Stati Uniti, poiché ritenuti capaci di offrire un livello di protezione adeguato, cioè conforme alla normativa europea. Per la Corte, invece, la legislazione americana autorizzava in maniera generale ed indiscriminata la conservazione di tutti i dati personali, trasferiti dall'Unione verso gli Stati Uniti, senza alcuna distinzione, limitazione o eccezione basate sull'obiettivo perseguito, e senza che fosse previsto alcun criterio oggettivo che permettesse di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore per fini precisi, rigorosamente ristretti ed idonei a giustificare tale ingerenza. Né le normative americane prevedevano alcuna possibilità per il cittadino europeo di avvalersi di rimedi giuridici per accedere ai propri dati personali, oppure per ottenerne la rettifica o la soppressione. Le perplessità di conformità agli standard europei permangono, seppur ridotte, nonostante la sostituzione dell'atto annullato, con la de-

[96] Art. 45.

[97] CGUE, 6 ottobre 2015, causa C- 362/14, *Maximillian Schrems* c. *Data Protection Commissioner*, in *ECLI:EU:C:2015:650*. L. Azoulai-M. van der Sluis, *Institutionalizing Personal Data Protection in Time of Global Institutional Distrust: Schrems*, in *Common Market Law Review*, 2016, p. 1343; M. Nino, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia U.E.*, in *Il diritto dell'Unione europea*, 2016, p. 754.

cisione sullo "scudo UE-USA sulla privacy"[98]. Il Parlamento europeo[99] al riguardo rileva come sia rimasta, sebbene circoscritta, una raccolta di massa di dati e di comunicazioni personali di cittadini non statunitensi. Il carattere generalizzato della raccolta non risulta quindi conforme ai più rigorosi criteri di necessità e proporzionalità stabiliti nella Carta di Nizza. Si evidenzia, poi, come gli strumenti di ricorso per la tutela dei cittadini europei sono ancora complessi, necessitando di soluzioni adeguate per rendere la procedura efficace e di semplice utilizzo.

[98] Decisione di esecuzione (UE) 1250/2016 della Commissione, in *GUUE* 1 agosto 2016, L 207/1. F. Rossi Dal Pozzo, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali (dal Safe Harbour al Privacy Shield*), in *Rivista di diritto internazionale*, 2016, p. 617; K. Kowalik-Banczyk. *Les aspects transfrontaliers des infractions à la privée par surveillance de masse de part des agences étatiques*, in *Revue génerele de droit international public*, 2016, p. 383.

[99] Risoluzione del Parlamento europeo del 26 maggio 2016 sui flussi di dati transatlantici (2016/2727 RSP), P8_TA(2016)0223, in *http://www.europarl.europa.eu*.

Fabrizio Marongiu Buonaiuti[1]
Università degli Studi di Macerata

La giurisdizione nelle controversie relative alle attività *on-line*

Abstract: Lo studio ha ad oggetto l'applicazione delle regole sulla competenza giurisdizionale in materia civile e commerciale contenute nel regolamento UE n. 1215/2012 (c.d. "Bruxelles I-*bis*"), con particolare riferimento al foro speciale per le controversie nascenti da fatto illecito, allo specifico contesto della violazione della privacy e dei diritti della personalità commesse tramite Internet. Il lavoro si sofferma innanzitutto sull'adattamento compiuto dalla Corte di giustizia della propria precedente giurisprudenza concernente la diffamazione a mezzo stampa al diverso contesto delle violazioni commesse tramite la diffusione *on-line* di informazioni lesive, per poi raffrontare la soluzione accolta in tale ambito, particolarmente generosa per la parte attrice, che si identifica tendenzialmente con la presunta vittima della violazione, con le soluzioni giurisprudenziali sviluppate relativamente a controversie di natura diversa. Tra queste, rilevano le azioni relative a contratti del commercio elettronico, ovvero a violazioni di diritti di proprietà intellettuale commesse tramite Internet. Il confronto si estende alle regole speciali di giurisdizione recate dal regolamento UE n. 2016/679 in materia di protezione dei dati personali, le quali si presentano ugualmente contrassegnate da un marcato *favor* per il titolare dei dati. Tale orientamento pone inevitabilmente un problema di compatibilità col principio della parità delle armi tra i litiganti, alla luce anche degli ultimi svi-

[1] Il presente lavoro riproduce, con aggiornamenti, la relazione svolta dall'Autore al Convegno "Il Mercato unico digitale", tenutosi il 26 ottobre 2016 presso il Dipartimento di Giurisprudenza dell'Università di Macerata – Centro di documentazione europea, nell'ambito del Progetto nazionale dei CDE italiani 2016 "Un Mercato unico digitale per l'Europa", promosso dalla Rappresentanza in Italia della Commissione europea.

luppi della giurisprudenza della Corte europea dei diritti dell'uomo in materia.

The present study concerns the application of the rules on jurisdiction in civil and commercial matters contained in Regulation EU No. 1215/2012 (s.c. "Brussels Ia") to violations of privacy and personality rights committed through the Web. The study focuses on the adaptation by the ECJ of its case law concerning actions for libel to the context of on-line defamation, commenting on the broad option between alternative fora which is thereby granted to the plaintiff, identified in principle with the alleged victim of defamation or of other violations of personality rights. The solution adopted by the ECJ in this field is compared to those adopted in respect of other actions arising from on-line activities, such as those related to e-commerce transactions or infringements of intellectual property rights via the Web. Lastly, the special rules on jurisdiction introduced by Regulation EU No. 2016/679 concerning the treatment of personal data are taken into consideration. These rules provide in turn a particularly favourable regime in terms of jurisdiction for the data subject, raising in turn the question of the compatibility of granting in such broad terms access to forum actoris with the principle of equality of arms among litigants, in view also of some more recent developments in the case law of the ECtHR in the field concerned.

foro delle violazioni del diritto alla tutela dei dati personali in base al regolamento UE n. 2016/679; 6. Considerazioni conclusive.

1. Il foro delle obbligazioni nascenti da illecito civile nel regolamento n. 1215/2012 nell'interpretazione della Corte di giustizia dell'Unione europea, con particolare riferimento alle violazioni dei diritti della personalità

La giurisdizione nelle controversie di natura civile relative alle attività *on-line*, non diversamente da quanto avviene per le attività corrispondenti che si svolgano in modalità per così dire tradizionale, trova la sua disciplina, nell'ambito dei paesi membri dell'Unione europea, innanzitutto nel regolamento UE n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, meglio noto come regolamento "Bruxelles I-*bis*". Nella sistematica di tale regolamento, non diversamente dal suo predecessore, il regolamento n. 44/2001 o "Bruxelles I" e, ancor prima, dalla Convenzione di Bruxelles del 27 settembre 1968, parallelamente al foro generale del domicilio del convenuto trovano applicazione una serie di fori speciali o alternativi, tra cui, per quanto rileva ai fini del presente studio, il foro relativo alle obbligazioni contrattuali e il foro delle obbligazioni extracontrattuali da fatto illecito. Tali fori sono oggi previsti dall'art. 7 del regolamento n. 1215/2012, rispettivamente al par. 1 e al par. 2, della medesima disposizione[2].

In questa sede, ci si intende concentrare principalmente sulle violazioni dei diritti della personalità commesse a mezzo di Internet, in relazione alle quali rileva in particolare quest'ultimo foro. La norma dell'art. 7, par. 2, del regolamento n. 1215/2012 trova un suo diretto

[2] Regolamento UE n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (rifusione), in G.U.U.E., L 351 del 20 dicembre 2012, p. 1 ss.

precedente nel corrispondente art. 5, par. 3, del regolamento n. 44/2001, così come, benché con alcune differenze nella formulazione delle rispettive disposizioni, nella medesima norma della Convenzione di Bruxelles del 1968. Il foro del fatto illecito, che presenta nella sistematica tanto dei due regolamenti quanto della Convenzione carattere alternativo rispetto al foro del domicilio del convenuto, si basa sul classico criterio del *locus commissi delicti*, che è generalmente impiegato anche al fine dell'individuazione della legge applicabile nella medesima materia[3]. Il riferimento al luogo in cui l'evento dannoso è avvenuto, operato dall'art. 5, n. 3, della Convenzione di Bruxelles del 1968, è stato esteso nella corrispondente disposizione del regolamento n. 44/2001, e così ora nell'art. 7, par. 2, del regolamento n. 1215/2012, al luogo in cui l'evento dannoso può avvenire, allo scopo di rendere la regola applicabile anche relativamente ad eventuali azioni inibitorie nei confronti di attività potenzialmente dannose. Il criterio in questione si è sin dai primi anni di applicazione della Convenzione di Bruxelles del 1968 rivelato foriero di difficoltà interpretative. Sulle principali di queste è sopraggiunto nondimeno l'intervento, spesso chiarificatore benché talvolta, come si dirà, discutibile, della Corte di giustizia europea[4].

Questa ha dapprima chiarito, nella sentenza relativa al caso *Bier c. Mines de Potasse d'Alsace*, che nelle ipotesi di illeciti c.d. a distanza, nei quali il luogo della condotta dannosa e il luogo dell'*eventus damni*

[3] Si confronti l'art. 4, par. 1, del Regolamento CE n. 864/2007 del Parlamento europeo e del Consiglio dell'11 luglio 2007 sulla legge applicabile alle obbligazioni extracontrattuali ("Roma II"), in G.U.U.E., L 199 del 31 luglio 2007, p. 40 ss.; in proposito, tra gli altri, A. Dickinson, *The Rome II Regulation. The Law Applicable to Non-Contractual Obligations*, Oxford, 2008, p. 295 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali nel diritto internazionale privato*, Milano, 2013, p. 108 ss.

[4] La letteratura in materia è molto vasta. Ci si permette di rinviare a F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 15 ss., spec. p. 25 ss.; più recentemente, P. Mankowski, *Article 7*, in Magnus; Mankowski (ed. by), *European Commentaries on Private International Law – ECPIL*, Vol. I – *Brussels Ibis Regulation*, Köln, 2016, p. 314 ss.

non coincidono e sono anzi ubicati in due Stati membri diversi, la regola deve intendersi come riferibile tanto al luogo in cui è stata posta in essere la condotta dannosa quanto al luogo in cui si è verificato l'evento dannoso[5]. Ciò nell'ottica, espressamente dichiarata, di voler offrire all'attore, in un sistema basato su di un concorso tra fori alternativi, più ampie possibilità di accesso ad un giudice munito di giurisdizione al fine della trattazione della domanda. In proposito, per quanto la soluzione accolta dalla Corte di giustizia possa apparire incline a favorire eventuali manovre di *forum shopping* da parte dell'attore, deve ritenersi che, a meglio considerare, uno dei due fori così individuati, e sovente, in casi come quello oggetto della sentenza richiamata della Corte di giustizia, il foro del luogo della condotta, viene a coincidere col foro generale del domicilio del convenuto. Inoltre, deve rilevarsi che l'opzione che la Corte di giustizia ha in questo modo lasciato aperta all'attore cade nell'un caso come nell'altro su fori che presentano un collegamento effettivo con la controversia, al punto da non creare sostanziali problemi in termini di prevedibilità della competenza giurisdizionale da parte del convenuto e, pertanto, di parità delle armi tra i litiganti quanto alla determinazione della competenza giurisdizionale[6].

Nei successivi sviluppi della propria giurisprudenza relativa al foro del fatto illecito la Corte di giustizia si è, peraltro, sforzata di contenere

[5] CGCE, 30 novembre 1976, in causa 21/76, *Bier c. Mines de potasse d'Alsace*, in *Raccolta*, 1976, p. 1735 ss., punti 13 ss. della motivazione.

[6] Si vedano in proposito, per tutti, A. Davì, *La responsabilità extracontrattuale nel nuovo diritto internazionale privato italiano*, Torino, 1997, p. 108 ss.; K. Kerameus, *La compétence internationale en matière delictuelle dans la Convention de Bruxelles*, in *Travaux du Comité français de droit intern. privé*, 1992-1993, Paris, 1994, p. 255 ss., spec. p. 257 ss.; L. Mari, *Il diritto processuale civile della convenzione di Bruxelles*, I, *Il sistema della competenza*, Padova, 1999, p. 388 ss.; con riferimento all'incidenza della prevedibilità della competenza giurisdizionale sul diritto delle parti alla tutela giurisdizionale si rinvia a F. Marongiu Buonaiuti, *La tutela del diritto di accesso alla giustizia e della parità delle armi tra i litiganti nella proposta di revisione del regolamento n. 44/2001*, in Di Stefano; Sapienza (a cura di), *La tutela dei diritti umani e il diritto internazionale*, XVI Convegno SIDI, Catania, 23-24 giugno 2011, Napoli, 2012, p. 345 ss., spec. p. 348 ss.

l'incentivo al *forum shopping* e il margine di imprevedibilità insito in un'interpretazione eccessivamente ampia del criterio di competenza giurisdizionale in questione. La Corte ha infatti precisato, nelle proprie sentenze relative ai casi *Dumez France e Tracoba c. Hessische Landesbank*[7] e *Marinari c. Lloyd's Bank*[8], nonché, più recentemente, *Kronhofer c. Maier*[9], che, per luogo dell'evento dannoso, ai fini della regola in questione, deve intendersi il luogo di produzione del danno inizialmente provocato dal fatto illecito, a prescindere dai luoghi eventualmente diversi nei quali si siano prodotte le conseguenze indirette o ulteriori del fatto stesso, e ciò indipendentemente dal fatto che tali ulteriori conseguenze si siano prodotte sullo stesso soggetto inizialmente danneggiato ovvero su altri soggetti[10].

Di particolare rilevanza ai fini del presente studio è l'interpretazione data dalla Corte di giustizia alla regola del *forum delicti*, come al tempo contenuta nella Convenzione di Bruxelles del 1968, in relazione all'ipotesi di azioni risarcitorie per diffamazione a mezzo stampa. Infatti, tale interpretazione, come si avrà modo di osservare specificamente più avanti, ha costituito il modello ispiratore per la soluzione interpretativa più recentemente accolta dalla Corte stessa con riferimento alle violazioni dei diritti della personalità commesse a mezzo di Internet[11]. Nella propria sentenza relativa alla causa *Shevill c. Presse Alliance*, infatti, la Cor-

[7] CGCE, 11 gennaio 1990, in causa 220/88, *Dumez France e Tracoba c. Hessische Landesbank*, in *Raccolta*, 1990, p. I-49 ss., punti 13 ss. della motivazione.
[8] CGCE, 19 settembre 1995, in causa C-364/93, *Marinari c. Lloyd's Bank*, in *Raccolta*, 1995, p. I-2719 ss., punti 10 ss. della motivazione.
[9] CGCE, 10 giugno 2004, in causa C-168/02, *Kronhofer c. Maier et al.*, in *Raccolta*, 2004, p. I-6009 ss., punti 18 ss. della motivazione.
[10] Si vedano in proposito A. Davì, *La responsabilità extracontrattuale*, cit., p. 110 ss.; ID., *Der italienische Kassationshof und der Gerichtsstand des Ortes des schädingenden Ereignisses nach Art. 5 Nr. 3 EuGVÜ bei reinen Vermögensschäden*, in *IPRax – Praxis des internationalen Privat- und Verfahrensrecht*, 1999, p. 484 ss.; M. Lehmann, *Where Does Economic Loss Occur?*, in *Journal of Private International Law*, 2011, p. 527 ss., spec. p. 538 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 23 ss.
[11] Si veda in proposito *infra*, par. 2.

te di giustizia ha configurato implicitamente l'illecito consistente nella diffamazione a mezzo stampa alla stregua di una forma *sui generis* di illecito plurilocalizzato. Conseguentemente, ha affermato che il criterio in questione potesse giustificare la competenza giurisdizionale, in alternativa ai giudici del domicilio del convenuto secondo la regola generale, dei giudici del luogo di stabilimento dell'editore della pubblicazione diffamatoria, che appare da identificarsi come sostanzialmente corrispondente al luogo della condotta dannosa laddove questo non coincida col luogo di produzione del danno. Come ulteriore alternativa offerta all'attore, la Corte ha ritenuto il criterio in questione atto a fondare la competenza giurisdizionale dei giudici del diverso luogo, o, meglio, dei diversi luoghi, in cui la pubblicazione diffamatoria sia stata successivamente diffusa, da identificarsi più nettamente come luogo, ovvero luoghi, di produzione dell'*eventus damni*[12]. La Corte di giustizia ha, in realtà, subordinato la riferibilità del criterio in questione al luogo ovvero ai luoghi di ulteriore diffusione della pubblicazione diffamatoria alla condizione che l'attore, che viene in questo caso identificato col soggetto che si pretende leso, possa dimostrare di aver subito un pregiudizio per la propria reputazione nel singolo Stato membro considerato. Corrispondentemente, la competenza giurisdizionale di questi ultimi giudici sarà limitata alle azioni risarcitorie relative ai danni prodottisi nel rispettivo Stato membro, mentre i giudici del luogo di stabilimento dell'editore della pubblicazione diffamatoria avranno competenza a giudicare dell'intero danno causato dalla pubblicazione diffamatoria. La soluzione accolta in proposito dalla Corte di giustizia, definita dalla dottrina in termini di *Mosaikbetrachtung* ovvero trattamento a mosaico, presenta l'innegabile vantaggio di favorire la concentrazione del contenzioso innanzi al giudice del luogo di stabilimento dell'editore. Si viene a limitare, in questo modo, l'incentivo al *fo-*

[12] CGCE, 7 marzo 1995, in causa C-68/93, *Fiona Shevill et al. c. Presse Alliance SA*, in *Raccolta*, 1995, p. I-415 ss. Si vedano in proposito, tra gli altri, A. Davì, *La responsabilità extracontrattuale*, cit., p. 31, 111 ss.; L. Mari, *Il diritto processuale civile*, cit., p. 378 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 25 ss.

rum shopping che sarebbe inevitabilmente stato insito nel consentire l'esercizio di una competenza giurisdizionale sull'intero danno causato dalla pubblicazione diffamatoria da parte dei giudici di ogni Stato membro in cui il soggetto che si pretenda leso potesse asserire di aver subito una lesione della propria reputazione. Nondimeno, questa soluzione presenta l'innegabile limite di non riuscire del tutto ad evitare una frammentazione del contenzioso che può scaturire da una medesima pubblicazione diffamatoria. Un rimedio non sempre risolutivo a questa frammentazione potrà provenire dalle regole contenute nel regolamento Bruxelles I-*bis*, così come già nel regolamento Bruxelles I ovvero inizialmente nella Convenzione di Bruxelles, in materia di coordinamento tra procedimenti paralleli pendenti innanzi a giudici di Stati membri diversi[13].

2. L'adattamento di tale interpretazione giurisprudenziale allo specifico contesto delle violazioni commesse tramite Internet

La soluzione interpretativa elaborata dalla Corte di giustizia relativamente alla disciplina del foro del fatto illecito con riferimento ad azioni risarcitorie traenti la loro origine da diffamazione a mezzo stampa ha in tempi più recenti formato oggetto di una delicata operazione di adattamento al diverso contesto della diffamazione, ovvero di altra violazione di diritti della personalità, avvenuta tramite Internet. Nella sentenza *eDate Advertising* e *Martinez*[14], la Corte di giustizia ha ritenuto di

[13] Con riferimento alle quali si rimanda a F. Marongiu Buonaiuti, *Litispendenza e connessione internazionale. Strumenti di coordinamento tra giurisdizioni statali in materia civile*, Napoli, 2008, spec., con riferimento alla disciplina in materia come contenuta nel regolamento n. 44/2001 ("Bruxelles I"), p. 166 ss.; con riferimento alle innovazioni introdotte in materia dal regolamento n. 1215/2012 ("Bruxelles I-*bis*"), ID., *Per una prima lettura del regolamento «Bruxelles I-bis»: il nuovo regime della litispendenza e della connessione privativa*, scritto pubblicato il 19 dicembre 2012 sul sito *http://aldricus.com*.

[14] CGUE, 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *e-Date Advertising GmbH c. X, Martinez c. MGN Ltd*, in *Raccolta*, 2011, p. I-10269 ss.; in proposito,

dover riadattare la soluzione interpretativa formulata nella sentenza *Shevill* in considerazione della sensibile differenza del contesto relativo ad una pubblicazione *on-line* rispetto ad una pubblicazione tradizionale. In proposito, la Corte di giustizia ha ritenuto anzitutto di dover mantenere fermo il riferimento al luogo di stabilimento dell'editore della pubblicazione. A tale riguardo, a dire il vero, la Corte ha fatto riferimento al luogo di stabilimento del soggetto emittente dei contenuti *on-line*, come tale sembrando doversi identificare essenzialmente il c.d. *content provider*, vale a dire colui che "posta" su di un sito *web* l'informazione lesiva, piuttosto che il c.d. *service provider*, che spesso si limita a mettere a disposizione la piattaforma informatica sulla quale l'informazione viene pubblicata. Ciò per quanto variabile possa essere, a seconda delle caratteristiche del sito *web* sul quale l'informazione lesiva è pubblicata, il grado di controllo e corrispondentemente di responsabilità del gestore del sito in relazione al contenuto delle informazioni che vi vengono pubblicate[15]. Il luogo di stabilimento dell'emittente l'informazione lesiva rileverà anche in questo contesto come tendenzialmente coincidente col luogo della condotta dannosa, se non anche col luogo di produzione dell'*eventus damni*, e potrà ugualmente coincidere, sempre nel caso di un'azione promossa dal presunto danneggiato, col foro generale del domicilio del convenuto.

La Corte di giustizia ha ampiamente sottolineato la difficoltà insita nell'applicazione del criterio parallelo del luogo, ovvero dei luoghi, di diffusione della pubblicazione lesiva, che era stato concepito in funzio-

---

si vedano O. Feraci, *Diffamazione internazionale a mezzo di Internet: quale foro competente? Alcune considerazioni sulla sentenza* eDate, in *Rivista di diritto internazionale*, 2012, p. 461 ss.; G. Guiziou, nota in *Journal du droit international*, 2012, p. 201 ss.; S. Marino, *La violazione dei diritti della personalità nella cooperazione giudiziaria civile europea*, in *Rivista di diritto internazionale privato e processuale*, 2012, p. 363 ss.

[15] Si veda al riguardo E. Gabellini, *La competenza giurisdizionale nel caso di lesione di un diritto della personalità attraverso Internet*, in *Riv. trim. dir. proc. civ.*, 2014, p. 271 ss., spec. p. 283 ss.

ne della diffamazione a mezzo stampa, al diverso contesto della pubblicazione *on-line*. In quest'ultimo contesto, infatti, appare difettare il presupposto implicito del controllo da parte dell'editore/emittente sulla diffusione dell'informazione pubblicata. Come rilevato dalla Corte, le informazioni pubblicate su un sito *web* il cui accesso sia libero sono per loro natura immediatamente visualizzabili da qualsiasi parte del mondo indipendentemente da una specifica intenzione dell'emittente di indirizzare tali informazioni verso utenti collocati in uno o più paesi ovvero aree geografiche[16]. Ciò nondimeno, tale intrinseca differenziazione del contesto della pubblicazione *on-line* da quello della pubblicazione tradizionale a mezzo stampa non è stata ritenuta sufficiente dalla Corte per abbandonare la soluzione della *Mosaikbetrachtung*, che era stata concepita per quest'ultimo contesto. Onde contenere il rischio di un altrimenti potenzialmente illimitato assoggettamento dell'emittente l'informazione lesiva alla giurisdizione dei giudici di qualsiasi Stato membro rimane ovviamente fermo, nella soluzione accolta dalla Corte di giustizia anche relativamente al contesto *on-line*, il presupposto implicito del doversi trattare di Stati in cui il soggetto che si pretende leso possa dimostrare di aver subito, o di paventare, una lesione della propria reputazione. Ne consegue la limitazione della competenza dei giudici così designati ai soli danni che il soggetto asseritamente leso possa dimostrare di aver subito nel paese del giudice adito[17]. Tale limitazione ripropone, pur sempre le difficoltà applicative che già si sono sottolineate relativamente all'applicazione di questo criterio nel contesto della pubblicazione tradizionale a mezzo stampa[18].

Una ragionevole limitazione dell'applicazione della *Mosaikbetrachtung* nel contesto considerato alle sole azioni di carattere strettamente

[16] CGUE, 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *e-Date Advertising GmbH c. X, Martinez c. MGN Ltd*, cit., par. 45.
[17] *Ibidem*, par. 52.
[18] Difficoltà applicative il cui acuirsi relativamente alle pubblicazioni diffuse tramite Internet è peraltro riconosciuto dalla stessa CGUE, *ibidem*, par. 46 ss.

risarcitorio è giunta dalla più recente sentenza *Bolagsupplysningen* della Corte di giustizia[19]. In quest'ultima sentenza, la Corte ha escluso che azioni volte non già al risarcimento del danno, bensì alla rettifica ovvero alla cancellazione di informazioni diffamatorie pubblicate tramite Internet possano proporsi innanzi ai giudici dei diversi Stati membri dai quali tale informazioni siano o siano state accessibili e abbiano causato danno alla reputazione della persona interessata, secondo la soluzione ammessa nella sentenza *eDate* per le azioni di carattere risarcitorio[20]. Infatti, diversamente da un'azione risarcitoria che potrebbe in linea di principio, pur con le difficoltà applicative evidenziate, limitarsi ai danni concretamente prodottisi in un dato paese, un'azione volta alla rettifica o cancellazione di determinate informazioni pubblicate su Internet, in considerazione dell'effetto ubiquitario che tale rettifica o cancellazione produrrebbe, non può che proporsi innanzi ai giudici competenti a pronunciarsi sul risarcimento dell'intero danno causato[21].

La differenza del contesto proprio della pubblicazione *on-line* della notizia diffamatoria rispetto alla tradizionale pubblicazione a mezzo stampa è stata invece ritenuta dalla Corte giustificare l'individuazione di un diverso criterio di localizzazione del luogo di produzione dell'*eventus damni*, destinato ad operare in alternativa agli altri già contemplati secondo la logica propria della precedente pronuncia. Tale criterio si riferisce al luogo in cui la presunta vittima della diffamazione ovvero della lesione del diritto della personalità avvenuta a mezzo di Internet ha il proprio centro degli interessi. La Corte di giustizia ha giustificato il ricorso a tale criterio avendo riguardo, per un verso, all'intrinseca ubiquità dei contenuti messi a disposizione tramite Internet e, per altro verso, alla conseguente maggiore lesività di una pubbli-

[19] CGUE, 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ilsjan c. Svensk Handel AB*, ECLI:EU:C:2017:766, par. 45 ss.
[20] *Ibidem*, par. 47.
[21] *Ibidem*, parr. 48-49.

cazione *on-line* per il soggetto danneggiato dalla notizia diffamatoria[22]. La Corte ha invocato, a sostegno dell'accoglimento di questo ulteriore criterio, argomentazioni attinenti al buon funzionamento della giustizia, in considerazione del fatto che il giudice del luogo in cui la presunta vittima della diffamazione o di altra violazione dei diritti della personalità ha il proprio centro d'interessi si trova in una posizione di particolare prossimità rispetto alla sfera giuridica del danneggiato. Essa si è spinta ad affermare che tale criterio si rivela inoltre rispettoso della parità delle armi tra i litiganti, in quanto è atto ad assicurare la prevedibilità, da parte del convenuto, come tale identificandosi il soggetto asseritamente responsabile, del foro innanzi al quale egli potrà essere citato, sul presupposto che l'autore della pubblicazione diffamatoria debba normalmente conoscere il luogo in cui la persona oggetto della pubblicazione stessa ha il proprio centro di interessi[23].

A questo riguardo, non può farsi a meno di osservare che la prevedibilità del luogo del centro degli interessi della persona oggetto della pubblicazione diffamatoria o altrimenti lesiva dei suoi diritti della personalità non può ritenersi in tutti i casi assicurata, particolarmente quando non si tratti di persona di particolare notorietà[24], ovvero si tratti di una persona che è menzionata incidentalmente nel dare conto di una vicenda nella quale è coinvolta una pluralità di soggetti. Non può infatti darsi per scontato che l'autore della pubblicazione abbia svolto indagini in ordine al centro degli interessi di ciascuna delle persone coinvolte, anche solo marginalmente, nella vicenda riportata. Per di più, non può farsi a meno di osservare che la stessa individuazione del centro di interessi della persona che si pretenda vittima di diffamazione o di altra le-

[22] CGUE, 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *e-Date Advertising GmbH c. X, Martinez c. MGN Ltd*, cit., par. 47 ss.
[23] *Ibidem*, par. 50, con riferimento a CGCE, 23 aprile 2009, in causa C-533/07; *Falco Privatstiftung e Rabitsch*, in *Raccolta*, 2009, p. I-3327 ss., par. 22; CGUE, 12 maggio 2011, in causa C-144/10, *BVG*, in *Raccolta*, 2011, p. I-3961 ss., par. 33.
[24] Si rimanda a quanto osservato in proposito in F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 27 ss.

sione dei diritti della personalità per effetto della pubblicazione *on-line* potrebbe rivelarsi problematica, in quanto non si tratta di un criterio di carattere strettamente giuridico, quale potrebbe essere la residenza o il domicilio, come tale determinabile con sufficiente certezza, bensì di un criterio di carattere fattuale. Il criterio in questione, pur presentandosi certamente strumentale ad assicurare un collegamento effettivo tra il foro e la controversia, nondimeno può presentare dei margini di incertezza quanto alla sua effettiva localizzazione. Ciò particolarmente nei casi in cui la persona oggetto della pubblicazione asseritamente diffamatoria o altrimenti lesiva sia persona che conduca una vita di carattere internazionale, che presenti elementi atti a ricollegarla in maniera sostanziale con più di un paese. In proposito, la Corte stessa è parsa ammettere la possibilità che il criterio del centro di interessi della persona asseritamente lesa possa in alcuni casi rivelarsi di incerta localizzazione, nella parte della motivazione della sentenza *eDate* in cui ha precisato che normalmente il centro degli interessi di una persona fisica deve ritenersi corrispondente al luogo in cui questa ha la propria residenza abituale. Quest'ultimo criterio, come è noto, può rivelarsi a sua volta di incerta localizzazione, particolarmente nel caso evocato di persone che dividano la propria vita tra più paesi. L'elemento di incertezza insito nel criterio del centro degli interessi del soggetto leso è peraltro evidenziato dalla Corte stessa, nel sottolineare che questo possa risultare eventualmente localizzato in un paese diverso da quello in cui il soggetto in questione ha la propria residenza abituale, col quale il medesimo possa presentare dei legami particolarmente stretti in ragione, tra l'altro, della propria attività professionale[25].

La Corte di giustizia è ritornata sulla questione della localizzazione del centro degli interessi del soggetto che abbia subito una lesione dei propri diritti della personalità per effetto di informazioni pubblicate tramite Internet nella più recente sentenza *Bolagsupplysningen*, nella

[25] CGUE, 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *e-Date Advertising GmbH c. X, Martinez c. MGN Ltd*, cit., par. 49.

quale ha esaminato le problematiche poste dall'applicazione di tale criterio con riferimento a una persona giuridica[26]. Riflettendo anche in questa ipotesi l'esistenza di un margine di incertezza quanto alla localizzazione del criterio in esame, la Corte di giustizia ha affermato che il centro degli interessi di una persona giuridica ai fini di un'azione traente origine dalla pubblicazione di informazioni diffamatorie debba ritenersi localizzato nel paese nel quale la persona giuridica goda di una più solida reputazione commerciale, e debba conseguentemente essere determinato sulla base del luogo nel quale questa svolga la parte essenziale della propria attività economica[27]. Evidenziando ancora una volta il carattere intrinsecamente fattuale del criterio in esame, la Corte di giustizia ha affermato che per quanto esso possa coincidere col paese nel quale la persona giuridica ha la propria sede statutaria, nondimeno nelle ipotesi in cui questa svolga la parte prevalente della propria attività in uno Stato membro diverso da quello in cui è ubicata la propria sede statutaria, il suo centro degli interessi debba ritenersi ubicato in tale diverso paese[28].

Come la Corte di giustizia è parsa rilevare, il luogo di prevalente svolgimento dell'attività economica della persona giuridica che si pretende lesa rileverà, nei casi in cui non coincida con la sua sede statutaria, come luogo di concretizzazione del danno causato dalle informazioni pubblicate tramite Internet[29]. La conclusione alla quale la Corte di giustizia è giunta sul punto non si segnala per esemplare chiarezza, parendo voler riferire solo a quest'ultima ipotesi la coincidenza del centro degli interessi della persona giuridica col luogo di concretizzazione del danno. Deve invece ritenersi maggiormente coerente con l'intera argomentazione svolta dalla Corte di giustizia, anche con riferimento alla

[26] CGUE, 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ilsjan c. Svensk Handel AB*, cit., par. 22 ss.
[27] *Ibidem*, par. 41.
[28] *Ibidem*, par. 42.
[29] *Ibidem*, par. 44.

precedente sentenza *eDate* dalla quale la Corte non è parsa volersi discostare, affermare che il centro degli interessi della persona giuridica che si pretende lesa rilevi in ogni caso, nell'ottica adottata dalla Corte stessa, come luogo di concretizzazione dell'*eventus damni*[30]. Ciò a prescindere dal fatto che esso coincida o meno, sulla base di una valutazione di carattere fattuale, col luogo in cui la persona giuridica ha la propria sede statutaria.

La tendenziale irrilevanza della localizzazione di quest'ultima, ove non coincidente col luogo di prevalente svolgimento dell'attività economica della persona giuridica, è peraltro sottolineata dalla Corte di giustizia, nel passo della motivazione della sentenza in esame nel quale esclude l'invocabilità, ai fini un risarcimento integrale, del criterio di cui all'art. 7, n. 2, del regolamento n. 1215/2012 a titolo di luogo di concretizzazione dell'*eventus damni* nei casi in cui non emerga una localizzazione preponderante dell'attività economica della persona giuridica che si pretende lesa in un determinato Stato membro[31]. Sembra doversi leggere tra le righe di quanto affermato dalla Corte di giustizia che in casi questo genere, in cui in altre parole il centro degli interessi della persona lesa non possa essere determinato, rimarrebbe aperta alla persona giuridica in questione l'alternativa tra l'agire dinanzi al foro generale del domicilio del convenuto e l'agire, a fini puramente risarcitori, davanti ai giudici dei singoli Stati membri dove possa dimostrare di aver subito una lesione della propria reputazione locale, limitatamente ai danni subiti in ciascuno di tali paesi. In questi limiti potrebbe ancora sussistere un limitato spazio per la *Mosaikbetrachtung* che la Corte stessa, in altra parte della stessa sentenza, ha condivisibilmente escluso

[30] Si veda in questo senso, assai sinteticamente, E. Márton, *CJEU on the place of the damage under Article 7(2) of Brussels I*a *as regards violations of personality rights of a legal person*, scritto pubblicato su http://conflictoflaws.net, 8 novembre 2017.

[31] CGUE, 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ilsjan c. Svensk Handel AB*, cit., par. 43.

relativamente alle azioni volte non già al risarcimento, bensì alla rettifica ovvero alla cancellazione delle informazioni diffamatorie[32].

Alle perplessità che si sono esposte con riferimento al margine di incertezza insito nella localizzazione del centro degli interessi della persona che si pretende lesa, con le inevitabili ricadute sulla prevedibilità della competenza giurisdizionale da parte dell'autore della pubblicazione asseritamente lesiva, altre se ne possono aggiungere relativamente al complessivo equilibrio delle armi tra i litiganti. Questo rischia di essere messo a repentaglio, per un verso, dalla previsione di un ventaglio eccessivamente ampio di fori alternativi a disposizione della parte attrice[33], per quanto questa possa eventualmente anche non coincidere con il danneggiato[34]. Per altro verso, la parità delle armi tra i litiganti

[32] Si veda *supra*, in questo paragrafo, testo in corrispondenza delle note 18-20.

[33] Si rimanda alle considerazioni svolte in proposito, in termini generali, in F. Marongiu Buonaiuti, *La tutela del diritto di accesso alla giustizia e della parità delle armi tra i litiganti*, cit., p. 348 ss. e, con riferimento al caso in esame, in ID., *Le obbligazioni non contrattuali*, cit., p. 27 ss.; sulla problematica anche, tra gli altri, P. Kinsch, *Droits de l'homme, droits fondamentaux et droit international privé*, in *Rec. des Cours*, vol. 318, 2005, p. 9 ss., spec. p. 65 ss.; F. Marchadier, *Les objectives généraux du droit international privé à l'épreuve de la Convention européenne des droits de l'homme*, Bruxelles, 2007, p. 183 ss., spec. p. 190 ss.; in precedenza, tra gli altri, P. Schlosser, *Jurisdiction in International Litigation - The Issue of Human Rights in Relation to National Law and to the Brussels Convention*, in *Rivista di diritto internazionale*, 1991, p. 5 ss.; R. Geimer, *Verfassung, Völkerrecht und internationales Zivilverfahrensrecht*, in *Zeitschrift für Rechtsvergleichung*, 1992, p. 321 ss. e 401 ss.; Th. Pfeiffer, *Internationale Zuständigkeit und prozessuale Gerechtigkeit*, Frankfurt am Main, 1995, p. 523 ss.; C. Focarelli, *The Right of Aliens Not to be Subject to So-Called "Excessive" Civil Jurisdiction*, in Conforti; Francioni (ed. by), *Enforcing International Human Rights in Domestic Courts*, The Hague, 1997, p. 441 ss.; J. Bertele, *Souveränität und Verfahrensrecht. Eine Untersuchung der aus dem Völkerrecht ableitbaren Grenzen staatlicher extraterritorialer Jurisdiktion im Verfahrensrecht*, Tübingen, 1998, p. 221 ss.

[34] Si veda, nel senso dell'applicabilità del criterio speciale contemplato al tempo dall'art. 5, n. 3 del regolamento n. 44/2001 ad azioni di accertamento negativo della responsabilità per fatto illecito, con particolare riferimento alle violazioni di norme in materia di concorrenza, CGUE, 25 ottobre 2012, in causa C-133/11, *Folien Fischer AG c. Ritrama s.p.a.*, ECLI:EU:C:2012:664, par. 41 ss., massima in *Rivista di diritto internazionale privato e processuale*, 2012, p. 964 s.; in *Revue*

rischia di essere pregiudicata dall'ammissione di un sostanziale *forum actoris* nell'ipotesi, tendenzialmente più frequente, in cui ad agire sia invero la persona che si pretende lesa nei suoi diritti della personalità dalla pubblicazione diffusa tramite Internet[35]. A questo riguardo, appare scarsamente convincente l'argomentazione fatta propria dalla Corte di giustizia per la quale la previsione di un foro alternativo, localizzato nel luogo in cui la persona che si pretende lesa ha il proprio centro di interessi, trova giustificazione nella particolare capacità lesiva che una pubblicazione *on-line* possiede rispetto ad una a mezzo stampa. Ciò avuto riguardo al fatto che se, da una parte, è un dato sufficientemente acquisito che le informazioni pubblicate in libero accesso su Internet sono potenzialmente accessibili da qualsiasi parte del mondo, eccettuati, evidentemente, quei paesi nei quali vigano limitazioni nell'accesso alla rete o ai materiali pubblicati su determinati siti, per altro verso alcuni fattori come la lingua e la rilevanza del sito su cui l'informazione è pubblicata possono in concreto incidere sulla effettiva probabilità che l'informazione stessa sia effettivamente consultata da un numero significativo di utenti della rete localizzati in un consistente numero di Stati diversi. Inoltre, appare doversi osservare che l'argomentazione sulla quale la Corte si è basata appare maggiormente pertinente nel senso di ridurre, se non escludere del tutto, la rilevanza dell'elemento della diffusione della pubblicazione diffamatoria o altrimenti lesiva, posto che è proprio su quest'ultimo che le ben diverse modalità di circolazione proprie delle pubblicazioni *on-line* sono suscettibili di andare ad incidere[36]. Tale elemento, invece, continua ad essere accolto nell'interpretazione accolta dalla Corte nella propria giurisprudenza[37], venendo escluso so-

critique de droit international privé, 2013, p. 501 ss., nota di H. Muir-Watt, ivi, p. 506 ss.

[35] CGUE, 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *e-Date Advertising GmbH c. X, Martinez c. MGN Ltd*, cit., par. 48.

[36] Come la Corte, peraltro, non manca di sottolineare, *ibidem*, par. 46.

[37] *Ibidem*, par. 52.

lamente nei casi in cui la natura dell'azione esperita non consenta di tenerne conto[38].

In definitiva, la valutazione operata dalla Corte nel senso di prevedere, sostanzialmente a favore della vittima, o presunta tale, di una diffamazione od altra lesione di un diritto della personalità commessa *on-line*, la possibilità di agire davanti al giudice del luogo in cui è situato il proprio centri di interessi rischia in ultima analisi di creare una discriminazione eccessiva e, pertanto, irragionevole, rispetto alle opzioni offerte secondo la sentenza *Shevill*, a chi si pretenda vittima di lesioni analoghe per effetto di una pubblicazione cartacea. Inoltre, dalla prospettiva dell'emittente dell'informazione asseritamente lesiva, l'interpretazione accolta dalla Corte rischia di sottoporre il *content provider* a un c.d. *litigation risk* ben più gravoso, in termini di ampiezza del novero dei giudici innanzi ai quali potrà essere citato da parte di chi si pretenda leso dalla pubblicazione, rispetto a quanto avverrebbe per chi pubblichi analoghe informazioni a mezzo stampa[39]. Peraltro, deve essere osservato che l'ampiezza del novero di fori alternativi dischiusa dall'interpretazione accolta dalla Corte di giustizia relativamente ad azioni per diffamazione od altre violazioni dei diritti della personalità causate da pubblicazioni *on-line* appare offrire un indebito incentivo al *forum shopping*. Quest'ultimo è alimentato dalla circostanza che, relativamente alla materia delle violazioni della *privacy* e dei diritti della personalità, non trovano applicazione le regole uniformi sull'individuazione della legge applicabile contenute nel regolamento "Roma II", con la conseguente sussistenza in questa materia, almeno fino ad un'auspicata revisione di quest'ultimo regolamento, di regole non coincidenti nei diversi sistemi

[38] CGUE, 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ e Ilsjan c. Svensk Handel AB*, cit., parr. 48-49.

[39] Si vedano al riguardo i rilievi di O. Feraci O., *Diffamazione internazionale a mezzo di Internet*, cit., p.467 s.; G. Guiziou, nota, cit., p. 202 ss.; S. Marino, *La violazione dei diritti della personalità*, cit., p. 366 ss.; nonché quanto osservato in F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 26 ss.

nazionali di diritto internazionale privato degli Stati membri[40]. La rilevanza di quest'ultimo problema è naturalmente acuita dalla parallela diversità della disciplina sostanziale in materia nei diversi Stati membri, potendosi osservare, banalmente, che non vi è omogeneità tra i presupposti in presenza dei quali una pubblicazione possa essere ritenuta diffamatoria, con particolare riferimento alla veridicità dell'informazione diffusa. Se questa disparità di trattamento sotto il profilo della giurisdizione può per certi versi apparire giustificata in un'ottica di politica del diritto, nel senso di stimolare una maggiore responsabilizzazione degli emittenti di contenuti *on-line* quanto al controllo della correttezza delle informazioni pubblicate a mezzo della rete e all'assenza al loro interno di contenuti lesivi della sfera personale delle persone interessate, nondimeno essa si presenta, dal punto di vista della corretta allocazione della competenza giurisdizionale, come ingiustificata.

3. Raffronto con le soluzioni giurisprudenziali accolte in ambiti contigui: in materia di contratti di consumo conclusi a mezzo di Internet

La particolare ampiezza con la quale la Corte di giustizia ha interpretato la norma relativa al foro delle obbligazioni derivanti da fatto illecito con riferimento alle azioni per diffamazione o per altre violazioni dei diritti della personalità commesse a mezzo della rete non trova, peraltro, corrispondenza nell'approccio adottato relativamente ad azioni di diversa natura traenti origine da attività *on-line*. Infatti, per quanto riguarda le controversie di natura contrattuale e relative più specificamente a contratti conclusi da consumatori, la Corte di giustizia si è attenuta ad un approccio più restrittivo nella sentenza relativa alle cause

[40] Si rimanda in proposito a F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 206 ss.

Pammer e *Hotel Alpenhof*[41]. I casi oggetto della pronuncia concernevano l'uno un contratto concluso tramite un intermediario sulla base di informazioni pubblicate su un sito Internet, e l'altro un contratto concluso a mezzo di un indirizzo e-mail indicato sul sito sul quale il servizio offerto era pubblicizzato. In questo diverso contesto, la Corte ha applicato senza adattamenti particolarmente incisivi le regole che sarebbero state applicabili relativamente a contratti della medesima natura che fossero stati interamente conclusi in modalità *off-line*. Infatti, trattandosi, nelle due fattispecie oggetto della decisione, di contratti conclusi da consumatori, la Corte di giustizia ha fatto applicazione dei criteri speciali di competenza giurisdizionale relativi a tali contratti, come contenuti *ratione temporis* nel regolamento n. 44/2001. L'applicazione di tali criteri presuppone, tra le altre ipotesi contemplate dalle rispettive disposizioni, che le attività commerciali o professionali della controparte del consumatore possano considerarsi dirette, con qualsiasi mezzo, verso lo Stato membro in cui il consumatore è domiciliato. Pur sempre, nel fare applicazione di tali criteri, la Corte di giustizia non ha mancato di sottolineare come questi fossero stati riformulati in termini più ampi in sede di trasposizione nel regolamento n. 44/2001 della disciplina precedentemente contenuta in materia nella Convenzione di Bruxelles del 1968.

Ciò proprio al fine di riflettere le peculiarità del contesto *on-line*, nel quale può rivelarsi difficoltosa ed in ultima analisi scarsamente rilevante la precisa collocazione spaziale di singoli atti prodromici alla conclusione di un contratto ai quali era attribuita rilevanza nella disciplina contenuta nella Convenzione di Bruxelles[42]. La Corte di giustizia ha dato atto che la finalità materiale perseguita dalla riformulazione nei termini accennati dei presupposti per l'applicazione della disciplina spe-

[41] CGUE, 7 dicembre 2010, cause riunite C-585/08 e C-144/09, *Pammer c. Reederei Karl Schlüter GmbH* e *Hotel Alpenhof GesmbH c. Heller*, in *Raccolta*, 2010, p. I-12527 ss.
[42] *Ibidem*, par. 59.

ciale della competenza giurisdizionale in materia di contratti conclusi da consumatori era da identificarsi nell'obiettivo di garantire a questi ultimi, per quanto possibile, la possibilità di agire per la tutela dei propri diritti innanzi ai giudici dello Stato membro del proprio domicilio. La Corte di giustizia ha tuttavia ritenuto che al fine di poter considerare l'attività commerciale della controparte come diretta verso il paese membro di domicilio del consumatore non potesse considerarsi sufficiente la mera accessibilità passiva, dallo Stato membro di domicilio del consumatore, di un sito Internet che sia gestito dalla controparte personalmente ovvero da un suo intermediario[43]. In questo senso, peraltro, già si poneva una dichiarazione congiunta del Consiglio e della Commissione in merito all'applicazione della disposizione dell'art. 15 del regolamento Bruxelles I, che era stata ripresa nel preambolo del regolamento "Roma I" con riferimento alle corrispondenti problematiche suscettibili di porsi relativamente alla legge applicabile ai contratti in questione[44].

L'accoglimento del criterio della mera accessibilità passiva del sito Internet sul quale i beni o i servizi offerti sono pubblicizzati avrebbe consentito, infatti, un illimitato assoggettamento degli imprenditori che pubblicizzino i loro servizi tramite Internet alla giurisdizione di qualsiasi Stato membro nel quale fosse domiciliato un consumatore che avesse concluso con essi un contratto sulla base delle informazioni contenute nel relativo sito Internet. Ciò avrebbe messo in pericolo, se non strettamente la prevedibilità della competenza giurisdizionale, in quanto pur sempre ogni imprenditore dovrebbe ritenersi informato dello Stato membro in cui ciascun consumatore col quale abbia concluso un contratto sia domiciliato, quantomeno la parità delle armi tra i litiganti. In-

[43] *Ibidem*, par. 68 ss.

[44] Regolamento CE n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali ("Roma I"), in G.U.U.E., L 177 del 4 luglio 2008, p. 6 ss, considerando n. 24, richiamato da CGUE, 7 dicembre 2010, cause riunite C-585/08 e C-144/09, *Pammer* e *Hotel Alpenhof*, cit., par. 74.

fatti, lo squilibrio che si sarebbe in questo modo venuto a creare nella disciplina della competenza giurisdizionale avrebbe finito probabilmente per eccedere quella finalità riequilibratrice delle posizioni sostanziali delle parti che la disciplina speciale della competenza giurisdizionale in materia di contratti conclusi dai consumatori è volta a perseguire, rischiando inoltre di fungere da disincentivo nei confronti dell'utilizzazione della rete come mezzo di promozione delle attività commerciali e imprenditoriali. Proprio allo scopo di contenere in termini ragionevoli lo squilibrio a favore del consumatore nell'allocazione della competenza giurisdizionale operato dalle norme in questione, la Corte di giustizia ha ritenuto, per un verso, che non possa considerarsi insito nel requisito per il quale le attività dell'imprenditore debbano potersi considerate rivolte con qualsiasi mezzo verso lo Stato membro del domicilio del consumatore il fatto che il contratto sia stato effettivamente concluso a mezzo del sito Internet dell'imprenditore. Ciò, infatti, restringerebbe ingiustificatamente l'ambito di applicazione delle norme in questione e sarebbe inconciliabile con l'ampiezza suggerita dall'espressione "con qualsiasi mezzo" contenuta nell'art. 15, par. 3, del regolamento Bruxelles I. Per altro verso, la Corte ha affermato che la mera accessibilità passiva del sito dal paese membro di domicilio del consumatore non possa considerarsi sufficiente. La Corte ha ravvisato piuttosto l'esigenza di qualche ulteriore indizio che possa considerarsi rivelatore dell'intenzione dell'imprenditore di indirizzare la propria offerta di servizi verso Stati membri diversi da quello del proprio stabilimento, indicando a titolo esemplificativo il carattere internazionale dell'attività svolta, con particolare riferimento a particolari attività turistiche, l'indicazione di recapiti telefonici preceduti dal prefisso internazionale, ovvero la scelta di un *top-level domain name* riferito ad un paese membro diverso, oppure di carattere neutro. La Corte ha preso in considerazione in proposito anche l'eventuale presenza di indicazioni di carattere maggiormente esplicito, come l'indicazione di mezzi o itinerari per giungere da altri Stati membri al luogo di prestazione dei servizi

offerti, ovvero il riferimento ad una clientela internazionale, ad esempio mediante l'inserimento di un link a recensioni redatte da clienti provenienti da diversi paesi membri, come pure l'uso di una lingua o l'indicazione di prezzi in valuta diversa da quella in uso nel paese membro di stabilimento dell'imprenditore[45].

In definitiva, ove si voglia raffrontare l'approccio accolto dalla Corte di giustizia nei due scenari fin qui considerati, dell'azione di carattere extracontrattuale per violazioni dei diritti della personalità causate da notizie pubblicate tramite Internet e dell'azione di carattere contrattuale che un consumatore intenda esperire nei confronti della controparte di un contratto concluso sulla base di informazioni pubblicate tramite il medesimo mezzo, ne emerge che, mentre, nel primo contesto, secondo la soluzione accolta dalla Corte di giustizia nella sentenza *eDate* e sostanzialmente confermata nella sentenza *Bolagsupplysningen*, il soggetto che lamenti la violazione potrà, in alternativa agli altri fori già contemplati nella soluzione *Shevill*, in ogni caso contare sulla possibilità di agire davanti ai giudici dello Stato membro in cui ha il proprio centro di interessi, nel secondo contesto la possibilità per il consumatore di agire davanti ai giudici dello Stato membro in cui è domiciliato – ove, ovviamente, tale Stato membro non coincida con quello in cui la controparte è a propria volta domiciliata – sussisterà unicamente quando quest'ultima parte abbia pubblicizzato i propri servizi su Internet in modalità tali da poter essere considerata aver diretto la propria attività nei confronti dello Stato membro in cui il consumatore è domiciliato, ovvero verso più paesi, tra cui quest'ultimo. Pur sempre, la relativa disparità di trattamento che ne risulta tra i due soggetti assunti, in pur diversa misura, a parti meritevoli di protezione dei rispettivi rapporti potrebbe dirsi riflettere, oltre che, certamente, la diversità dei due contesti giuridici, extracontrattuale il primo e contrattuale il secondo, in cui il

[45] *Ibidem*, par. 80, 83 ss. Si veda in proposito V. Pironon, *Dits et non-dits sur la méthode de la focalisation dans le contentieux – contractuel et delictuel – du commerce électronique*, in *Journal du droit international*, 2011, p. 915 ss.

rapporto obbligatorio è sorto tra le parti, congetturalmente anche la diversità dei diritti della cui tutela si discute nei due contesti considerati, di carattere assoluto nel primo e di carattere relativo ovvero squisitamente patrimoniale nel secondo.

4. *Segue*: in materia di violazioni del diritto d'autore o di altri diritti di proprietà intellettuale commesse tramite Internet

La diversità dei diritti della cui tutela giurisdizionale si discute è invece certamente all'origine della diversità dell'approccio accolto dalla Corte di giustizia in materia di giurisdizione nelle controversie concernenti le violazioni dei diritti della personalità commesse a mezzo di informazioni pubblicate tramite Internet rispetto all'approccio adottato dalla Corte stessa relativamente all'applicazione del criterio di competenza giurisdizionale concernente le azioni derivanti da fatto illecito con riferimento alle violazioni di diritti di proprietà intellettuale commesse tramite materiale pubblicato su Internet. In questo diverso ambito, appare rilevare innegabilmente il carattere territorialmente limitato dei diritti di proprietà intellettuale. Questo porta ad identificare come luogo dell'*eventus damni* lo Stato membro per il quale è concessa la protezione del diritto, posto che in altri Stati membri in cui il diritto di cui si discute non riceva protezione difetterebbe evidentemente il presupposto stesso della violazione come fonte della pretesa risarcitoria vantata, ovvero, nel caso reciproco di un'azione di accertamento negativo, negata. Così, nella sentenza relativa al caso *Wintersteiger*[46], nella quale si trattava della violazione di un marchio nazionale registrato in un paese membro per effetto di un'inserzione commerciale effettuata su un motore di ricerca operante su scala globale ma provvisto di siti recanti *top-level domain names* distinti per paesi, in una fattispecie in cui

[46] CGUE, 19 aprile 2012, in causa C-523/10, *Wintersteiger AG c. Products 4U Sondermaschinenbau GmbH*, ECLI:EU:C:2012:220.

l'inserzione asseritamente lesiva figurava sul sito recante il *top-level domain name* di un paese membro diverso da quello nel quale il marchio era registrato, la Corte di giustizia ha ritenuto doversi identificare come luogo dell'*eventus damni* lo Stato membro nel quale il marchio della cui violazione si discuteva era registrato[47].

Alternativamente a tale foro la Corte ha pur sempre ritenuto sussistere, in ogni caso in alternativa al foro generale del domicilio del convenuto, il foro del luogo della condotta dannosa. La Corte ha identificato quest'ultimo foro con lo Stato membro nel quale l'inserzionista aveva inserito, sul sito recante il *top level domain name* del medesimo Stato membro, l'inserzione contenente la pretesa contraffazione del marchio[48]. La soluzione accolta dalla Corte di giustizia per un verso si rivela atta a garantire la prevedibilità della competenza giurisdizionale, in quanto limita l'alternativa al foro dello Stato membro di registrazione del diritto di proprietà intellettuale e a quello dello Stato membro nel quale l'inserzionista ha proceduto all'inserimento sul *web* dell'annuncio comportante l'asserita violazione del diritto di proprietà intellettuale, Stato membro coincidente con quello indicato dal *top-level domain name* del sito stesso. Essa solleva per altro verso qualche perplessità in ordine all'opportunità di lasciare sussistere affatto tale alternativa. Deve infatti considerarsi che essa non è contemplata in termini generali dalla giurisprudenza della Corte di giustizia interpretativa della norma relativa al foro del fatto illecito, la quale la prevede unicamente con riferimento all'ipotesi degli illeciti a distanza, oggetto della sentenza *Bier c. Mines de potasse d'Alsace*[49].

---

[47] *Ibidem*, par. 27 ss.
[48] *Ibidem*, par. 34 ss.
[49] Si vedano, per alcune considerazioni critiche in merito alla soluzione accolta nella pronuncia esaminata, S. Marino, *Nuovi sviluppi in materia di illecito extracontrattuale* on line, in *Rivista di diritto internazionale privato e processuale*, 2012, p. 879 ss., spec. p. 884 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 28 ss.; in senso positivo, valutando con favore in un'ottica di prevedibilità della competenza giurisdizionale la soluzione accolta dalla Corte d giustizia, M.

Pur sempre, si deve osservare che, a ben considerare, il foro del luogo in cui l'inserzionista ha pubblicato su Internet l'annuncio pubblicitario lesivo tendenzialmente verrà a coincidere, nelle azioni rivolte nei suoi confronti dal titolare del diritto, col foro comunque competente in base al criterio generale del domicilio del convenuto, rispetto al quale il foro del fatto illecito opera comunque come criterio alternativo. Ciò posto, ove si voglia confrontare l'approccio adottato dalla Corte nel caso appena esaminato con la soluzione accolta relativamente alle violazioni dei diritti della personalità commesse tramite Internet, si ha l'impressione che nel primo dei due ambiti l'approccio accolto si riveli in qualche misura più restrittivo[50]. Nell'uno come nell'altro caso, tuttavia, si ha l'impressione che la Corte di giustizia tenda a considerare gli illeciti commessi tramite Internet alla stregua di una nuova categoria di illeciti a distanza, nei quali meriti attribuire rilevanza al luogo della condotta dannosa in alternativa al luogo di produzione del danno, che nel caso della violazione di un diritto di proprietà intellettuale di carattere nazionale è da identificarsi con lo Stato membro nel quale tale diritto è registrato[51].

L'approccio adottato dalla Corte di giustizia nella sentenza *Wintersteiger* è stato adattato da alcune pronunce successive alla diversa ipotesi delle violazioni del diritto d'autore commesse, nel caso *Pinckney*[52], mediante riproduzione del contenuto protetto su un supporto materiale ven-

---

Köhler, *Der fliegende Gerichtsstand. Die Bestimmung des zuständingen Gerichts bei ubiquitäre Rechtsverletzungen*, in *WRP – Wettbewerb im Recht und Praxis*, 2013, p. 1130 ss., spec. p. 1134.

[50] Come già si osservava in F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 29; v. anche, nello stesso senso, M. Köhler, *Der fliegende Gerichtsstand*, cit., p. 1134.

[51] Si veda ancora F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 29 ss.

[52] CGUE, 3 ottobre 2013, in causa C-170/12, *Pinckney c. KDG Mediatech AG*, ECLI:EU:C:2013:635.

duto tramite un sito Internet, e, nel caso *Hejduk*[53], mediante riproduzione del contenuto protetto direttamente su un sito *web*. In entrambi i casi oggetto delle due pronunce da ultimo menzionate, la Corte di giustizia ha sottolineato ancora una volta la diversità delle caratteristiche proprie del diritto tutelato, in quanto il diritto d'autore, pur essendo, non diversamente dal marchio nazionale, tutelato su base territoriale, si presenta tuttavia suscettibile di ricevere tutela in tutti gli Stati membri, sulla base, in ciascuno di essi, del diritto nazionale armonizzato ai sensi della direttiva 2001/29[54]. Conseguentemente, in entrambi i casi la Corte di giustizia ha ritenuto competenti a conoscere dell'azione risarcitoria esperita dal titolare del diritto d'autore, quali giudici del luogo di produzione dell'*eventus damni*, i giudici dello Stato membro in cui il diritto è tutelato e nel quale è accessibile tramite Internet il sito sul quale è consultabile, ovvero tramite il quale è acquistabile, il materiale integrante la violazione[55].

Nel dare atto che tale competenza è comunque limitata al diritto così come protetto nello Stato membro del giudice adito, la Corte di giustizia ha recuperato la logica della *Mosaikbetrachtung*, lasciando sussistere la possibilità che azioni parallele siano intentate dinanzi ai giudici degli altri Stati membri nei quali il diritto riceva ugualmente protezione e nei quali sia stato al tempo stesso possibile accedere ovvero acquistare tramite Internet il materiale integrante la violazione[56]. La soluzione, che appare certo presentare la problematica, già evidenziata a proposito della sentenza *Shevill*, di non favorire il perseguimento di un obiettivo di coordinamento tra giurisdizioni[57], appare suscettibile di applicarsi anche in relazione a violazioni di un brevetto europeo non a protezione unitaria, il quale ugualmente è suscettibile di dar vita a un fascio di diritti di privati-

[53] CGUE, 22 gennaio 2015, in causa C-441/13, *Hejduk c. EnergieAgentur.NRW GmbH*, ECLI:EU:C:2015:28.
[54] CGUE, 3 ottobre 2013, *Pinckney*, cit., par. 36; 22 gennaio 2015, *Hejduk*, cit., par. 29.
[55] CGUE, 3 ottobre 2013, *Pinckney*, cit., par. 36; 22 gennaio 2015, *Hejduk*, cit., par. 29.
[56] Si veda con riferimento alla soluzione accolta dalla Corte di giustizia nelle pronunce da ultimo citate P. Mankowski, *Article 7*, cit., p. 326 ss.
[57] Si rimanda a quanto osservato *supra*, par. 2.

va paralleli, ciascuno con efficacia territoriale limitata al singolo Stato membro per il quale ne è richiesta la registrazione[58], mentre non appare estensibile ai diritti di proprietà intellettuale che beneficiano di un regime di protezione unitaria per l'intera Unione europea. Relativamente a questi ultimi, e salva restando, relativamente ai brevetti europei a protezione unitaria, la competenza del Tribunale unificato dei brevetti allorquando questo diverrà operativo[59], ammettere la competenza dei giudici di ciascuno degli Stati membri da cui possa accedersi al materiale lesivo pubblicato ovvero offerto in vendita tramite Internet relativamente all'intero danno causato dalla violazione del diritto a protezione unitaria rischierebbe di esporre il soggetto emittente del materiale lesivo ad una eccessiva imprevedibilità del foro innanzi al quale potrà essere citato.

Un maggiore margine di prevedibilità può essere assicurato facendo riferimento, invece, allo Stato membro nel quale l'emittente del mate-

[58] Secondo quanto rilevato dalla Corte di giustizia al fine di escludere l'applicazione del criterio di competenza giurisdizionale per connessione di cui all'art. 6, n. 1, del regolamento n. 44/2001 (ora corrispondente all'art. 8, n. 1, del regolamento n. 1215/2012) relativamente ad azioni introdotte in diversi paesi membri per la violazione di diverse componenti nazionali di un brevetto europeo in CGCE, 13 luglio 2006, in causa C-539/03, *Roche Nederland c. Primus*, in *Raccolta*, 2006, p. I-6535 ss., par. 25 ss.; successivamente, nel senso dell'applicabilità della norma ove le diverse azioni riguardino, invece, le medesime componenti nazionali del brevetto europeo, CGUE, 12 luglio 2012, in causa C-616/10, *Solvay SA c. Honeywell Flourine Products Europe BV et al.*, ECLI:EU:C:2012:445; in *Revue critique de droit international privé*, 2013, p. 472 ss., con nota di E. Treppoz, ivi, p. 479 ss.; si veda anche F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., p. 39 ss.

[59] Accordo su un Tribunale unificato dei brevetti, in *GUUE*, C 175 del 20 giugno 2013, p. 1 ss. Si vedano, con riferimento alle modifiche introdotte nel regolamento n. 1215/2012 ("Bruxelles I-bis") tramite il regolamento UE n. 542/2014 allo scopo di realizzare un coordinamento della disciplina in materia di giurisdizione recata dal regolamento con le regole contenute nell'accordo, P. Mankowski, *Die neuen Regeln über gemeinsame Gerichte in Artt. 71a-71d Brüssel Ia-VO*, in *GPR – Zeitschrift für Gemeinschaftsprivatrecht*, 2014, p. 330 ss.; F. Marongiu Buonaiuti, *The Agreement Establishing a Unified Patent Court and its Impact on the Brussels I Recast Regulation. The New Rules Introduced under Regulation (EU) No 542/2014 in respect of the Unified Patent Court and the Benelux Court of Justice*, in *Cuadernos de derecho transnacional*, 2016, n. 1, p. 208 ss.

riale lesivo lo ha pubblicato, ovvero offerto in vendita su Internet, quale luogo della condotta dannosa[60]. Il riferimento a quest'ultimo luogo, posto che esso si riveli accertabile sulla base di elementi oggettivi, per un verso consente di evitare un'inopportuna ubiquità della competenza giurisdizionale e, per altro verso, nell'ipotesi di un'azione esperita dal titolare del diritto violato, si rivelerebbe maggiormente in linea con la regola generale per la quale *actor sequitur forum rei*, rispetto alla quale, come la Corte stessa ha osservato nel caso *Melzer*[61], le eccezioni sono per principio generale da interpretarsi restrittivamente.

5. Segue: il foro delle violazioni del diritto alla tutela dei dati personali in base al regolamento UE n. 2016/679

L'opzione tra il foro del luogo della condotta dannosa e il foro del luogo dell'*eventus damni* appare lasciata aperta anche dalle nuove disposizioni che disciplinano la giurisdizione contenute nel regolamento UE n. 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali[62]. Il regolamento, che sostituirà a far data

[60] Al luogo della condotta, o, meglio, ai giudici dello Stato membro nel quale l'atto di contraffazione è stato commesso ovvero minaccia di essere commesso fanno invero riferimento, in alternativa al foro del domicilio del convenuto, i criteri speciali di competenza giurisdizionale previsti dall'art. 97 del regolamento CE n. 207/2009, sul marchio dell'Unione europea, così come i criteri contenuti negli altri atti istitutivi di diritti di proprietà intellettuale con effetto unitario per l'intero territorio dell'Unione, tra cui l'art. 101, par. 3, del regolamento CE n. 2100/94 concernente la privativa comunitaria per ritrovati vegetali e l'art. 82, par. 5, del regolamento (CE) n. 6/2002 su disegni e modelli comunitari. Al medesimo criterio è fatto riferimento, nell'art. 33, par. 1, lett. a), dell'accordo istitutivo del Tribunale unificato dei brevetti, al fine della ripartizione della competenza tra le diverse sezioni locali del Tribunale unificato. Si veda in proposito M. Köhler, *Der fliegende Gerichtsstand*, cit., p. 1134 ss.

[61] CGUE, 16 maggio 2013, in causa C-228/11, *Melzer c. MF Global UK*, ECLI:EU:C:2013:305, par. 23 ss.

[62] In *GUUE*, L 119 del 4 maggio 2016, p. 1 ss.

dal 25 maggio 2018 la direttiva 95/46/CE, nel prevedere all'art. 79, par. 1, il diritto del titolare dei dati ad un rimedio giurisdizionale effettivo per le eventuali violazioni dei diritti tutelati dal regolamento stesso, introduce, nel par. 2 della stessa disposizione, alcuni criteri speciali di competenza giurisdizionale relativi alle azioni contemplate dalla norma. Tali criteri sono destinati a prevalere sulle regole generali contenute in quest'ultimo regolamento, in virtù del criterio di specialità *ratione materiae* recepito dal regolamento Bruxelles I-*bis* al suo art. 67. Conformemente a tale criterio, le regole contenute in quest'ultimo regolamento potranno trovare applicazione solo nella misura in cui non siano incompatibili con la disciplina speciale. I criteri speciali contemplati dall'art. 79, par. 2 del regolamento concernente la tutela dei dati personali, riflettendo l'ottica protettiva della persona del titolare dei dati che ispira l'intera disciplina recata dal regolamento evidenziata dal par. 1 della stessa norma, si applicano unicamente alle azioni promosse dal titolare dei dati nei confronti del titolare o del responsabile del trattamento. Essi contemplano un'alternativa tra i giudici dello Stato membro in cui il titolare o il responsabile del trattamento possiedono uno stabilimento, e i giudici dello Stato membro in cui il titolare dei dati ha la propria residenza abituale, quest'ultima opzione restando peraltro esclusa nei casi in cui il titolare o il responsabile del trattamento sia una pubblica autorità di uno Stato membro, la quale agisca nell'esercizio dei propri pubblici poteri[63].

[63] Si vedano in proposito, tra gli altri, P. de Miguel Asensio, *Aspectos internacionales del Reglamento general de protección de datos de la UE (I): cuestiones de competencia*, in www.pedrodemiguelasensio.blogspot.it, 11 maggio 2016, p. 3 ss.; P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, Antwerp, Portland, 2016, p. 81 ss., spec. p. 96 ss.; Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, in *Rivista di diritto internazionale privato e processuale*, 2017, p. 653 ss., spec. p. 668 ss.; *adde* F. Marongiu Buonaiuti, *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati*

In proposito, il primo dei due criteri contemplati dalla norma appare tendenzialmente coincidere col foro del luogo della condotta, nell'economia di un'azione di carattere extracontrattuale, come nella gran parte dei casi appare dover essere qualificata un'azione che trova il suo fondamento nella violazione delle disposizioni del regolamento sul trattamento dei dati personali, benché il trattamento dei dati possa materialmente avere luogo anche in occasione della conclusione o in relazione con l'esecuzione di un contratto[64]. Deve infatti osservarsi che è normalmente nel luogo in cui il titolare o il responsabile del trattamento dei dati è stabilito che il trattamento stesso ha luogo.

Pur sempre, la norma appare fare riferimento genericamente allo Stato membro in cui il titolare o il responsabile del trattamento ha uno stabilimento, senza specificare in proposito che debba trattarsi dello stabilimento principale di tale soggetto, ciò che consentirebbe di accostare tale criterio al foro generale del domicilio del convenuto come contemplato dal regolamento Bruxelles I-*bis*. Nemmeno precisa la norma che debba trattarsi dello stabilimento presso il quale ha avuto luogo il trattamento dei dati personali che ha dato origine all'azione in giudizio, ciò che consentirebbe propriamente di assimilare tale foro al

---

personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis*"*, in *Cuadernos de derecho transnacional*, 2017, n. 2, p. 448 ss.

[64] Si veda in proposito Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 669 ss., 671 ss., il quale prospetta l'applicazione alternativa dei criteri recati, rispettivamente, dall'art. 7.1 e 7.2 del regolamento n. 1215/2012 ("Bruxelles I-*bis*"), sulla base di una lettura restrittiva della clausola di cui all'art. 67 di quest'ultimo regolamento, il quale, nel prevedere che il regolamento non pregiudica l'applicazione delle disposizioni che disciplinano la competenza giurisdizionale in materie particolari, contenute in atti dell'Unione europea o in legislazioni nazionali armonizzate in applicazione di tali atti, appare invece escludere la possibilità di fare ricorso ai criteri di competenza giurisdizionale recati dal regolamento Bruxelles I-*bis* relativamente ad azioni per le quali un altro atto dell'Unione preveda una diversa allocazione della competenza giurisdizionale in considerazione dei caratteri specifici delle controversie contemplate da tale atto. Si vedano, in quest'ultimo senso, P. de Miguel Asensio, *Aspectos internacionales del Reglamento general de protección de datos*, cit., p. 3; P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights*, p. 105.

foro del luogo della condotta dannosa, secondo l'interpretazione c.d. ubiquitaria che è stata data dalla Corte di giustizia al foro contemplato dall'attuale art. 7, par. 2, del regolamento Bruxelles I-*bis* nella giurisprudenza della Corte di giustizia relativa agli illeciti a distanza. Piuttosto, nei termini vaghi e generici nei quali è concepito il foro in questione nel regolamento sul trattamento dei dati personali, esso appare assimilabile a un criterio di competenza giurisdizionale basato sulla mera presenza commerciale, la cui portata va ben al di là del foro dell'agenzia, succursale o filiale contemplato dal regolamento Bruxelles I-*bis*. Quest'ultimo criterio, come è noto, oltre a presupporre che il convenuto sia domiciliato in uno Stato membro, è invocabile unicamente con riferimento alle azioni che traggano il loro fondamento dalle attività dell'agenzia, succursale o filiale in questione[65].

Nella sua ampiezza, il foro contemplato dal regolamento n. 2016/679 appare invocabile anche nei confronti di un titolare o responsabile del trattamento che abbia il proprio stabilimento principale in uno Stato terzo, qualora abbia uno stabilimento nello Stato membro del giudice adito, a condizione, pur sempre, che il diritto la cui tutela è invocata dal titolare dei dati ricada nell'ambito di applicazione *ratione loci vel personarum* del regolamento stesso. In proposito, ai sensi dell'art. 3 del regolamento, la presenza di uno stabilimento del titolare o responsabile del trattamento in uno Stato membro è sufficiente al fine dell'applicazione delle disposizioni del regolamento al trattamento di dati che sia effettuato nel contesto delle attività di quello stabilimento. Ciò, in definitiva, nelle ipotesi di un titolare o responsabile del trattamento il cui stabilimento principale sia situato in uno Stato terzo e che abbia uno stabilimento in uno Stato membro, consente di invocare il fo-

[65] Si veda in proposito P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights*, cit., p. 99 ss., sottolineando la chiara finalità protettiva nei confronti del titolare dei dati insita nella previsione di un così ampio criterio di competenza giurisdizionale.

ro in questione relativamente alle sole azioni scaturenti dal trattamento dei dati che sia effettuato nel contesto delle attività di tale stabilimento.

La norma dell'art. 3, par. 1, del regolamento, a questo riguardo, appare recepire l'interpretazione senz'altro ampia dell'ambito di applicazione *ratione personarum* della disciplina europea del trattamento dei dati personali fatta propria, con riferimento alla direttiva 95/46/CE, dalla Corte di giustizia nella sentenza *Google Spain*[66]. La norma precisa, infatti, che la disciplina contenuta nel regolamento si applica indipendentemente dal fatto che il trattamento dei dati sia materialmente avvenuto all'interno dell'Unione o meno, essendo sufficiente che esso sia imputabile a uno stabilimento del titolare o responsabile del trattamento ubicato nell'Unione. Del resto, nel caso, al quale si riferiva la sentenza appena evocata, in cui il trattamento dei dati sia effettuato da un gestore di un sito Internet, non è certo insolito che questo possa materialmente delocalizzare le operazioni relative al trattamento dei dati degli utenti, eventualmente affidandole a un soggetto terzo ubicato in un paese che non presenta alcun effettivo collegamento con la vicenda che ha dato luogo all'acquisizione dei dati. Conseguentemente, appare ragionevole, anche a fini di certezza del diritto e di prevenzione dell'elusione della disciplina imperativa recata dal regolamento stesso, che a rilevare ai fini dell'applicazione della disciplina recata dal regolamento nelle situazioni che presentano collegamenti con paesi terzi sia lo stabilimento del titolare o del responsabile del trattamento nel contesto delle attività del

[66] CGUE, 13 maggio 2014, in causa C-131/12, *Google Spain SL, Google Inc*, ECLI:EU:C:2014:317. Nel senso di un'interpretazione estensiva della nozione di trattamento dei dati che intervenga nel contesto delle attività di uno stabilimento del responsabile del trattamento nell'Unione, ai fini dei corrispondenti criteri di applicazione territoriale della disciplina contenuta nella precedente direttiva 95/46/CE, si veda anche CGUE, 1 ottobre 2015, in causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639, in *Revue critique de droit international privé*, 2016, p. 377 ss., con nota di B. Haftel, ivi, p. 378 ss.; si veda anche Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 658 ss.

quale i dati in questione sono stati acquisiti[67]. In un'ottica ulteriormente estensiva dell'ambito di applicazione soggettivo del regolamento, ai sensi dell'art. 3, par. 2, le sue norme, e di conseguenza i criteri di competenza giurisdizionale contemplati dall'art. 79, par. 2, sono invocabili anche nei confronti di un titolare o responsabile del trattamento che non abbia alcun stabilimento in uno Stato membro, ogniqualvolta i dati oggetto del trattamento si riferiscano a persone che si trovino materialmente in uno Stato membro.

A questo fine, però, all'evidente scopo di tutelare il titolare ovvero il responsabile del trattamento, stabilito in un paese terzo, da un'applicazione "a sorpresa" della disciplina recata dal regolamento e di contenere in qualche misura la tendenza all'applicazione extraterritoriale della disciplina protettiva da esso recata, l'art. 3, par. 2, pone alcuni requisiti ulteriori, atti a garantire l'esistenza di un collegamento oggettivo e prevedibile del trattamento dei dati con lo Stato membro in cui il titolare dei dati stessi si trova. Tali requisiti ulteriori sono individuati dalla norma nell'essere il trattamento dei dati legato, alternativamente, all'offerta di beni o servizi a titolari dei dati che si trovino nell'Unione, ovvero al monitoraggio del loro comportamento, nella misura in cui il comportamento oggetto del monitoraggio abbia luogo nell'Unione. Per di più, il regolamento, all'art. 3, par. 3, tende a superare i normali limiti territoriali dell'applicazione del diritto dell'Unione, per i quali questo di regola non si applica nei territori extraeuropei soggetti alla sovranità degli Stati membri, prevedendo l'applicazione delle proprie norme ai titolari o re-

[67] Si veda ancora Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 659 s. Diversamente, ai fini del criterio di competenza giurisdizionale contemplato dall'art. 79, par. 2, del regolamento n. 679/2016, la genericità del riferimento a "uno stabilimento" del responsabile del trattamento e la *ratio* consistente nell'obiettivo di assicurare al titolare dei dati le più ampie prospettive di accesso a un giudice innanzi al quale poter agire nei confronti del responsabile del trattamento suggeriscono un'interpretazione più ampia: v. P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights*, cit., p. 100 ss.

sponsabili del trattamento che siano stabiliti in un luogo soggetto al diritto di uno Stato membro in base al diritto internazionale[68].

Sussistendo le condizioni che ne determinano l'assoggettamento alla disciplina recata dal regolamento n. 2016/679 che si sono evidenziate, il titolare ovvero il responsabile del trattamento potranno essere citati, in alternativa allo Stato membro in cui hanno un proprio stabilimento nel senso che si è indicato, innanzi ai giudici dello Stato membro in cui il titolare dei dati ha la propria residenza abituale, salvo che, come già si è menzionato, il titolare o il responsabile del trattamento sia una pubblica autorità che agisca nell'esercizio dei propri pubblici poteri. Ciò, per definizione, ne rende difficilmente configurabile l'assoggettamento alla giurisdizione dei giudici di uno Stato diverso. Il criterio alternativo costituito dalla residenza abituale del titolare dei dati presenta un'innegabile assonanza col criterio del centro degli interessi della persona che si pretenda vittima di una violazione della privacy o di altro diritto della personalità, utilizzato dalla Corte di giustizia nelle sentenze *eDate* e *Bolagsupplysningen*[69], e si rivela atto a coincidere tendenzialmente col giudice del luogo dell'*eventus damni* in un'azione risarcitoria da fatto illecito. Ciò può trovare giustificazione alla luce della considerazione che la violazione dei diritti conferiti dal regolamento n. 2016/679 al titolare dei dati personali, in quanto atta a colpire la persona del titolare dei dati in un suo diritto della personalità quale è quello al controllo dei propri dati personali, deve considerarsi materializzata,

[68] In base al considerando n. 25 del preambolo del regolamento, in base a questa disposizione le norme del regolamento potrebbero trovare applicazione a un responsabile del trattamento che sia stabilito all'interno di una rappresentanza diplomatica o posto consolare di un paese membro ubicati in un paese terzo, ipotesi abbastanza singolare ove non la si intenda riferire al trattamento dei dati personali effettuato dagli uffici stessi della rappresentanza diplomatica o del posto consolare per l'esercizio delle loro funzioni. Si veda, nel senso che l'ambito di applicazione del regolamento si estenda fino ai limiti più esterni della giurisdizione statale secondo il diritto internazionale, Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 660.

[69] Si rimanda a quanto osservato *supra*, par. 2.

quale luogo dell'evento dannoso, nel luogo in cui la persona è stabilita, che il regolamento, con una soluzione che è ormai ampiamente accolta nella generalità degli atti dell'Unione europea in materia di diritto internazionale privato, identifica con la residenza abituale del soggetto[70].

Inevitabilmente, l'opzione che l'art. 79, par. 2, del regolamento n. 2016/679 prevede a favore del foro dello Stato membro della residenza abituale del titolare dei dati si presta alla medesima obiezione che è stata rivolta al foro del centro degli interessi della persona che si pretenda vittima di una violazione della privacy o di altro diritto della personalità. Tale foro, come si è rilevato, è contemplato dalla Corte di giustizia nell'interpretazione del criterio speciale oggi contenuto nell'art. 7, par. 2, del regolamento n. 1215/2012 accolta nelle sentenze *eDate* e *Bolagsupplysningen*. Tale obiezione riguarda il rischio di pregiudicare eccessivamente, a favore del soggetto che si pretenda leso, la parità delle armi tra i litiganti, che è parte integrante del diritto all'equo processo tutelato dall'art. 6, par. 1, della Convenzione europea dei diritti dell'uomo e, trattandosi dell'applicazione, nell'un caso come nell'altro, di un atto dell'Unione europea, dall'art. 47 della Carta dei diritti fondamentali dell'Unione[71]. A questo proposito, possono per un verso venire in considerazione le giustificazioni già addotte dalla Corte di giustizia nelle sentenze appena evocate, le quali, come si è osservato, si incentravano essenzialmente sulla particolare attitudine pregiudizievole della diffusione di informazioni tramite Internet, attesa la grande facili-

[70] Si veda P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights*, cit., p. 101 ss. Nel senso per cui, problematicamente, il criterio in questione potrebbe coesistere col criterio del centro degli interessi del titolare dei dati derivante dall'art. 7.2 del regolamento Bruxelles I-bis secondo l'interpretazione datane nella sentenza *eDate*, per cui tale centro potrebbe anche materialmente non coincidere ed essere potenzialmente ubicato in un paese membro diverso da quello della residenza abituale del soggetto in questione, Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 669 ss.

[71] Si rimanda alle considerazioni svolte in F. Marongiu Buonaiuti, *La tutela del diritto di accesso alla giustizia e della parità delle armi tra i litiganti*, cit., p. 348 ss.

tà ed immediatezza con la quale esse possono essere consultate da utenti situati in diverse parti del mondo.

Queste considerazioni svolte dalla Corte di giustizia nelle sentenze da ultimo evocate, peraltro, sono trasponibili solo in parte al contesto della tutela dei dati personali apprestata dal regolamento n. 679/2016, considerato che questa presenta una portata generale ed è pertanto destinata ad applicarsi indipendentemente dal mezzo attraverso il quale possa essere arrecata una lesione ai diritti che il regolamento conferisce al titolare dei dati. Per altro verso, deve rilevarsi che la scelta che è offerta al titolare dei dati – e a lui soltanto data l'ottica nella quale è concepita la norma dell'art. 79, par. 2, del regolamento – tra due possibili fori alternativi, dei quali il secondo presenta un evidente legame di stretta prossimità con la sua sfera giuridica personale, si inserisce pienamente nella logica d'insieme del regolamento, volta a garantire un elevato livello di tutela dei diritti del titolare dei dati[72]. In proposito, oltre al rilievo per il quale la norma in questione si presenta espressamente come una specificazione delle modalità di attuazione del diritto ad un rimedio giurisdizionale effettivo che è riconosciuto al titolare del dati dal par. 1 della stessa disposizione dell'art. 79 del regolamento, si deve osservare come l'ampiezza della tutela offerta sul piano processuale dalla norma in esame rifletta l'ampiezza della protezione che al titolare dei dati è offerta sul piano sostanziale dalla disciplina uniforme recata dal regolamento stesso. Particolarmente indicativa di tale ampiezza si presenta la disposizione di cui all'art. 82 del regolamento n. 2016/679, la quale prevede, al par. 1, il diritto del titolare dei dati al risarcimento dei danni materiali e immateriali da parte del titolare ovvero del responsabile del trattamento dei dati, prevedendo al par. 2 un regime particolarmente rigoroso per il primo di questi due soggetti[73].

[72] Secondo quanto osservato anche da P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights*, cit., p. 97 ss.

[73] Si veda in proposito Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 672.

La particolare imperatività della tutela del titolare dei dati che ispira la disciplina recata dal regolamento sul trattamento dei dati personali è ulteriormente sottolineata, tra l'altro, dai rigidi limiti che il regolamento stesso pone alla possibilità per un titolare ovvero un responsabile del trattamento, la cui attività ricada nell'ambito territoriale ovvero personale di applicazione della disciplina da questo recata, di sottrarsi alla sua applicazione. Rileva in questo senso particolarmente la disposizione dell'art. 48 del regolamento, la quale, con un approccio che si rivela peraltro eccessivamente rigido e massimalista, esclude il riconoscimento di decisioni giudiziarie o adottate da autorità amministrative di Stati terzi, che richiedano al titolare o al responsabile del trattamento di trasferire o rivelare dati personali, in assenza di un accordo internazionale in vigore tra lo Stato in questione e l'Unione europea o un suo Stato membro, salvo che il regolamento stesso disponga diversamente. La norma, che sottolinea il carattere anche internazionalmente imperativo della disciplina recata dal regolamento, in quanto non consente che la sua applicazione possa essere esclusa, relativamente a situazioni ricadenti nel suo ambito di applicazione, per effetto dell'applicazione di una disciplina potenzialmente non corrispondente da parte di un giudice di un paese terzo[74], appare peraltro criticabile nell'approccio adottato. Infatti, facendo riferimento unicamente al dato formale della presenza o meno di un accordo con lo Stato terzo da cui la decisione provenga, non attribuisce alcuna rilevanza agli *standards* di tutela dei dati personali in vigore nello Stato terzo in questione, ovvero previsti dalla legge di cui i giudici di tale Stato abbiano fatto applicazione, che potrebbero non necessariamente rivelarsi deteriori rispetto a quelli previsti dal

[74] Si veda ancora Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., p. 661 s., con riferimento a un'affermazione in questo senso, riferita alla precedente disciplina di cui alla direttiva 95/46/CE, contenuta nella già citata sentenza della CGUE, 13 maggio 2014, in causa C-131/12, *Google Spain SL, Google Inc*, cit., par. 58, nonché all'affermazione del carattere internazionalmente imperativo della disciplina comunitaria protettiva dei diritti degli agenti commerciali indipendenti contenuta in CGCE, 9 novembre 2000, in causa C-381/98, *Ingmar GB Ltd c. Eaton Leonard Technologies Inc.*, in *Raccolta*, 2000, p. I-9305 ss., par. 25.

regolamento, a prescindere dall'esistenza di alcun accordo con lo Stato terzo che viene in considerazione.

6. Considerazioni conclusive

La giurisprudenza della Corte di giustizia relativa all'interpretazione del foro del fatto illecito come previsto dall'attuale art. 7, par. 2, del regolamento n. 1215/2012 relativamente alle ipotesi di violazioni della privacy e dei diritti della personalità commesse a mezzo di Internet, per un verso, e la disciplina della giurisdizione relativamente alle violazioni dei diritti inerenti alla tutela dei dati personali introdotta dal regolamento n. 2016/679, per altro verso, dimostrano come il sistema generale di allocazione della giurisdizione in materia civile e commerciale contenuto attualmente nel regolamento n. 1215/2012 e con esso il principio *actor sequitur forum rei*, al quale tale sistema è ispirato, possano subire ampie deroghe. Ciò non soltanto nell'ottica, che è propria in generale dei fori speciali previsti dal regolamento Bruxelles I-*bis*, di prevedere relativamente ad alcune categorie di controversie fori alternativi al foro generale del domicilio del convenuto, che possano rivelarsi maggiormente idonei a soddisfare un obiettivo di prossimità tra il giudice e gli elementi fattuali rilevanti della controversia. Bensì anche, e più decisivamente, al fine di perseguire una tutela maggiormente effettiva di diritti ed interessi da considerarsi come particolarmente meritevoli di tutela, come i diritti della personalità degli individui, e, tra questi, il diritto alla tutela dei propri dati personali, che rischiano di essere minacciati, in misura più consistente di quanto potesse avvenire in precedenza, dal ricorso sempre più pervasivo ai nuovi mezzi offerti dalla società dell'informazione. L'orientamento che si è evidenziato può, di riflesso, anche rivelarsi volto a tutelare l'interesse generale a che gli operatori attivi in tale ambito siano richiamati ad un uso dei mezzi in questione che si riveli maggiormente responsabile e rispettoso dei diritti dei sog-

getti interessati, a fronte del rischio di trovarsi esposti ad azioni giudiziarie innanzi a fori diversi da quello del paese in cui sono stabiliti.

Questa evoluzione della giurisprudenza e della legislazione dell'Unione europea in relazione alle minacce per i diritti della personalità degli individui, che sono poste dalle pur innegabili opportunità offerte al giorno d'oggi dalla società dell'informazione, appare del resto in linea con le più recenti evoluzioni anche della giurisprudenza della Corte europea dei diritti dell'uomo. Questa ha avuto recentemente occasione di soffermarsi sull'incidenza dell'affermazione, piuttosto che del diniego, della giurisdizione dei giudici di uno Stato contraente sul diritto di accesso alla giustizia tutelato dall'art. 6, par. 1 della Convenzione europea. Ciò particolarmente nel caso in cui, come avvenuto nella fattispecie oggetto della recente pronuncia della Corte europea relativa al caso *Arlewin c. Svezia*[75], l'attività ritenuta lesiva del diritto della personalità invocato presenti dei collegamenti effettivi con lo Stato in cui il soggetto che si pretenda leso è stabilito. Ciò in termini tali che la parità delle armi tra i litiganti, declinata in termini di prevedibilità, per il soggetto asseritamente responsabile, della allocazione della giurisdizione relativamente alla controversia, possa dirsi rispettata attraverso l'esercizio della giurisdizione da parte dei giudici di tale Stato. Rimane da domandarsi se lo stesso *fair balance* possa ritenersi rispettato con l'ammettere indiscriminatamente, come la Corte di giustizia nelle sentenze *eDate* e *Bolagsupplysningen* e, ancor più, l'art. 79, par. 2, del regolamento n. 679/2016 appaiono fare, il diritto della persona che si pretenda lesa nella propria *privacy* o in un proprio diritto della personalità come il diritto alla tutela dei propri dati personali, la possibilità di convenire il presunto responsabile innanzi ai giudici del proprio paese membro di residenza abituale, anche in assenza di un collegamento altrettanto effettivo dell'attività di quest'ultimo soggetto con tale Stato.

[75] CEDU, 1° marzo 2016, *Arlewin c. Svezia*, ricorso n. 22302/10, pubblicata *on-line* al sito www.echr.coe.int, nota di F. Marchadier, *La compétence directe en matière de diffamation transfrontière*, in *Revue critique de droit international privé*, 2016, p. 560 ss.

Fiammetta Borgia
Università di Roma "Tor Vergata"

Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei

SOMMARIO: 1. L'era delle "aziende piattaforma" e la questione della trasferibilità dei dati personali verso Paesi extra-europei: il difficile bilanciamento tra diritto alla privacy, creazione di valore e necessità di sorveglianza – 2. Il "Pacchetto UE sui dati": ammissibilità e regolamentazione del trasferimento dei dati dagli Stati membri dell'Unione europea verso Paesi terzi – 3. Profili critici delle decisioni di adeguatezza della Commissione: dal "Safe Harbour" al "Privacy Shield" – 4. Le clausole contrattuali standard – 5. Le norme vincolanti d'impresa – 6. Cenni sulla direttiva PNR e gli accordi internazionali tra UE e Stati terzi – 7. Osservazioni conclusive.

1. L'era delle "aziende piattaforma" e la questione della trasferibilità dei dati personali verso Paesi terzi: il difficile bilanciamento tra diritto alla privacy, creazione di valore e necessità di sorveglianza

Il tema della raccolta, utilizzo e trasferimento dei dati personali costituisce una argomento particolarmente delicato e complesso per il diritto, sia interno che sovranazionale, soprattutto in rapporto al necessario equilibrio con la protezione dei diritti di libertà che il loro utilizzo impone[1].

[1] Recentemente, anche l'Assemblea generale delle Nazioni Unite, si è occupata della questione. In particolare, nel novembre 2016, la Terza Commissione dell'Assemblea generale ha espresso la necessità di rispettare e proteggere il diritto alla riservatezza, anche nel contesto delle comunicazioni digitali, chiedendo agli Stati di rendere rivedere le proprie legislazioni, pratiche e procedure per assicurare

La necessità di bilanciamento, tra la tutela di tali diritti e l'utilizzo dei dati personali, diviene poi imprescindibile ove si consideri la recente ed esponenziale diffusione delle cosiddette "aziende-piattaforma" [2]. Si tratta di imprese multinazionali, con sedi in diversi Paesi, che utilizzano la tecnologia per collegare individui, modelli organizzativi e beni in una rete complessa e interattiva, capace di conservare, trasferire e utilizzare una notevole quantità di informazioni ottenute proprio grazie alla navigazione sulle piattaforme digitali. Per tali imprese, è proprio il patrimonio di dati e collegamenti a diventare merce di scambio sul mercato o, in altri termini, creazione di valore.

Se quindi dal punto di vista economico, la diffusione pervasiva e globale dell'interazione digitale ha il merito di generare nuovi e forse inaspettati profitti, è innegabile che, dal punto di vista giuridico, tali scambi di informazioni tra imprese, anche appartenenti al medesimo gruppo aziendale ma a diversi ordinamenti giuridici, pongono crescenti questioni, soprattutto in considerazione della tutela di quei valori e diritti che, seppur sempre più comuni (si pensi alla salvaguardia dei diritti e delle libertà fondamentali), continuano a ricevere differenti livelli di protezione nei diversi ordinamenti giuridici nazionali[3].

---

un'applicazione effettiva degli obblighi derivanti dalle norme internazionali a tutela dei diritti umani, con particolare riferimento alla privacy e alle imprese di sviluppare norme di trasparenza e *disclosure* sulle pratiche utilizzate in materia di dati personali. Cfr. A/C.3/71/L.39/Rev.1 del 16.11.2016. D'altra parte, già nella risoluzione n. 68/167 del 2013 l'Assemblea generale aveva espresso profonda preoccupazione per l'impatto negativo che la sorveglianza e l'intercettazione delle comunicazioni possono avere sui diritti umani (UN Doc. A/RES/68/167 del 21.1.2014).

[2] Per un'interessante ed esaustiva descrizione del fenomeno si veda tra tutti: G.G. PARKER, M.W. VAN ALSTYNE, S.P. CHOUDARY, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*, New York. Norton & Co., 2016.

[3] Su questi temi si veda, fra gli altri, O. BASSINI, M. POLLICINO, *Reconciling right to be forgotten and freedom of information in the digital age: past and future of personal data protection in the EU*, in *Diritto pubblico comparato europeo*, 2014, p. 640 ss.; C. GAYREL, J. HERVEG, J-M. VAN GYSEGHEM, *La protection des données à caractère personnel en droit européen*, in *Journal européen des droits de*

D'altra parte, è necessario poi considerare che la velocità e la quantità di dati disponibile nelle comunicazioni digitali ha certamente accentuato e favorito le attività di controllo e sorveglianza sugli individui degli Stati che, soprattutto sotto la minaccia del terrorismo internazionale, hanno talvolta travalicato e violato gli stessi limiti delle libertà personali[4]. A tal proposito, ad esempio, è innegabile che la vicenda "PRISM" – legata al programma statunitense di sorveglianza delle comunicazioni rivelato nel giugno 2013 da Edward Snowden – oltre ad aver evidenziato i contrasti tra Unione europea e Stati Uniti in materia di protezione e trasferimento dei dati personali, ha finito per riaccendere l'allarme "sorveglianza globale" di orwelliana memoria[5].

---

l'homme, n°16/1, 2016, p. 98 ss.; E. DE BUSSER, *Private Companies and the Transfer of Data to Law Enforcement Authorities: Challenges for Data Protection*, in *Maastricht Journal of European and Comparative Law*, vol. 23, n. 3, 2016, pp. 478 ss.

[4] Si tratta spesso di violazioni del diritto alla privacy, riconosciuto a livello internazionale da numerosi strumenti. Basti ricordare a livello universale l'art. 12 della Dichiarazione universale sui diritti umani, l'art. 17 del Patto internazionale sui diritti civili e politici, l'art. 16 della Convenzione sui diritti dell'infanzia, l'art. 14 della Convenzione internazionale sulla protezione di tutti i lavoratori migranti e membri delle loro famiglie, nonché a livello regionale l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, l'art. 11 della Convenzione americana sui diritti dell'uomo, l'art. 18 della Dichiarazione del Cairo sui diritti umani nell'Islam, l'art. 16 e 21 della Carta araba dei diritti umani: articoli 16 e 21, l'art. 19 della Carta africana sui diritti e il benessere del fanciullo e l'art. 21 della Dichiarazione dei diritti umani dell'associazione delle Nazioni del Sud-Est asiatico. Si ricordi, infine, la Convenzione del Consiglio d'Europa per la tutela delle persone in materia di trattamento automatico dei dati personali, il Protocollo aggiuntivo alla Convenzione per la protezione degli individui in materia di trattamento automatico dei dati personali in materia di autorità di vigilanza e flussi transfrontalieri di dati, la Raccomandazione n. R (99) 5 del Consiglio d'Europa per la protezione della privacy su Internet e la normativa europea in materia, oggetto di questo scritto.

[5] Le rivelazioni di Edward Snowden, pubblicate per la prima volta il 5 giugno 2013 da parte del giornale britannico *The Guardian* hanno dato origine allo scandalo "Datagate", nel corso del quale è venuta alla luce la raccolta di metadati da parte dell'Agenzia per la sicurezza nazionale statunitense sulle telefonate dei clienti dell'operatore *Verizon*. A ciò ha seguito tutta una serie di rivelazioni circa un vero

Proprio tali circostanze, da un lato di natura privatistica, con riferimento alle attività delle imprese piattaforma, e dall'altra pubblicista, con riferimento ai programmi di sorveglianza e intelligence statale, hanno fatto da teatro per la nota vicenda Schrems[6], che in Europa ha contribuito a rianimare l'annoso dibattito sul trasferimento dei dati personali verso i Paesi extra-europei. Ciò ha, dunaque, accelerato la necessaria riformulazione della disciplina europea a protezione dei dati personali, nonché la "demolizione" del c.d. "Safe Harbour" e l'adozione di

---

e proprio sistema di controllo e monitoraggio gestito dalla medesima agenzia governativa, in collaborazione con le più importanti compagnie telefoniche e operatori Internet. Si veda sul A. DI CORINTO, L. REITANO, *Digito ergo spio, le armi del mestiere*, in *Limes*, luglio 2014; F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it*, n. 13, 2013.

[6] Cfr. Corte di giustizia, sentenza 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, EU:C:2015:650, punti 73-74. Per un commento alla sentenza "Schrems" si veda: 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*,* p. 779 e ss.; A MANTELERO, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per i cittadini ed imprese?,* in *Contratto e impresa / Europa*, 2015, p.719 e ss.; V. SALVATORE, *La Corte di giustizia restituisce (temporaneamente) agli Stati membri la competenza a valutare l'adeguatezza del livello di protezione dei dati personali soggetti a trasferimento verso gli Stati Uniti,* in *Studi sull'integrazione europea*, 2015, p. 623 e ss.; V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems : la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in *Il diritto dell'informazione e dell'informatica*, 2015, p. 683 e ss., L. AZOULAI, S., M. VAN DER, *Institutionalizing personal data protection in times of global institutional distrust: Schrems,* in *Common Market Law Review,* 2016, p. 1343 e ss.; R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy,* in *Giur. cost.*, 2016, p. 289 e ss.; B. CAROTTI, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa,* in *Giornale dir. amm.*, 2016, p. 333 e ss.; A. GIATTINI, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso Schrems e l'invalidità del sistema di "approdo sicuro",* in *Diritti umani e diritto internazionale,* 2016, p. 247 e ss.; M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il diritto dell'Unione Europea*, 2016, p.755 e ss.; G. SCARCHILLO, *Dal Safe Harbor al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems,* in *Diritto del commercio internazionale,* 2016, p. 901 e ss.

una nuova decisione di adeguatezza relativa al trasferimento di dati negli USA (Privacy Shield)[7].

Il 2016, dunque, ha segnato in Europa l'entrata in vigore di un pacchetto di norme in materia: il regolamento n. 679[8], che il 6 maggio 2018 andrà a sostituire la direttiva n. 46 del 1995[9], la direttiva n. 680[10], che sostituirà il 25 maggio dello stesso anno la decisione quadro GAI n. 977 del 2008[11], e la direttiva n. 681 (c.d. direttiva PNR)[12], primo intervento in materia del legislatore europeo che dovrà essere recepita entro il maggio 2018.

Per quanto concerne il Regolamento n. 679 del 2016, la finalità espressa degli interventi normativi è quella di assicurare che i dati per-

[7] Infatti, la Corte di Giustizia europea con la sentenza del 6 ottobre 2015 ha dichiarato invalida la decisione di adeguatezza relativa al trasferimento di dati negli USA (c.d. Safe Harbour) ed ha spinto la Commissione europea nell'agosto 2016 ad adottare il c.d. Privacy Shield, che sostituisce il precedente strumento per la protezione dei dati personali.

[8] Cfr. 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), in GU L 119 del 4 maggio 2016, pp. 60-65

[9] Cfr. 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, in GU L 281 del 23 novembre 1995, p. 31-39.

[10] Cfr. Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in GU L 119 del 4 maggio 2016, pp. 89-131.

[11] Cfr. Decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, in GU L 350 del 30 dicembre 2008, p. 60-71.

[12] Cfr. Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, in GU L 119, del 4 maggio 2016, pp.132–149.

sonali dei cittadini europei continuino a beneficiare di un elevato standard di protezione, anche nell'ipotesi in tali dati siano trasferiti al di fuori del territorio degli Stati membri, in un'ottica di applicazione extraterritoriale della normativa europea[13].

Il principale mezzo scelto dalla direttiva del 1995 e dagli accennati interventi normativi del 2016 per garantire i diritti di libertà è quello di impedire il trasferimento di dati personali allorquando lo Stato destinatario del flusso di dati non offra un adeguato livello di protezione e, viceversa, di consentirlo soltanto laddove lo Stato terzo di destinazione assicuri, invece, detto standard di tutela.

Ad un esame più attento della disciplina, tuttavia, l'impedimento al trasferimento avviene raramente.

È innegabile, infatti, che al di là delle enunciazioni di principio, l'attenzione del legislatore europeo si sia piuttosto concentrata sull'esigenza di evitare che il trasferimento di dati tra Stati sia intralciato dall'esistenza di difformità normative ed incertezze giuridiche, piuttosto che garantire un effettiva e concreta protezione dei diritti di libertà (e quindi a volte il divieto di trasferimento). Ciò in una duplice prospettiva: a livello interno, al fine di assicurare la libera circolazione dei dati per un migliore funzionamento del mercato comune europeo[14], mentre all'esterno, al fine di rafforzare i rapporti commerciali con i Paesi terzi. È indubbio, dunque, che la possibilità concreta di impedire il flusso frontaliero dei dati viene di fatto esclusa nell'applicazione della normativa europea, soprattutto se si vuole evitare l'isolamento commerciale

[13] L. ZAGATO, *Il trasferimento di dati personali verso stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*, in *Diritto del Commercio internazionale*, 2008, n. 2, p. 297 ss. La produzione normativa europea ha in altri termini finito per generare "esternalità giuridiche", del tutto simili a quelle che gli Stati Uniti hanno in passato prodotto attraverso la loro egemonia economica. richiedendo e talvolta pretendendo dagli altri Stati risposte politiche (o legislative) per difendersi dall'impatto extraterritoriale degli strumenti di politica interna USA.

[14] P. PALLARO, *Rapporti Commerciali tra UE e Stati Terzi e la questione della tutela dei dati personali. Il difficile confronto UE-USA*, in *Diritto del Commercio internazionale* 2000, n.3, p. 753 ss.

dell'Europa[15]. Tale atteggiamento, definito da taluni "progressista"[16], forse in maniera troppo ottimistica, appare inoltre confermato dal considerando n. 101 del regolamento, secondo il quale i flussi dei dati verso e da Paesi al di fuori dell'Unione sono "necessari" per l'espansione del commercio internazionale e della cooperazione internazionale.

Ne deriva allora che il regolamento finisce per operare già a monte una scelta nel bilanciamento degli interessi dell'Unione e l'effettiva garanzia di un livello "elevato" di protezione dei dati personali, a favore della promozione – e non certo del rallentamento – del trasferimento di dati personali intra ed extraeuropeo.

In particolare, ciò che appare particolarmente rischioso in tema di garanzia dei diritti di libertà è proprio l'obiettivo "di appianare le divergenze" tra ordinamenti, piuttosto che ostacolare o controllare il flusso di dati transfrontalieri. Ciò soprattutto ove si consideri la nozione ormai pacifica e restrittiva di trasferimento[17], secondo la quale non costituisce trasferimento l'inserimento di dati personali da parte di un soggetto stabilito nell'Unione, in una pagina internet, caricata presso un *web hosting provider* stabilito nell'Unione, anche quando i dati così inseriti divengano accessibili da Paesi terzi, nonché le criticità nell'applicazione un po' troppo indulgente delle decisioni di adeguatezza e le altre deroghe espresse al divieto di trasferimento, presenti nel regolamento: dalle clausole contrattuali standard alle norme vincolanti d'impresa.

Evidentemente tutto ciò finisce per essere in antitesi con le premesse e le esigenze di riforma del sistema, a discapito dei diritti di libertà che si volevano in principio garantire in maniera più efficace.

---

[15] G. M. RICCIO, *Model Contract Clauses e Corporate Binding Rules: valide alternative al safe arbor agreement?,* in *Il diritto dell'informazione e dell'informatica,* 2015, p. 215 e ss, in part. pag. 219.

[16] D. PITTELLA, *Trasferimento verso Paesi terzi*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, 2016.

[17] Cfr. Corte di giustizia, sentenza 6 novembre 2003, ***Lindqvist*,** causa C-101/01, in Racc. 2003 p. I-12971 ss, punti 69-70.

A completamento di questa prima disamina sul trasferimento dei dati personali verso Paesi extraeuropei e a conferma del quadro piuttosto critico sin qui offerto, è infine utile ricordare che simili e congenite compressioni dei diritti di libertà sono altresì previste nella Direttiva PNR, giacché la stessa finisce in definitiva per autorizzare una raccolta indiscriminata e generalizzata di dati personali, trasferiti anche verso Stati extra-europei, permettendo una notevole ingerenza nella privacy di qualsiasi individuo[18].

2. Il "Pacchetto UE sui dati": ammissibilità e regolamentazione del trasferimento dei dati dagli Stati membri dell'Unione europea verso Paesi terzi

Per quanto concerne l'analisi della disciplina oggetto di tale commento, l'articolo cardine del sistema è costituito dall'art. 45 del Regolamento 679/2016, secondo il quale il trasferimento di dati personali da Stati membri dell'Unione europea verso Paesi extra-europei o un'organizzazione internazionale, ossia non appartenenti all'UE o allo Spazio Economico Europeo, è consentito solo quando il destinatario in questione garantisca un livello di protezione "adeguato" [19]. In tal caso, evidentemente, il trasferimento dei dati non necessita di autorizzazioni specifiche.

---

[18] F. DI MATTEO, *Una raccolta indiscriminata e generalizzata dei dati personali: un vizio congenito nella direttiva PNR?*, in *Diritti umani e diritto internazionale*, vol. 11, 2017, p. 213 ss., part. pp. 222-223.

[19] Cfr. art. 25 della Direttiva e art. 45 del Regolamento 679. Al riguardo la Corte di giustizia, nella sentenza Schrems aveva già chiarito che l'espressione «livello di protezione adeguato» figurante all'articolo25, paragrafo 6, della direttiva 95/46/CE, pur non implicando un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, deve essere intesa nel senso che esige che il paese terzo assicuri un livello di protezione delle libertà e dei diritti fondamentali «sostanzialmente equivalente» a quello garantito all'interno dell'Unione in forza della direttiva 95/46/CE, letta alla luce della Carta dei diritti fondamentali. Si noti, tuttavia, che anche se gli strumenti dei quali tale Paese terzo si avvale al riguardo possono essere

L'organo che ha il potere di stabilire tale adeguatezza è la Commissione, attraverso uno specifico atto di esecuzione. Si tratta di uno strumento avente ad oggetto, come si vedrà meglio in seguito, una valutazione piuttosto sommaria degli ordinamenti degli Stati terzi, che però è vincolante per gli Stati membri dell'Unione, con la quale la Commissione stabilisce che il livello di protezione offerto in un determinato Paese è "adeguato", e che pertanto è possibile trasferirvi dati personali.

L'operato della Commissione, seppure molto ampio, non è però del tutto discrezionale. Il legislatore europeo stabilisce, infatti, dei parametri a mezzo dei quali la Commissione compone tale valutazione: in particolare, rispetto alla direttiva, che prevedeva tale giudizio caso per caso tenendo conto di varie circostanze, il regolamento limita tale discrezionalità e offre degli elementi di dettaglio che assistono la Commissione, limitandone la discrezionalità, così come d'altro canto era stato richiesto dalla Corte di giustizia nella già citata sentenza Schrems.

Tuttavia, anche se la decisione di adeguatezza, nell'attuale riforma, viene meglio delineata, resta il problema del fondamento stesso ti tale strumento. Il requisito dell'adeguatezza, infatti, nella volontà del legislatore europeo, non implica un raffronto tra sistemi di protezione dei diritti di ordinamenti diversi, ma si ferma piuttosto alla cosiddetta "equivalenza" che, sempre in quest'ottica piuttosto ottimista, consentirebbe agli Stati di utilizzare diverse vie per garantire l'effettiva protezione dei dati personali. In altri termini, la prova diabolica che si chiede alla Commissione è quella di operare una valutazione *ex ante* dell'ordinamento del Paese terzo (*rectius* dell'effettività *ex ante* dell'ordinamento dello Stato terzo in materia di tutela dei diritti), nonché la facoltà di operare un successivo controllo e un eventuale riesame periodico del provvedimento adottato[20].

---

diversi da quelli attuati all'interno dell'Unione, tali strumenti devono cionondimeno rivelarsi efficaci nella prassi (punti 73-74 della già citata sentenza).

[20] Il Regolamento prevede, infatti, un meccanismo di revisione periodica ogni quattro anni.

L'obbligo di monitoraggio della normativa di riferimento del Paese terzo dove sono trasferiti i dati è volto ad individuare eventuali modifiche, nell'ordinamento giuridico dello Stato di destinazione, che possono influire sulle decisioni di adeguatezza già adottate in modo da poterle sottoporre a revoca o modifica. Tuttavia, anche questo sistema di monitoraggio presenta indiscutibili limiti: così come l'accertamento *ex ante*, anche il controllo *ex post* dell'adeguatezza è, infatti, attribuito in via esclusiva alla Commissione, mentre agli Stati resta unicamente la possibilità di adire la Corte di giustizia in caso di inerzia della Commissione o illegittimità della sua decisione.

A tale quadro di incertezza, si aggiunga che in mancanza della decisione di adeguatezza, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall'articolo 46 del regolamento, cioè sulla base di "garanzie adeguate".

Quest'ultime possono essere distinte in due categorie, a seconda che sia necessaria o meno un'autorità di controllo. Nel primo caso, il trasferimento avviene senza specifica autorizzazione a condizione che lo Stato terzo (o l'organizzazione) offra garanzie adeguate che possono consistere in: i) uno strumento vincolante che sia stato approvato dall'autorità nazionale di controllo, ii) norme vincolanti d'impresa, iii) clausole standard di protezione dei dati, adottate dalla Commissione o iv) da un'autorità di controllo nazionale e approvate dalla Commissione, v) codice di condotta con l'impegno vincolante del destinatario dei dati ad applicare le garanzie adeguate, vi) il c.d. sigillo europeo di protezione dei dati, un contrassegno concesso a soggetti appartenenti a stati terzi da parte di organismi di certificazione a livello nazionale ai sensi dell'art. 43 del regolamento[21]. Nel secondo caso, costituiranno garanzie

[21] Si noti che la prassi di certificazione, effettuata da un ente imparziale e terzo di standardizzazione e avallata come *best practice* dallo stesso Gruppo Art. 29, non è stata recepita dal regolamento. Si pensi alla norma ISO 27018, standard internazionale per certifica il rispetto dei principi e delle norme privacy, da parte dei fornitori di servizi *public cloud*.

adeguate, dopo la necessaria autorizzazione rilasciata dall'autorità di controllo: i) le clausole contrattuali tra il responsabile o l'incaricato del trattamento e il destinatario di tali dati o ii) le disposizioni da inserire in accordi amministrativi tra autorità o organismi pubblici.

Infine, il regolamento prevede eccezionalmente la possibilità di trasferire verso stati extra-europei che non garantiscano un livello adeguato di protezione. Si tratta di una serie di ipotesi previste nell'art. 59 del Regolamento, che vanno dal consenso informato dell'individuo titolare dei dati, alla necessità di concludere un contratto alla ammissibilità del trasferimento per pubblico interesse.

È di tutta evidenza, dunque, sin dalla semplice lettura degli articoli della novellata disciplina e della struttura stessa del regolamento, che quelle che dovrebbero essere eccezioni al "divieto di trasferimento" in mancanza di un'adeguata protezione dei diritti di libertà degli utenti nei Pesi terzi, siano in realtà così numerose che finiscono per svuotare quasi interamente di significato la nuova regolamentazione europea, che avrebbe dovuto garantire una tutela efficace dei diritti di libertà al di là dei confini dell'Unione europea, addirittura in un'ottica extraterritoriale.

3. Profili critici delle decisioni di adeguatezza della Commissione: dal Safe Harbour al Privacy Shield

Ad oggi il numero degli Stati per i quali la Commissione ha adottato le decisioni di adeguatezza alla luce della vecchia normativa è esiguo[22]. Inoltre, gli strumenti adottati sono destinati a rimanere in vigore sino

[22] Si tratta in particolare delle seguenti decisioni: Andorra 2010/625/EU, Argentina 2003/490/EC, Canada 2002/2/EC, Svizzera 2000/518/EC, Isole Faroe 2010/146/EU, Guernsey 2003/821/EC, Israele 2011/61/EU, Isola di Man 2004/411/EC, Isola di Jersey 2008/393/EC, Nuova Zelanda 2013/65/EU, Uruguay 2012/484/EU, Stati Uniti d'America 2000/520/EC e 2016/1250/EU.

alla emanazione di nuovi giudizi sulla base dell'art. 45 del regolamento del 2016.

In attesa della rielaborazioni delle decisioni di adeguatezza già esistenti è possibile in ogni caso fare qualche osservazione. In particolare, non solo appare piuttosto controversa non solo l'efficacia giuridica di tali strumenti, ma anche poco definito il loro contenuto, che presenta numerosi punti critici.

Per quanto attiene al primo profilo, si tratta generalmente di una serie di atti unilaterali adottati dalla Commissione e (talvolta) dalla Commissione e dagli Stati terzi, diretti a regolare il traffico transfrontaliero di dati. Con riferimento a quest'ultima ipotesi, tuttavia, è evidente, che tali atti, anche quando sottintendono obbligazioni sinallagmatiche tra Unione e Stati terzi, non possano in ogni caso essere considerati alla stregua di accordi in forma semplificata. Infatti, né l'Unione né gli Stati terzi, in alcuno degli atti menzioinati, hanno mai espresso la volontà di concludere un accordo internazionale[23], né è utilizzata la procedura di cui all'art. 218 TFUE, che prevede peraltro la previa approvazione del Parlamento europeo[24]. Essi rimangono, dunque, in entrambi i casi atti secondari dell'Unione vincolanti per gli Stati membri (o persone fisiche e giuridiche degli Stati membri)[25], con una (ovvia) scarsa incidenza all'esterno, verso i Paesi terzi.

[23] Cfr. art. 12 e 13 della Convenzione di Vienna sul diritto dei trattati.

[24] L'articolata disciplina per la conclusione degli accordi internazionali tra l'Unione europea ed i Paesi terzi, nonché le organizzazioni internazionali, è contemplata agli artt. 218, 219 e 207 del Trattato sul funzionamento dell'Unione europea (TFUE), coinvolgendo tutte le istituzioni del processo legislativo dell'Unione, la Corte di giustizia, e l'Alto Rappresentante per gli affari esteri e la politica di sicurezza (AR). Sul punto si veda per tutti E. BARONCINI, *L'Unione europea e la procedura di conclusione degli accordi internazionali dopo il Trattato di Lisbona*, in Cuadernos de *Derecho Transnacional*, 2013, vol. 5, n. 1, p. 5-37, in part. pag. 14 dove si sottolineano i nuovi e decisivi poteri del Parlamento europeo in materia di accordi internazionali, anche con riferimento alla "bocciatura" degli accordi SWIFT del 2009.

[25] Cfr. Corte di Giustizia, sentenza 14 aprile 2011, causa C-327/09, Mensch und Natur AGL dove la Corte di giustizia ha chiarito che: «Una decisione della Com-

Per quanto attiene al secondo profilo, cioè quello dei contenuti, tra le decisioni di adeguatezza, la più nota è quella n. 520 del 26 luglio 2000, fondata sui *Safe Harbour Principles*, che ha consentito il trasferimento dei dati tra Unione europea e Stati Uniti, fino alla sentenza "Schrems" della Corte di giustizia del 2015, decisione poi sostituita nel 2016 dal EU-US Privacy Shield[26].

La vicenda merita un breve approfondimento. Nel 2008, lo studente austriaco Maximilian Schrems si convince che alcuni dei dati personali immessi dagli utenti sulla piattaforma di Facebook vengano trasferiti dai server della società irlandese controllata da Facebook verso server ubicati negli Stati Uniti, dove sono oggetto di trattamento in contrasto con la normativa europea, senza che sia garantito un livello adeguato di protezione dei dati personali. Dopo aver proposto ricorso presso l'Autorità per la protezione dei dati irlandese, lamentando di aver subito un trattamento dei sui dati non adeguato, ed essersi visto rigettare il ricorso sulla base della decisione di adeguatezza della Commissione n. 520 del 26 luglio 2000 (c.d. Safe Harbour), Schrems decide di adire l'Alta Corte irlandese, che a sua volta propone un rinvio pregiudiziale alla Corte di giustizia europea.

Nella sentenza del 2015, la Corte di Giustizia ha ribadito il ruolo cardine della Commissione nel giudizio di adeguatezza: quest'ultima avrebbe dovuto verificare se gli Stati Uniti avessero assicurato di fatto un livello di protezione dei diritti fondamentali in materia di dati personali essenzialmente "equivalente" a quello garantito all'interno dell'Unione Europea. A tale scopo, secondo la Corte, non sarebbe stato sufficiente che la Commissione esaminasse in astratto il c.d. "schema di

---

missione [...] non è vincolante per soggetti diversi dalla persona o dalle persone che essa designa come destinatari».

[26] Cfr. Decisione di esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, notificata con il numero C(2016) 4176, in Gazzetta ufficiale dell'Unione europea L 207/6 IT del 1.8.2016

approdo sicuro", ma sarebbe stato invece necessario valutare in concreto il rispetto effettivo dei diritti garantiti dall'ordinamento statunitense.

La Corte ha rilevato, dunque, che la previsione – contenuta nel Safe Harbour – di una semplice adesione volontaristica a principi relativi alla protezione dei dati da parte di soggetti con sede negli Stati Uniti ha reso non solo possibile la compressione di diritti fondamentali da parte delle autorità pubbliche americane, come di fatto è accaduto, ma ha mancato anche di prevedere effettive tutele giurisdizionali che potessero evitare tali interferenze[27].

Nella ricostruzione della Corte, è ben chiaro, tuttavia, che la protezione del diritto fondamentale al rispetto della vita privata impone che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario[28]. Nel caso specifico, tali deroghe non erano certamente strettamente necessarie dal momento che consentivano alle autorità pubbliche statunitensi di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche, in contrasto con il contenuto essenziale del diritto fondamentale al rispetto della vita privata, garantito dall'articolo 7 della Carta dei diritti fondamentali[29].

A seguito di queste considerazioni, enunciate dalla sentenza della Corte europea, 12 luglio 2016, la Commissione ha adottato una decisione fondata sui nuovi principi contenuti nel c.d. *Privacy Shield*, riconoscendo nuovamente l'adeguatezza della tutela offerta dall'ordinamento statunitense.

Dal punto di vista formale, si tratta pur sempre di una serie di atti di organi governativi statunitensi e dalla decisione di adeguatezza della

[27] Le medesime preoccupazioni emergevano in due Comunicazioni della Commissione UE: la Comunicazione "Ricostruire la fiducia UE-USA nello scambio dei dati personali" (COM2013/846 del 27 Novembre 2013) e la Comunicazione della Commissione europea al Parlamento europeo sul funzionamento del Safe Harbour dalla prospettiva dei cittadini europei e delle imprese con sede nell'Unione Europea (COM2013/847 del 27 Novembre 2013).
[28] Cfr. la sentenza Schrems, punto 92 e la giurisprudenza ivi citata.
[29] *Ibidem*, punto 94.

Commissione del 2016, che non possono essere assimilati a un vero e proprio accordo internazionale su base consensuale. Rispetto alla precedente versione, è però rafforzata l'adesione volontaria delle imprese impegnate nel trasferimento ad una serie di principi a tutela dei diritti fondamentali al fine di ottenere una certificazione, utile alla ricezione e gestione dei dati personali provenienti dall'UE. Si tratta, tuttavia, di rassicurazioni e garanzie offerte dal governo americano, che pur suggerendo tale adesione continuano ad avere natura meramente politica. Per quanto riguarda i meccanismi di controllo, gestiti da alcuni dipartimenti dell'esecutivo statunitense, questi soffrono, di scarsa chiarezza in ordine alle modalità di svolgimento, alle possibili conseguenze in caso di risultato negativo, nonché in materia di finanziamento.

Dal punto di vista dei contenuti, nel *Privacy Shield* permangono alcune criticità, sia considerato come sistema complessivo che riguardo alle singole ipotesi di deroga al divieto di trasferimento previste[30].

Una questione generale che rimane sostanzialmente aperta, infatti, è quella del rispetto delle c.d. *European essential guarantees*[31]. Infatti, secondo l'ordinamento europeo, è ammissibile una eventuale compressione dei diritti fondamentali unicamente nel caso in cui siano sin ogni caso soddisfatte quelle garanzie ricavate dalla giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo, incentrate sul

[30] Il *Privacy Shield* prevede la possibilità di derogare ai principi sul trattamento dei dati personali quando: a) ciò sia necessario per soddisfare esigenze di sicurezza nazionale, di interesse pubblico o di applicazione della legge; b) la legge (così come una giurisprudenza costante) imponga un obbligo confliggente con i principi o autorizzi l'organizzazione a discostarsi dal rispetto di tali principi, purché l'organizzazione dimostri che le misure in deroga sono strettamente funzionali al raggiungimento degli obiettivi perseguiti dalla norma confliggente; c) quando eccezioni o deroghe previste dalla Direttiva 95/46 o dalle leggi degli Stati membri dell'Unione siano applicabili per analogia al contesto ("*in a comparable context*") in cui opera l'organizzazione statunitense..

[31] Cfr. Gruppo di lavoro articolo 29 per la protezione dei dati, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 aprile 2016.

rispetto del principio di legalità, sulla rispondenza delle deroghe ai criteri di necessità e proporzionalità e sulla sussistenza di adeguati meccanismi di tutela (non necessariamente giurisdizionali) nelle ipotesi di lesione dei diritti dei singoli.

Si tratta, dunque, di verificare se – nelle ipotesi di deroga previsti dallo "scudo" – tali principi siano rispettati.

Dalla decisione della Commissione e dalla stessa giurisprudenza europea si può ritenere che le deroghe in astratto rimangano nell'ambito delle c.d. garanzie essenziali e siano dunque perfettamente ammissibili, anche se è innegabile che la loro formulazione è ancora eccessivamente ampia e dai contorni incerti. In ogni caso, i dubbi permangono quando la valutazione da astratta diventa concreta: quando cioè è necessario esaminare in concreto il tipo di lesione e l'asserito rispetto dei principi europei procurata (ad esempio al diritto alla privacy). Si tratta, infatti, di valutazioni che la Commissione è in grado di effettuare solo ex post, nella fase di controllo della decisione di adeguatezza, mentre la tutela effettiva della lesione dei diritti di libertà potrà essere oggetto di ricorso davanti alla Corte di giustizia, ma sempre successivamente.

Quanto alle singole ipotesi di deroga espressamente previste, quella che desta particolare perplessità è la possibilità di ricorrere a strumenti di sorveglianza di massa da parte agenzie di *intelligence* statunitensi, ipotesi questa già consentita dal Privacy Harbour, ma in questo caso ristretta a specifiche ipotesi. Tale deroga appare particolarmente problematica ove si consideri la possibilità di fare ricorso alla c.d. *bulk collection of data*, vale a dire la raccolta e la conservazione indiscriminata su larga scala di dati e informazioni personali. Tale pratica, allorché sia assimilabile a *mass surveillance,* appare di per sé stessa incompatibile con il principio di proporzionalità[32]. In tale circostanza, il fatto che ad essa si faccia ricorso in circostanze eccezionali è del tutto irrilevante ai fini dell'inammissibilità o quantomeno della criticità della deroga.

[32] v. UN High Commissioner for Human Rights, Report on The right to privacy in the digital age, par. 25, nonché il parere dell'*Article 29 Working Party*, par. 3.3.

Altra questione irrisolta è poi quella della compatibilità di intercettazioni massive con i principi di necessità e proporzionalità, come recentemente interpretati nella sentenza *Schrems*[33]. Se tale forma di intercettazione appare astrattamente legittima anche allo sguardo della Corte di Strasburgo, proprio in considerazione della necessità della lotta la terrorismo internazionale[34], dubbi affiorano invece ove si consideri che la legislazione statunitense basa proprio la legittimità delle intercettazioni sulla raccolta di dati indiscriminata di cui sopra[35].

Infine, un ulteriore elemento di criticità della decisione di adeguatezza in esame è posto dal c.d. "trasferimento successivo" *onward transfers*), ossia del trasferimento di dati di origine UE da un operatore statunitense verso un Paese terzo.

In tal caso, l'operatore statunitense – che abbia aderito al *Privacy Shield* – è tenuto a concludere un contratto con il controllore ricevente che ha sede nel Paese terzo, con il quale quest'ultimo si impegna a utilizzare i dati ricevuti per una finalità specifica e definita e a garantire una tutela equivalente a quella garantita dai principi del *Privacy Shield*[36]. Se però tali dati saranno poi raccolti dal Paese terzo nell'ambito di attività di *intelligence* la disciplina non è chiara: secondo

[33] Cfr. sentenza Schrems, cit., punto 93. In senso contrario, tuttavia, si è recentemente espresso l'Avvocato generale Saugmandsgaard Øe, nella causa Tele2 Sverige, ritenendo che la possibilità di una raccolta e di una conservazione generalizzata di dati personali non possa ritenersi a priori incompatibile con il requisito di proporzionalità, dovendosi di volta in volta ponderare i vantaggi connessi ad operazioni di sorveglianza massiva con i rischi da questa derivanti per i diritti fondamentali degli individui.

[34] v. Corte EDU, *Zakharov v. Russia*, par. 264

[35] Il problema, però, potrebbe essere risolto dalla giurisprudenza in un futuro prossimo, poiché, sia davanti alla Corte EDU (ric. n. 58179/13, ric. n. 62322/14, ric. n. 24960/15) che davanti alla Corte di giustizia (cause riunite C-203/15 e C-698/15; v. anche la richiesta di parere A-1/15 in merito all'accordo con il Canada sui codici di prenotazione dei passeggeri), pendono ricorsi aventi ad oggetto la legittimità dei programmi di sorveglianza di massa.

[36] Regole analoghe, che non necessitano però di un regime contrattuale ad hoc, sono previste quando il soggetto ricevente nel paese terzo operi come agente di un'organizzazione statunitense.

il parere dell'*Article 29 Working Party*, le regole in materia di trasferimenti successivi dovrebbero comunque trovare applicazione, quantomeno nel senso di richiedere, all'organizzazione che trasferisce dati UE in un paese terzo, di valutare il livello di tutela offerto dall'ordinamento di quel paese e, se del caso, di sospendere il trasferimento, dopo aver informato il titolare del trattamento. Quando invece sia lo stesso responsabile del trattamento di origine UE a conoscere i rischi di un eventuale successivo trasferimento verso un paese terzo e lo autorizzi ugualmente, o partecipi direttamente al trasferimento di dati, tale trasferimento si configurerà come trasferimento di dati direttamente dall'UE verso lo Stato terzo e quindi sottoposto alla disciplina europea in materia.

Rimane oscuro in ogni caso quali regole siano applicabili al trasferimento di dati da una pubblica autorità statunitense ad un altro soggetto pubblico di un paese terzo.

In conclusione, anche se il *Privacy Shield* costituisce un avanzamento rispetto al sistema precedente, attraverso impianto normativo più dettagliato, le numerose deroghe continuano a svuotare dall'interno il sistema di protezione dei diritti fondamentali approntato dal legislatore europeo. Inoltre, la possibilità di controllo da parte dell'*intelligence* solleva alcuni dubbi quanto alla conformità con le garanzie di terzietà ed indipendenza dello strumento in esame. Infine, la stessa possibilità conferita agli individui agire di fronte al Dipartimento di Stato per ottenere un rimedio a fronte della violazione del proprio diritto alla riservatezza e, contestualmente, il *Judicial Redress Act* del 2015, ha sì esteso anche ai cittadini europei la possibilità di agire in sede civile – di fronte al giudice statunitense – per ottenere il risarcimento del danno derivante da intercettazioni illecite, ma non ha spostato il bilanciamento tra tutela dei diritti e necessità economiche o di sorveglianza, che sembra essere rimasto a favore di un'interpretazione quantomeno disinvolta del criterio di adeguatezza sancito nel regolamento oggetto di questo commento.

4. Le clausole contrattuali standard

Le clausole contrattuali standard, così come le norme vincolanti d'impresa, sono ulteriori strumenti, previsti dal legislatore europeo, che consentono il trasferimento dei dati verso Stati terzi, anche in assenza di una decisione di adeguatezza, ma a costi transattivi più elevati[37].

Si tratta di clausole-tipo, di natura contrattuale, approvate dalla Commissione europea, che derogano al divieto di trasferimento dei dati personali tra soggetti privati non appartenenti allo stesso gruppo economico. Tali clausole, inserite nel contratto utilizzato per il trasferimento, hanno la finalità di garantire che importatore ed esportatore siano vincolati al rispetto dei principi e degli obblighi che la normativa europea individua in tema di dati personali quando il Paese extra europeo non offra garanzie "adeguate" ai sensi della normativa europea[38]. La loro previsione non esclude, infine, che gli operatori possano formulare altre clausole contrattuali *ad ho*c (quindi non standard), che in ogni caso dovrebbero garantire un livello adeguato di protezione dei dati.

In particolare, la Commissione si è resa promotrice dell'elaborazione di clausole contrattuali tipo attraverso quattro diverse decisioni – rispettivamente, del 15 giugno 2001, 27 dicembre 2001, 27 dicembre 2004 e 5 febbraio 2010 – che rivestono una particola importanza nell'ottica di semplificare i rapporti internazionali e fornire garanzie sufficienti per la tutela della vita privata e dei diritti e della libertà fondamentali delle persone, come previsto dalla normativa europea.

Quanto alla forma, le clausole contrattuali standard sono determinate con una decisione della Commissione che contiene: un allegato con le clausole standard ed uno da compilare per le parti, con i loro dettagli,

[37] Così in G.M. Riccio, cit., pag. 24.

[38] Questa modalità di trasferimento è prevista anche dal Protocollo addizionale alla Convenzione 108/81, all'art.2 comma 2(b), secondo il quale" […] each Party may allow for the transfer of personal data: if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law".

i dati trasferiti, le modalità di trattamento dei dati, l'organizzazione ed i dettagli tecnici delle misure di sicurezza che saranno implementate dall'importatore. Si tratta evidentemente di modelli diversi, da adottare a seconda della qualifica dell'importatore estero dei dati.

Per i trasferimenti da un titolare europeo del trattamento ad un importatore estero qualificato anch'esso come titolare sono previsti sostanzialmente due tipi di clausole. Il primo è stato realizzato dalla Commissione con la decisione 2001/497/CE del 15 Giugno 2001, a cui è allegato. Il secondo insieme di clausole è stato aggiunto il 27 Dicembre 2004 con la decisione 2004/915/CE80, a seguito della presentazione di un insieme alternativo di clausole contrattuali da parte di un consorzio di imprenditori. Se invece l'importatore dei dati è qualificato come responsabile del trattamento, si applicheranno clausole contrattuali apposite previste in origine dalla decisione 2002/16/CE, in seguito abrogata e sostituita dalla decisione 2010/87/UE.

Tra le clausole contrattuali approvate dalla Commissione, quest'ultima (decisione 2010/87/UE) merita particolare attenzione, in quanto disciplina i trasferimenti dal titolare del trattamento europeo al soggetto che li elabora stabilito in un Paesi terzo[39].

In tale strumento, vengono stabiliti specifici obblighi informativi nei confronti delle parti attive nel trasferimento dei dati personali: entrambe, infatti, dovranno informare i soggetti interessati che i dati personali a questi ultimi riferiti saranno oggetto di trasferimento, nonché indicare, in un'apposita appendice allegata alle clausole contrattuali, le misure tecniche ed organizzative adottate affinché il livello di sicurezza sia commisurato ai rischi inerenti il trattamento ed alla natura dei dati da tutelare.

Gli obblighi contenuti nelle clausole contrattuali standard, secondo la decisione n. 87 del 2010, dovrebbero essere rispettati anche dagli eventuali

[39] Si tratta di un fenomeno molto diffuso nella oratica degli scambi: spesso, infatti, le società europee si appoggiano ad operatori esteri che offrono servizi di *cloud computing*, *outsourcing*, *application service providing* (ASP), *software as a service* (SaaS) o *Human Resources Information System* (HRIS).

sub-processor coinvolti nel flusso dei trasferimenti, sempre attraverso strumenti contrattuali transfrontalieri che per la loro applicazione, in una fase eventualmente patologica, contano sul controllo delle corti nazionali.

Altra possibilità, sempre prevista dalla decisione in esame, è poi quella legata alla possibilità dell'importatore dei dati di sub-contrattare il trattamento: tale strumento, tuttavia, trova un'applicazione piuttosto ampia, dal momento che comprende sia l'ipotesi che la terza parte abbia accesso ai dati, in toto o a parte di essi.

I soli requisiti richiesti dalla norma per il subcontratto del trattamento sono il consenso dell'esportatore e l'imposizione al sub-responsabile degli stessi termini contrattuali previsti nel trasferimento estero. In conseguenza di ciò, l'esportatore acconsente con troppa frequenza e disinvoltura al subcontratto di determinati trattamenti come il mantenimento dei server, la conservazione dei dati o l'amministrazione delle banche dati da parte del soggetto sub-responsabile, identificato da ragione sociale ed indirizzo. Infine, per ragioni di ordine pratico, l'importatore dei dati, è portato ad ottenere un consenso più ampio, come per il subcontratto a qualunque società affiliata: in questo caso, e le parti possono addirittura decidere che l'importatore debba semplicemente notificare l'esportatore riguardo l'intenzione di affidarsi ad un certo sub-responsabile, con la conseguenza che il consenso potrà essere ricavato dalla mancata opposizione dopo un certo periodo di tempo.

La seconda condizione prevista dalla decisione del 2010 consiste nell'imposizione degli stessi obblighi gravanti sull'importatore anche sul sub-responsabile. Tuttavia, tale questo requisito può essere soddisfatto anche attraverso la co-sottoscrizione da parte del sub-responsabile del contratto intervenuto tra esportatore ed importatore dei dati. Tale possibilità apre diverse problematiche. Come si è detto in molti casi l'importatore non sub-contratta l'intero trattamento dei dati, ma solo parte di esso: è evidente, dunque, che sarà difficile stabilire con certezza quali obbligazioni saranno applicabili al sub-responsabile. Inoltre, poiché la pratica del subcontratto può riguardare diversi opera-

tori, la co-sottoscrizione potrebbe essere costruita in modo tale che il sub-responsabile sia obbligato non solo verso il proprio partner contrattuale, ma anche verso l'esportatore dei dati, nei confronti del quale non ha alcuna relazione oppure, più frequentemente, che la ripartizione degli obblighi e delle responsabilità sul trasferimento e trattamento dei dati personali non sia tra loro chiaramente definita .

Infine, è necessario ricordare che, secondo il legislatore europeo, non sarebbero in contraddizione con le clausole contrattuali tipo le restrizioni necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato, della protezione della persona cui si riferiscono i dati o dei diritti o delle libertà altrui. Quest'ultima circostanza, quindi, potenzialmente è in grado da sola di aprire il rompere di pandora dell'intera disciplina, dal momento che attraverso l'utilizzo di clausole standard ammette la possibilità di una compressione dei diritti di libertà di difficile controllo.

L'adozione di clausole contrattuali tipo non è, tuttavia, l'unico strumento tramite il quale operare legittimamente un trasferimento di dati verso Paesi terzi: infatti, sebbene possano essere impiegate esclusivamente nell'ambito di trasferimenti di dati infra-gruppo, sempre più frequente è il ricorso alle c.d. *binding corporate rules*, previste dallo stesso art. 47 del Regolamento, che si concretizzano in un documento contenente una serie di clausole che fissano i principi vincolanti per tutte le società appartenenti allo stesso gruppo.

5. Le norme vincolanti d'impresa

Le norme o regole vincolanti d'impresa permettono il trasferimento di dati tra tutte le società partecipanti al medesimo gruppo multinazionale,

garantendo in principio un'adeguata protezione dei dati oggetto dei trasferimenti transfrontalieri.

Tale strumento non può essere considerato come l'unico od il migliore per il trasferimento di dati personali tra le società partecipanti al gruppo, ma come uno strumento in aggiunta a quelli già esistenti. A tale scopo, la normativa europea richiede l'indicazione della struttura del gruppo societario, dei trattamenti e dei trasferimenti dei dati, con precisazione delle finalità dei trattamenti che verranno effettuati fuori dall'Unione ed identificazione dei Paesi terzi in cui i dati saranno trattati, nonché un'approvazione da parte dell'autorità di controllo nazionale competente[40], che deve verificare la sussistenza dei requisiti minimi previsti dalla lunga lista contenuta nell'art. 46 del regolamento.

L'autorità presso la quale occorre presentare la richiesta è quella dove ha sede la società madre o quella della sede societaria dove avviene in via principale il trattamento dei dati: la società scelta evidentemente deve comunque avere sede nel territorio dell'Unione. In tal modo, si finisce tuttavia per frammentare le competenze autorizzative nel territorio europeo. Probabilmente, anche per coerenza di sistema, il potere di autorizzare le corporate binding rules sarebbe dovuto essere accentrato nelle mani della Commissione, lasciando alle autorità nazionali i poteri di vigilanza e protezione dei diritti delle persone.

Anche in tema di responsabilità, in caso di eventuali violazioni commesse in Paesi terzi il regime presenta delle fragilità, dal momento che quest'ultima incombe sulla società prescelta, salvo che il gruppo societario abbia proposto al Garante nazionale un criterio di ripartizione delle responsabilità di tipo diverso. In altri termini, può accadere che il titolare del trattamento stabilito nell'Unione possa essere esonerato anche completamente da tale responsabilità, a condizione che dimostri che l'evento dannoso non è a lui imputabile[41]. Tale possibilità – in evidente contrasto con gli obiettivi della normativa europea in materia –

[40] V. artt. 63 e ss.
[41] V. art. 47, par. 2, lett. f).

finisce per minare le stesse fondamenta dello strumento in esame, sottraendo di fatto un soggetto economico alla sua stessa applicazione.

L'accordo tra società madre e quelle satelliti è, inoltre, alla base dello creazione stessa delle norme vincolanti d'impresa, che devono essere concertate secondo il meccanismo di cui agli art. 57 e ss. del regolamento in esame. Tale circostanza ha il merito di estendere le norme in oggetto a tutte le società appartenenti al gruppo, ma il meccanismo di concertazione ad un esame più attento appare piuttosto laborioso e poco praticabile dal punto di vista dei costi e benefici. In caso di trasferimento a società terze infatti si dovrà in ogni caso fare ricorso alle clausole contrattuali standard analizzate precedentemente.

Infine, quanto alla eventuale modifica delle norme vincolanti d'impresa, sembra che la modificazione delle possa essere soggetta a mera comunicazione all'autorità di controllo, senza necessità di preventiva autorizzazione[42], circostanza questa che non consentirebbe di prevedere ex ante le regole che dovranno sovrintendere al trattamento dei dati[43].

Alla luce di tali rilevi, relativi sia alle clausole standard che alle norme vincolanti d'impresa, si deve concludere che sebbene tali istituti rappresentino di fatto delle alternative al giudizio di adeguatezza della Commissione, questi senza dubbio non sono in grado di rappresentare strumenti un pari grado di tutela dei diritti umani. Se già i giudizi di adeguatezza presentano profili critici sul piano della loro efficacia, è chiaro che strumenti di questo tipo sottolineano la natura formalistica della legislazione europea in materia di protezione dei dati personali, senza peraltro essere in grado di garantire una tutela effettiva e concreta dei diritti dei soggetti interessati.

[42] Cfr. art. 47 par. 2 lett. k).
[43] Di diversa opinione, G.M. RICCIO, cit., p. 878.

6. Cenni sulla direttiva PNR e gli accordi internazionali tra UE e Stati terzi

Le decisioni sull'adeguatezza della Commissione del livello di protezione dei dati di un Paese estero, possono anche riguardare uno specifico settore normativo e, di conseguenza, ammettere trasferimenti basati su singole tipologie di dati. Ciò consente ad operatori che vogliano trasferire specifici dati in caso di mancanza di decisione di adeguatezza di poter basare tale trasferimento su accordi *ad hoc*. Ciò avviene ad esempio attraverso accordi internazionali bilaterali stipulati tra UE e Paesi terzi quale l'accordo *Passenger Name Records* (PNR) .

Per PNR, in sostanza, si intendono i dati identificativi che i passeggeri forniscono ai vettori aerei, che questi ultimi utilizzano per scopi e finalità di tipo commerciale[44]. In particolare, tutti i dati che contengono una serie di informazioni che attengono al singolo passeggero – fra cui il nome, l'indirizzo dell'abitazione e quello di posta elettronica, i recapiti telefonici, le modalità di pagamento, la data di prenotazione, il numero del posto, l'informazione sulle precedenti assenze all'imbarco, ecc. [45] – sono utilizzati sin dagli anni Cinquanta dagli Stati o dalle autorità a ciò preposte come strumento di lotta al terrorismo e alla criminalità organizzata e, dunque, per finalità connesse alla sicurezza e alla salvaguardia degli interessi nazionali.

La prassi degli Stati di adottare strumenti unilaterali in tale materia, ha poi trovato ulteriore sostegno dopo l'attacco terroristico dell'11 Settembre 2001 in territorio statunitense, che ha richiesto una più stringente sicurezza dei voli aerei[46]. A livello internazionale, invece,

---

[44] F. ROSSI DAL POZZO, *EU Legal Framework for Safeguarding Air Passenger Rights*, Cham-Heidelberg-New York- Dordecht-London, 2015, p. 99 ss.

[45] L'elencazione tassativa delle informazioni che vengono veicolate con i codici di prenotazione raccolti dai vettori aerei è contenuta nell'allegato della direttiva 2016/681/UE, in esame.

[46] In particolare, gli Stati Uniti imposero restrizioni a tutti i voli in arrivo e partenza, richiedendo che i PNR (Passenger Name Records) raccolti dalle

solo in un secondo momento gli Stati hanno iniziato a stipulare accordi internazionali in materia, soprattutto sotto la spinta dell'Organizzazione internazionale dell'aviazione civile (ICAO)[47].

Ad oggi, l'Unione europea ha concluso accordi in materia con tre Stati terzi: gli Stati Uniti[48], l'Australia[49], il Canada,[50] e nel 2015 sono

---

compagnie aeree fossero resi disponibili al Dipartimento di sicurezza ed in particolare all'ufficio protezione e controllo dei confini e delle dogane. Ciò ovviamente ha riguardato anche tutti voli provenienti dall'Unione Europea, con evidenti conseguenze sulla protezione dei dati personali dei passeggeri comunitari.

[47] Si veda sul punto F. ROSSI DAL POZZO, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione" (PNR)*, in Rivista di diritto internazionale privato e processuale, vol. 4, 2016, p. 1020 ss, il quale a p. 1022 osserva che problematica della raccolta dei dati PNR da parte degli Stati è stata affrontata per la prima volta (con grave ritardo viene da aggiungere), in ambito internazionale, durante la dodicesima sessione del Facilitation Division dell'Organizzazione internazionale dell'aviazione civile (ICAO), tenutasi al Cairo tra il 22 marzo e il 1° aprile 2004, con l'adozione della raccomandazione B/5 nella quale si invitava la stessa ICAO a sviluppare linee guida rivolte agli Stati che avessero deciso di utilizzare i dati PNR come strumento ulteriore di identificazione dei dati API (Advance Passenger Information).

[48] Un primo accordo è stato concluso il 17 maggio 2004 con la decisione 2004/496/CE (in GU L 183 del 20 maggio 2004, p. 83), in seguito annullata dalla Corte di giustizia (con sentenza del 30 maggio 2006, Parlamento c. Consiglio e Commissione, cause riunite C-317/04 e C-318/04), perchè fondata non su di una corretta base giuridica. La conclusione di un nuovo accordo è avvenuta con la decisione 2006/729/PESC/GAI del Consiglio 16 ottobre 2006 (in GU L 298 del 27 ottobre 2006, p. 27). L'accordo cosìì concluso è rimasto in vigore fino al luglio del 2007 per poi essere sostituito, il 23 luglio 2007, da un nuovo accordo, concluso con la decisione 2007/551/ PESC/GAI del Consiglio (in GU L 204 del 4 agosto 2007, p. 16. L'accordo è allegato alla decisione). Il 5 maggio 2010, il Parlamento europeo, adottando una risoluzione ad hoc, ha sollecitato la rivisitazione dei termini dell'accordo (risoluzione del Parlamento europeo del 5 maggio 2010 sull'avvio dei negoziati per la conclusione di accordi sui dati del codice di prenotazione (PNR) con gli Stati Uniti, l'Australia e il Canada, ibidem, n. C 81E del 15 marzo 2011, p. 70), autorizzando poi, il 2 dicembre dello stesso anno, la Commissione ad intraprendere le iniziative necessarie per una sua rinegoziazione con gli Stati Uniti. Con decisione 2012/471/UE (in GU L 215 del 11 agosto 2012, p. 1) del Consiglio, il 13 dicembre 2011 è stata autorizzata la firma da parte dell'Unione europea del suddetto accordo. La conclusione dell'accordo a seguito dell'approvazione da parte del Parlamento europeo si è avuta il 26 aprile 2012 con la decisione 2012/472/UE del Consiglio (ibidem, n. L 215 del 11 agosto 2012, p. 4). Il nuovo accordo UE-

stati avviati i negoziati per la conclusione di un accordo con il Messico. Infine, alcuni Stati terzi – Arabia Saudita, Brasile, Federazione russa, Emirati Arabi Uniti, Giappone, Messico e Sud Corea – hanno iniziato a chiedere all'Unione europea di trasferire i dati PNR, anche in mancanza di accordi internazionali in materia.

Stati Uniti, entrato in vigore il 1° luglio 2012, a differenza dei precedenti, contiene numerose disposizioni in tema di tutela della privacy dei passeggeri.

[49] Cfr. l'Accordo tra l'Unione Europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione [Passenger Name Record — PNR] originari dell'Unione Europea da parte dei vettori aerei all'amministrazione doganale australiana, in GU L 213 dell'8 agosto 2008, p. 49, preceduto dalla decisione 2008/651/PESC/GAI del Consiglio del 30 giugno 2008 relativa alla firma, a nome dell'Unione Europea, di un accordo tra l'Unione Europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) originari dell'Unione Europea da parte dei vettori aerei all'amministrazione doganale australiana, ivi, p. 47. l'Accordo è stato oggetto di rinegoziazione a causa della posizione ostile del Parlamento europeo. Si veda, dunque, il nuovo accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record — PNR) da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera, in GU L 186 del 14 luglio 2012, p. 4, la cui firma è stata autorizzata dalla decisione 2012/380/UE del Consiglio, del 22 settembre 2011, relativa alla firma, a nome dell'Unione, dell'accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record — PNR) da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera, in GU L 186 del 14 luglio 2012, p. 2.

[50] Cfr. l'Accordo tra la Comunità europea e il governo del Canada sul trattamento delle informazioni anticipate sui passeggeri e dei dati delle pratiche passeggeri, in GU L 82 del 21 marzo 2006, p. 15, la cui firma è stata autorizzata dalla decisione 2006/ 230/CE del Consiglio del 18 luglio 2005, relativa alla conclusione di un accordo tra la Comunità europea e il governo del Canada sul trattamento dei dati API/PNR, ivi. Con lo scadere del termine fissato da tale decisione, il 22 settembre 2009 la base giuridica per la trasmissione dei dati PNR alla Agenzia canadese per i servizi transfrontalieri (CBSA) è venuta meno, anche se quest'ultima ha unilateralmente provveduto a garantire all'UE che gli impegni rimarranno validi sino a che non troverà applicazione il nuovo accordo firmato il 25 giugno 2014. Si veda sul punto la decisione 2006/253/CE della Commissione del 6 settembre 2005, che constata il livello di protezione adeguato dei dati personali contenuti nei PNR (Passenger Name Record) dei passeggeri aerei trasferiti all'Agenzia dei servizi di frontiera del Canada (Canada Border Services Agency – CBSA), in GUL 91 del 29 marzo 2006, p. 49 e i pareri del Gruppo di lavoro Articolo 29, nn. 1/2005 del 19 gennaio 2005 (WP 103), dell'11 febbraio 2004 (WP 88).

Degli accordi menzionati, di stretta attualità è tra Unione europea e Canada, che è stato recentemente oggetto di una parere della Corte di giustizia secondo la quale l'accordo non può essere concluso nella sua forma attuale a causa dell'incompatibilità di varie sue disposizioni con i diritti fondamentali riconosciuti dall'Unione[51].

Il parere era stato richiesto dal Parlamento europeo, dopo che il Consiglio UE aveva inviato a quest'ultimo per la sua approvazione e si tratta della prima pronuncia della Corte sulla compatibilità di un progetto di accordo internazionale con la Carta dei diritti fondamentali dell'UE.

L'accordo con il Canada avrebbe consentito il trasferimento sistematico e continuo dei dati PNR di tutti i passeggeri aerei a un'autorità canadese ai fini del loro uso e della loro conservazione, nonché del loro eventuale trasferimento ad altre autorità e ad altri Paesi terzi, allo scopo di lottare contro il terrorismo e i reati gravi di natura transnazionale.

Tuttavia, Corte ha affermato che l'uso dei dati e il loro eventuale trasferimento ulteriore ad autorità pubbliche canadesi, europee o estere comportano un'ingerenza nel diritto fondamentale al rispetto della vita privata, e l'accordo comporta un'ingerenza nel diritto fondamentale alla protezione dei dati di carattere personale. Anche se, come si è visto precedentemente tali deroghe al divieto di trasferimento sono giustificate dal perseguimento di una finalità d'interesse generale, secondo la Corte varie disposizioni dell'accordo non sono limitate allo stretto necessario e non prevedono norme chiare e precise.

In altri termini, il trasferimento dei dati sensibili verso il Canada richiederebbe una giustificazione precisa e particolarmente solida, vertente su motivi diversi dalla protezione della sicurezza pubblica contro il terrorismo e i reati gravi di natura transnazionale, ma nella fattispecie,

[51] Cfr. Parere 1/15 della Corte (Grande Sezione) del 26 luglio 2017 secondo il quale l'accordo tra il Canada e l'Unione europea sul trasferimento e sul trattamento dei dati del codice di prenotazione (Passenger Name Record – PNR) è incompatibile con gli articoli 7, 8 e 21 nonché con l'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, in quanto non esclude il trasferimento dei dati sensibili dall'Unione europea al Canada nonché l'uso e la conservazione di tali dati.

una siffatta giustificazione manca, e quindi la Corte ne trae la conclusione che le disposizioni dell'accordo sul trasferimento dei dati sensibili verso il Canada nonché sul trattamento e sulla conservazione degli stessi sono incompatibili con i diritti fondamentali. La sentenza in esame non potrà che avere ripercussioni sulla normativa europea, anche se non è possibile al momento stabilire quanto dirompenti.

Il pacchetto di norme europee sui dati personali si completa infatti con la recente Direttiva n. 681 del 2016. Si tratta di uno strumento, complementare rispetto agli strumenti in materia di trasferimento e agli accordi PNR precedentemente analizzati, che ha ad oggetto essenzialmente il trattamento dei dati personali dei passeggeri di vettori aerei (anche detta per questo Direttiva PNR).

Come si è visto, gli accordi internazionali PNR precedono da un punto di vista cronologico tale strumento. Il ritardo con il quale si è giunti alla Direttiva PNR è probabilmente imputabile alle criticità che presenta la questione in ambito europeo, dove – come ormai appare chiaro dalla giurisprudenza della Corte europea – qualsiasi limitazione dei diritti e delle libertà fondamentali, anche in tema di terrorismo e criminalità organizzata, deve apparire necessaria affinché sia possibile trovare un giusto equilibrio tra l'esigenza di tutelare la sicurezza pubblica e quella di limitare il diritto alla privacy. In altri termini, il trasferimento e il successivo trattamento dei dati PNR da parte di autorità pubbliche costituisce, innegabilmente, un'invasione nella sfera privata del singolo e, come tale, deve essere giustificata e proporzionata: il rispetto dei principi proporzionalità e necessità costituisce dunque la base di qualsiasi normativa che incida sui diritti fondamentali dell'individuo.

Senza entrare nell'analisi approfondita della disciplina prevista dalla direttiva 2016/681/UE, che non è oggetto precipuo di questo lavoro, è comunque innegabile che essa costituisca il tentativo migliore di un difficile bilanciamento tra garanzie di sicurezza, protezione della vita e dell'incolumità delle persona e la realizzazione di un quadro normativo che tuteli i diritti fondamentali della persona relativi alla riservatezza. Tuttavia,

nonostante i progressi fatti in materia di controllo e tutela dei diritti che possono (facilmente) essere violati in materia di dati PNR, permangono alcune criticità strutturali[52]. Infatti, nulla è cambiato rispetto alla mole di dati che possono essere acquisiti ai sensi della direttiva. Ciò indubbiamente resta, come osservato, un'interferenza piuttosto seria, a largo spettro e soprattutto tale da ingenerare negli individui interessati la sensazione che le proprie vite private siano oggetto di sorveglianza costante[53].

7. Osservazioni conclusive

Lo sforzo del legislatore europeo in materia di trasferimento dei dati personali verso Stati terzi è apprezzabile, ma anche inadeguato. Se un certo avanzamento sostanziale della disciplina in materia è innegabile, dal momento che si tratta di un pacchetto di norme abbastanza coerente e coordinato, resta in ogni caso un sostanziale esercizio di equilibrismo giuridico. Da un lato, si è cercato di salvaguardare l'esigenza di non contrastare la circolazione delle informazioni, mentre, dall'altro, si è tentato di introdurre maggiori tutele per il singolo, nuovi strumenti di controllo, repressione e di prevenzione degli atti di interferenza illecita.

In tale prospettiva, dunque, è necessario leggere la nuova disciplina in tema di protezione dei dati personali, da una parte, e della direttiva PNR. Si tratta evidentemente di strumenti complementari: prova ne è che il Parlamento europeo non abbia messo in agenda il voto sulla direttiva PNR finché non vi è stato un voto favorevole anche sulla proposta per l'adozione del nuovo regolamento generale sul trattamento e la circolazione dei dati personali nell'Unione.

[52] Sul punto si veda, F. DE BENEDETTI, *Privacy, il Garante Ue: Il pnr misura invasiva e inefficace*, disponibile su www.repubblica.it del 14.4.2016.
[53] Cfr. Corte di giustizia, sentenza dell'8 aprile 2014, *Digital Rights Ireland e Seilinger e altri*, cause riunite C-293/12 e C-594/12.

Tuttavia, come si è visto nei paragrafi che precedono, l'impegno profuso non appare ancora adeguato a offrire un corretto equilibrio delle due esigenze da bilanciare.

Si è visto come il "pacchetto dati", soprattutto attraverso le deroghe al divieto di trasferimento verso Paesi extra-europei, offra in verità numerosi spunti per la violazione di quei diritti riconosciuti agli individui agli artt. 7, 8 e 52 della Carta dei diritti fondamentali, all'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nonché all'art. 16 TFUE ,che riconosce espressamente ad ogni persona il diritto alla protezione dei dati di carattere personale che la riguardano.

A stessa o ben più triste sorte sembrano essere destinati gli accordi PNR e, oggi, la stessa direttiva PNR dove l'invasione nella sfera privata del singolo è certa. Ingerenza questa che sembra in ogni caso eccedente lo stretto necessario a causa della natura indifferenziata e generalizzata della conservazione dei dati di chiunque utilizzi servizi di comunicazione elettronica nell'Unione europea, indipendentemente dall'obiettivo di lotta contro i reati gravi, che non mancherà senz'altro di destare l'attenzione della Corte in un prossimo futuro.

Cristina Grieco[1]
Università degli Studi di Macerata e Università di Colonia

L'attuazione in Italia del diritto all'oblio

Abstract: Il contributo esamina lo sviluppo del diritto all'oblio. Partendo da un'analisi dell'evoluzione giuridica, che passa necessariamente attraverso il fondamentale apporto fornito dalla Corte di giustizia nell'ambito del celebre caso *Google Spain*, si ha cura di esaminare da vicino la situazione italiana, le percentuali di incidenza del rimedio in forma specifica messo a disposizione da *Google* all'indomani della pronuncia della Corte, ma anche lo stato della normativa, la posizione della giurisprudenza nonché quella del Garante per la Privacy.

The contribution aims to address the development of the right to be forgotten, starting from an analysis of the existing legal framework, due to the fundamental judgement of the Court of Justice in Google Spain case. Following, it focuses, particularly, on the Italian case. Namely, it deals with the results which have been achieved by using the specific format being made available by Google after Court of Justice's ruiling, the present state of the Italian regulations, the position of the case-law among Italian Courts and the position of the Italian Privacy Authority.

[1] Il presente lavoro riproduce, con aggiornamenti, la relazione svolta dall'Autrice al Convegno "Il Mercato unico digitale", tenutosi il 26 ottobre 2016 presso il Dipartimento di Giurisprudenza dell'Università di Macerata – Centro di documentazione europea, nell'ambito del Progetto nazionale dei CDE italiani 2016 "Un Mercato unico digitale per l'Europa", promosso dalla Rappresentanza in Italia della Commissione europea.

diritto all'oblio – 4. L'attuazione in Italia del diritto all'oblio – 5. La Carta dei diritti Internet – 6. La posizione del Garante per la Privacy sul diritto all'oblio – 7. La posizione della giurisprudenza italiana sul diritto all'oblio – 8. Conclusioni

1. Introduzione

Quello del diritto all'oblio è un tema particolarmente attuale viste le tragiche vicende che, con frequenza sempre più allarmante, sono balzate agli onori della cronaca negli ultimi tempi. Quanto accaduto offre uno spaccato di quella che è la realtà sociale nell'era di *Internet* e dei *social network,* dove, sempre più di frequente, si assiste ad episodi di sovraesposizione della vita del singolo individuo[2].

Nella società dell'informazione, in cui si parla addirittura di "supremazia della Rete", la riservatezza e la vita privata necessariamente vanno ad assumere una dimensione diversa, molto più ampia. Il *focus* si è spostato sulla necessità di stabilire opportuni confini e predisporre i dovuti rimedi ma, soprattutto, sul diritto al controllo dei dati che circolano in rete e che riguardano il singolo individuo. Ciò in quanto, le informazioni private circolano, quotidianamente, connesse a molteplici attività e a diversi livelli (utilizzo di *social network*, corrispondenza elettronica, *e-shopping,* pagamenti con carte di credito e di debito, accessi in *Internet*, telefonate) che lasciano una traccia "elettronica" indelebile nelle banche dati dei *provider* che gestiscono i servizi. Attraverso tali dati è possibile ricostruire preferenze, relazioni, rapporti, gusti, spostamenti ma anche avere accesso a dati sensibili quali orientamento sessuale e credenze religiose.

[2] Cfr. C. Matranga, *Luci ed ombre del caso Google Spain, Una vittoria del diritto all'oblio*, in *Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, Vol. XII, 2014, pp. 93 ss. Inoltre in prospettiva comparatistica anche O. Pollicino, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?,* 2013, pdf disponibile al seguente indirizzo http://www.forumcostituzionale.it/wordpress/images/stories/pdf/documenti_forum/paper/0454_pollicino.pdf.

È innegabile che le tecnologie informatiche offrano numerosi vantaggi in ambito economico (costituiscono spesso veicoli di informazione e marketing molto efficaci a costi decisamente ridotti) ma moltiplicano anche esponenzialmente la diffusione di dati e, dunque, di possibile danno ai soggetti coinvolti. Tale sovraesposizione, nel tempo, rischia di tradursi, inevitabilmente, in una potenziale violazione della dignità umana, di diritti e delle libertà fondamentali. È stato addirittura evidenziato che l'emergere di nuovi diritti, che ridefiniscono l'integrità stessa della persona e che ne legittimano la tutela, comporterebbe una rivisitazione della distinzione tra *habeas corpus* e *habeas data*. L'antico *habeas corpus*, legato alla libertà personale intesa come libertà fisica, oggi deve considerarsi anche un *habeas data*[3].

È proprio in questa dimensione della realtà, che non può dirsi poi così distante da quella che Orwell ha descritto nel suo celebre 1984, alla presenza di strumenti tanto pervasivi, che nasce la necessità di intervenire per limitare gli effetti indesiderati. In questo modo, come sosteneva Betti, il diritto tipizzando una determinata fattispecie ed effettuando una selezione degli interessi da proteggere e dei valori da tutelare, riesce a dominare e strutturare la realtà "estranea al diritto" collegando determinati effetti giuridici ad aspetti rilevanti tratti dalla realtà sociale[4].

È in questo quadro che si deve inserire quello che oggi è noto come diritto all'oblio, che letteralmente e in modo semplicistico si traduce con "il diritto ad essere dimenticati"[5].

---

[3] Cfr. G. Preite, *Welfare State. Storie, Politiche, Istituzioni*, Trento, 2011, p. 175; e anche i contributi di S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 2004, *passim*; Id., *Tecnologie e diritti*, Bologna, Il Mulino, 1995, *passim.*

[4] Cfr. E. Betti, *Interpretazione della legge e degli atti giuridici. Teoria generale e dogmatica*, Milano, 1971, pp. 40 ss.

[5] Cfr. G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica,* 2014, pp. 592 e ss. Secondo l'A., con l'espressione "diritto all'oblio" si fa riferimento ad almeno tre differenti accezioni: quella tradizionale, più risalente nel tempo, elaborata dalla dottrina civilistica e dalla giurisprudenza, in epoca antecedente all'avvento della Rete; quella rela-

Nello studio che *"We are Social"* pubblica annualmente, sono stati analizzati il volume di utilizzo della rete, le modalità di accesso e l'uso dei singoli *social network* per ciascuna area geografica. Nell'ultima ricerca relativa al 2017, pubblicata il 24 gennaio, è emerso un *trend* in costante crescita nell'utilizzo della rete, specialmente da dispositivi mobili, il che suggerisce che, in pratica, si tende a rimanere costantemente connessi. Inoltre, seppure con volumi diversi per ciascuna aerea geografica di riferimento, su una popolazione di oltre sette miliardi di persone, più della metà utilizza costantemente la rete e, sebbene con preferenze diverse che variano soprattutto in base all'età anagrafica, oltre due miliardi e settecento milioni sono fruitori regolari di piattaforme *social*[6].

2. La consacrazione del diritto all'oblio nella sentenza della Corte di giustizia nel caso *Google Spain*

La definitiva affermazione del diritto all'oblio si è avuta con la nota sentenza della Corte di Giustizia dell'Unione europea resa nel caso *Google Spain*[7]. In tale pronuncia la Corte ha affermato la prevalenza dell'interesse

tivo al l'utilizzo di Internet e delle reti telematiche, per le modalità proprie di diffusione dell'informazione; quella che si riferisce al diritto alla cancellazione, al blocco, al congelamento dei dati o all'opposizione al trattamento dei dati previsti dalla 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".

[6] La ricerca è disponibile al seguente link: http://wearesocial.com/blog/2017/01/digital-in-2017-global-overview.

[7] CGUE, Grande Sezione, C-131/2012, del 14 febbraio 2014, «Dati personali – Tutela delle persone fisiche con riguardo al trattamento di tali dati – Direttiva 95/46/CE – Articoli 2, 4, 12 e 14 – Ambito di applicazione materiale e territoriale – Motori di ricerca su Internet – Trattamento dei dati contenuti in siti web – Ricerca, indicizzazione e memorizzazione di tali dati – Responsabilità del gestore del motore di ricerca – Stabilimento nel territorio di uno Stato membro – Portata degli obblighi di tale gestore e dei diritti della persona interessata – Carta dei diritti fon-

alla riservatezza dei soggetti privati a fronte dell'attività economica esercitata dal motore di ricerca che, con una certa sorpresa, è stata qualificata come «trattamento dei dati personali».

Il caso riguardava un avvocato spagnolo il quale aveva convenuto in giudizio una famosa testata giornalistica dinanzi all'Audiencia Nacional lamentando l'illiceità del mantenimento di una notizia, riguardante una procedura esecutiva immobiliare subita anni prima, che, a suo dire, risultava pregiudizievole per la propria reputazione. Il professionista, però, non si è limitato a chiamare in giudizio la testata giornalistica ma ha citato anche il motore di ricerca *Google* responsabile, a suo dire, di aver mantenuto attivo l'accesso a tali notizie. Il giudice spagnolo, vista la novità della materia, ha rimesso la questione alla Corte di giustizia con rinvio pregiudiziale. In particolare, il tribunale ha chiesto alla Corte se fosse o meno possibile qualificare l'attività del motore di ricerca quale "trattamento dei dati personali", con conseguente possibilità di configurare una responsabilità in capo al *search engine*; e se fosse o meno possibile riconoscere l'esistenza in capo al soggetto privato del diritto di rivolgersi direttamente al motore di ricerca, al fine di ottenere la rimozione del contenuto indesiderato, in forza dell'esistenza di un c.d. diritto all'oblio, annoverabile tra i diritti della personalità protetti dagli articoli 7 e 8 della Carta di Nizza.

La Corte, pronunciandosi sulla questione, ha ritenuto non ravvisabile alcuna responsabilità in capo alla testata giornalistica, in quanto la pubblicazione della notizia, nell'immediato, doveva considerarsi del tutto legittima. Al contrario, inaspettatamente, la Corte ha ritenuto responsabile il motore di ricerca *Google*. In particolare, la Corte ha stabilito che *Google Spain* debba annoverarsi all'interno della categoria dei c.d. *Internet Service Provider* (ISP - disciplinati dalla direttiva 2000/31/CE – recepita in Italia con il D.Lgs. 70/2003) e che la sua attività debba considerarsi come "trattamento dei dati personali".

---

damentali dell'Unione europea – Articoli 7 e 8».

La Corte, in questo modo, ha spostato il carico della responsabilità dal soggetto che materialmente effettua la pubblicazione della notizia a quello che, al contrario, si occupa unicamente di rendere disponibili i dati e le informazioni attraverso una procedura di indicizzazione.

Ne consegue che, nell'annosa battaglia che vede contrapposti il diritto di cronaca e il diritto alla privacy[8], la Corte, ha dimostrato di ritenere prevalente il secondo e ciò necessariamente a discapito dell'interesse economico connesso all'attività del motore di ricerca, gravato di un compito di controllo che, di fatto, almeno a priori, non sembrerebbe competergli.

Sul punto, sonoro appare il richiamo all'articolo 2, lettera b, della direttiva 95/46, all'interno del quale vengono ricomprese tutte le operazioni compiute dal motore di ricerca. Secondo la Corte, infatti, non può prescindersi dall'applicazione della normativa in questione anche all'indicizzazione dei dati, alla loro raccolta, memorizzazione temporanea e a tutte le procedure simili che costituiscono il fulcro del servizio di ricerca *online*. Così argomentando la Corte, in definitiva, stabilisce l'attrazione di tali operazioni nell'orbita del trattamento dei dati personali chiarendo che «il trattamento dei dati effettuato nel contesto dell'attività di un motore di ricerca si distingue da e si aggiunge a quel-

[8] In Italia la questione ha trovato una risposta nella celeberrima sentenza della Cass., Sez. I, 18 ottobre 1984, n. 5259, in *Foro it*., 1984, CVII, c. 2712 ss., nonché in *Dir. inf*., 1985, pp. 143 ss. dove si legge «Come ormai la giurisprudenza di questa Corte ha più volte avuto occasione di precisare, sia in sede civile che penale – il diritto di stampa (cioè la libertà di diffondere attraverso la stampa notizie e commenti) sancito in linea di principio nell'art. 21 Cost. e regolato fondamentalmente nella L. 8 febbraio 1948 n. 47, è legittimo quando concorrano le seguenti tre condizioni: 1. utilità sociale dell'informazione; 2. verità (oggettiva o anche soltanto putativa purché, in quest'ultimo caso, frutto di un serio e diligente lavoro di ricerca) dei fatti esposti; 3. forma "civile" della esposizione dei fatti e della loro valutazione: cioè non eccedente rispetto allo scopo informativo da conseguire, improntata a serena obiettività almeno nel senso di escludere il preconcetto intento denigratorio e, comunque, in ogni caso rispettosa di quel minimo di dignità cui ha sempre diritto anche la più riprovevole delle persone, sì da non essere mai consentita l'offesa triviale o irridente i più umani sentimenti».

lo effettuato dagli editori di siti web e incide ulteriormente sui diritti fondamentali della persona interessata»[9].

Nondimeno, non può sottacersi che tale assimilazione susciti delle perplessità, visto e considerato che il motore di ricerca non tratta direttamente i dati inseriti. Il fulcro dell'attività in questione, infatti, è la ricerca di tutti i contenuti presenti sul web che si ricollegano a delle parole chiave scelte ed inserite direttamente dagli utenti, sulla base di un linguaggio specifico (SEO), all'interno dei quali confluiscono anche i dati di titolarità di soggetti privati. In questo caso, quindi, la Corte qualifica come "trattamento dei dati" un'attività che, in prima battuta, opera attraverso degli automatismi, in base a criteri di attinenza e popolarità (sarebbe impossibile, infatti, ipotizzare a priori uno *screening* sui miliardi di dati inseriti ogni giorno)[10]. In sostanza, dunque, la Corte addossa in capo al motore di ricerca, che non effettua alcuna operazione di filtraggio delle notizie, tantomeno basata su valutazioni di tipo meritorio, una responsabilità che agevolmente potrebbe essere definita oggettiva e che, addirittura, prescinde dalla liceità stessa della prima pubblicazione della notizia effettuata dall'editore[11].

Ora, se da una parte appare legittimo imporre al motore di ricerca di operare in condizioni di legalità, evitando la diffusione di contenuti notoriamente e palesemente illeciti quando manifestamente verificabili, dall'altra risulta piuttosto complesso pretendere che il motore di ricerca (e a questo punto bisognerebbe interrogarsi anche sul come) possa veri-

[9] CGUE, C-131/2012, cit., punto 83.

[10] Cfr. R. Pardolesi, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, Milano, 2003, pp. 48 ss.; anche A. Spagnolo, *Bilanciamento tra libertà d'espressione su Internet e tutela del diritto d'autore nella giurisprudenza recente della Corte europea dei diritti umani*, in www.federalismi.it, 17 maggio 2013, p. 9. Si v. anche S. Calzolaio, *Gli ISP si salvano nel P2P. Ma reggeranno allo streaming?,* in www.forumcostituzionale.it., 14 febbraio 2012.

[11] Cfr. C. Matranga, *Luci ed ombre del caso Google Spain, Una vittoria del diritto all'oblio*, cit., pp. 93 ss.

ficare, a priori, quali indirizzi siano lesivi dei diritti dei singoli e quali no, qualora non sia intervenuta alcuna comminatoria a riguardo.

Ciò posto, appare assai complesso giustificare l'assimilazione di posizioni tanto diverse tra loro, ovvero quella di chi tratta quei dati personali come scopo principale della propria attività (come può essere l'attività della testata giornalistica che riporta la notizia) e quella di chi (motore di ricerca), al contrario, si limita a rendere disponibili gli stessi dati, già esistenti in quanto precedentemente trattati da altri soggetti[12]. Peraltro, occorre altresì sottolineare che la normativa sul commercio elettronico esclude espressamente che possa rinvenirsi in capo al *provider* un obbligo generale di sorveglianza sulle informazioni che si ritrovi a trattare[13].

---

[12] Cfr. C. Matranga, *Luci ed ombre del caso Google Spain, Una vittoria del diritto all'oblio*, cit., p. 97 e anche F. Macario, *La protezione dei dati personali nel diritto privato europeo*, in *La disciplina del trattamento dei dati personali*, a cura di V. Cuffaro-V. Ricciuto, Torino, 1997, p. 53 s.

[13] Con il D.Lgs. n. 70 del 9 aprile 2003, l'ordinamento italiano ha recepito la direttiva europea n. 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico. Il legislatore italiano, nel delineare la responsabilità del *provider*, ha distinto tre figure di prestatore:
- prestatori di semplice trasporto, la cui attività consiste nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione (*mere conduit*);
- prestatori di servizi di memorizzazione automatica, intermedia e temporanea delle informazioni, effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta (*caching*);
- prestatori di servizi di memorizzazione di informazioni fornite da un destinatario del servizio (*hosting*).
La responsabilità dell'intermediario viene definita negli artt. 14, 15 e 16 del D.Lgs. n. 70 del 2003 in negativo, in quanto, se sussistono le condizioni di cui al decreto, l'intermediario non è responsabile degli illeciti commessi dagli utenti utilizzando i suoi servizi. L'art. 17 del D.Lgs. n. 70 del 2003 sancisce per i destinatari nella prestazione dei servizi della società dell'informazione sopradescritti l'assenza di un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, e su questo presupposto si prevede un generale esonero da responsabilità per l'illiceità delle informazioni, con determinate deroghe, che attengono principalmente all'art. 14 allo svolgimento di un ruolo attivo nella trasmissione delle informazioni, all'art.

Alla luce di tutto quanto sopra, posto che risulta irrealizzabile porre a carico del motore di ricerca un generale e aprioristico dovere di controllo sui dati inseriti, è evidente che un'eventuale responsabilità, nei fatti, sarà attivabile solo *ex post,* con la richiesta diretta al motore di ricerca di rimozione dei contenuti ritenuti pregiudizievoli, ricalcato sul sistema statunitense del *notice* and *takedown*[14].

Nondimeno, stabilita la responsabilità del *provider*, la Corte passa ad esaminare la sussistenza in capo al soggetto privato del diritto di rivolgersi direttamente al motore di ricerca, per ottenere la rimozione del contenuto indesiderato in forza di un c.d. diritto all'oblio.

Sebbene l'espressione sia piuttosto risalente – visto che il primo celebre contributo sul diritto alla *privacy* fu pubblicato nel 1890 sulla *Harvard Law Review*[15] dove gli autori Warren e Brendeis identificarono l'essenza del diritto oblio nel «*right to be let alone*» – cioè a non vedere infranta l'intangibilità della propria dimensione personale – il diritto ad essere dimenticati vive un'evoluzione parallela e direttamente proporzionale all'evolversi della morfologia del diritto alla riservatezza.

Per ciò che riguarda il diritto all'oblio due sono le principali problematiche che si pongono, la prima riguarda la configurabilità di un diritto all'oblio rispetto ad una pubblicazione avvenuta lecitamente parecchi anni prima; la seconda concerne l'attuazione dello stesso diritto direttamente a carico del motore di ricerca.

Quanto al primo profilo, la Corte ha ritenuto che «sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta», il soggetto possa chiedere che una determinata informazione non venga più messa a disposizione del grande pubblico mediante la sua inclusio-

---

15 al mancato rispetto delle informazioni medesime e all'art. 16 alla effettiva conoscenza della loro illiceità o all'esercizio di una "autorità o controllo" sul destinatario del servizio.

[14] Cfr. C. Matranga, *Luci ed ombre del caso Google Spain, Una vittoria del diritto all'oblio*, cit., p. 98.

[15] Cfr. S. Warren-L. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. IV, 1890, n. 5.

ne in un determinato elenco di risultati. La Corte evidenzia, infatti, che il diritto all'oblio e, dunque, alla riservatezza prevalgono «non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse [del] pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona». Ciò vale anche nei confronti di contenuti già disponibili da tempo e che emergono da ricerche successive. In questo caso, la Corte ha riconosciuto in capo al soggetto un diritto di opposizione a che quei dati vengano riconnessi al proprio nome, anche a prescindere dal pregiudizio che ciò possa arrecargli[16]. Le uniche eccezioni, secondo la Corte, sarebbero da rinvenire in condizioni particolari, come il ruolo ricoperto da un determinato soggetto nella vita pubblica. In tal caso l'ingerenza a scapito della propria sfera personale sarebbe giustificata dall'interesse preponderante del pubblico ad avere accesso a determinate informazioni[17].

Da tale ragionamento emerge un dato fondamentale. Il diritto all'oblio è strettamente connesso al fattore tempo. Ne consegue che tale diritto risulterà lecitamente esercitabile qualora il trascorrere di un dato lasso di tempo non giustifichi più la permanenza in rete e la conseguente diffusione di quelle stesse informazioni che, in un primo momento, erano state lecitamente rese pubbliche. Ciò che concorre, dunque, a configurare l'azionabilità del diritto all'oblio è l'assenza o il venir meno delle ragioni che un tempo avevano reso possibile la diffusione di determinate informazioni e, soprattutto, il legame tra queste ragioni ed un nuovo trattamento degli stessi tramite la rievocazione di quelle stesse vicende in un momento posteriore.

Il problema successivo che si pone, è capire come possa essere legittimamente avanzata tale pretesa da parte del soggetto interessato e, in definitiva, come possa essere concretamente esercitato il diritto all'oblio. La questione, infatti, attiene ancora una volta alla qualificazione dell'attività di indicizzazione effettuata dal motore di ricerca che,

[16] CGUE, C-131/12, cit., punto 97.
[17] CGUE, C-131/12 cit., punto 98.

secondo la Corte, deve ritenersi un'ingerenza ancora più rilevante nel diritto al rispetto della vita privata della persona interessata che non la pubblicazione da parte dell'editore della notizia sulla pagina *web*. Ciò in quanto, secondo quanto stabilisce l'articolo 6, paragrafo 1, lettere da c) a e), della direttiva 95/46, «anche un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso»[18].

L'effetto pratico che è disceso dalla sentenza della Corte di giustizia è stato di conferire al singolo uno strumento che gli consenta di ottenere una tutela in forma specifica che, agendo sulla sfera giuridica di un altro soggetto, gli consenta di ristabilire lo *status quo ante.*

In definitiva, dunque, la Corte riconosce il diritto all'oblio e la sua azionabilità in forma specifica, fornendo come legittimazione giuridica e normativa gli articoli 7 e 8 della Carta di Nizza ed effettuando una lettura orientata della direttiva 95/46/CE.

3. Il regolamento UE n. 679/2016 "*Data Protection*" e la positivizzazione del diritto all'oblio

A livello normativo, il passo definitivo verso la positivizzazione del diritto all'oblio è stato compiuto dal legislatore europeo con il regolamento UE n. 679/2016[19], entrato in vigore il 24 maggio 2016, la

[18] CGUE, C-131/2012, cit., punto 93.

[19] Regolamento UE n. 679/2016 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), pubblicato in GUUE, L 119/1, 4 mag-

cui applicazione è stata posticipata, per tutti i Paesi membri, al 25 maggio 2018**.**

La nuova normativa, che risulta molto articolata, visto che si compone di 173 considerando e 99 articoli, in linea di massima introduce regole uniformi in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Unione europea e per i casi di violazione dei dati personali (*data breach*).

All'interno del regolamento il diritto all'oblio viene esplicitamente disciplinato all'articolo 17, dove viene stabilito che l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, al verificarsi di determinate condizioni. In particolare, tale obbligo sussiste qualora i dati non risultino più necessari rispetto alle finalità per le quali sono stati inizialmente raccolti o trattati; l'interessato ritiri il consenso su cui si basa il trattamento e non sussista altro motivo legittimo per proseguire nel trattamento degli stessi; l'interessato si opponga al trattamento dei dati personali e non sussista alcun motivo legittimo prevalente per procedere con il trattamento ovvero nel caso in cui i dati siano stati trattati, *ab origine*, in maniera illecita. Inoltre, i dati dovranno devono essere cancellati anche in adempimento ad un obbligo legale previsto dal diritto dell'Unione o degli Stati

---

gio 2016. È stata altresì adottata la direttiva n. 680/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini. Pubblicata in GUUE, L. 119/89, del 4 maggio 2016. La direttiva è entrata in vigore ufficialmente il 5 maggio 2016 e a tutti gli Stati membri sono stati concessi due anni per procedere all'attuazione.

membri cui è soggetto il titolare del trattamento ovvero qualora i dati siano stati raccolti relativamente ad un'offerta di servizi.

La tutela che appresta l'articolo 17 appare particolarmente ampia. Al paragrafo 2, infatti, si stabilisce, in aggiunta, che il titolare del trattamento, se ha reso pubblici dei dati personali che ha l'obbligo di cancellare, tenendo conto della tecnologia disponibile e dei costi di attuazione, «deve prendere le misure ragionevoli, anche tecniche, per informare terzi soggetti, che a loro volta stanno trattando i medesimi dati, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali».

Chiaramente, non si tratta di un diritto assoluto e il suo esercizio può essere soggetto a limitazioni, anch'esse disciplinate dallo stesso articolo. Al paragrafo 3 sono elencate le condizioni al verificarsi delle quali il diritto all'oblio può essere compresso. È previsto, infatti, che dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere ad un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

I contorni del diritto all'oblio possono essere meglio precisati anche guardando al contenuto del preambolo del regolamento. Particolarmente interessanti appaiono, al riguardo, i considerando 65, 66 e 156.

Il considerando 65, in particolare, oltre ad evidenziare genericamente che «un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento», sottolinea, con riguardo alla possibilità di ritirare il consenso precedentemente prestato, l'opportunità

che venga prevista tale possibilità soprattutto laddove l'interessato abbia prestato il proprio consenso quando era minore e, quindi, non pienamente consapevole dei rischi derivanti dal trattamento. In base a quanto specifica il considerando, la possibilità di esercitare tale diritto dovrebbe prescindere dal fatto che l'interessato non sia più minorenne.

Per ciò che riguarda il considerando 66 questo è specificamente dedicato alle misure necessarie per rafforzare il «diritto all'oblio» in rete. Viene suggerito, in particolare, che il diritto alla cancellazione dovrebbe essere esteso in modo tale da obbligare il titolare del trattamento, che ha pubblicato i dati personali, a informare coloro che, sulla base di tale pubblicazione, stiano utilizzando i dati in questione, al fine di procedere alla cancellazione di qualsiasi *link*, copia o riproduzione degli stessi.

Da ultimo, il considerando 156 evidenzia come il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici debba essere adeguatamente contemperato con il diritto all'oblio dell'interessato. Tale contemperamento deve avvenire attraverso la previsione di opportune garanzie, che è compito degli Stati membri predisporre, cercando di assicurare il c.d. principio della minimizzazione dei dati.

4. L'attuazione in Italia del diritto all'oblio

Tratteggiato il contenuto del diritto all'oblio, anche alla luce degli ultimi interventi normativi europei in materia, occorre ora soffermarsi sulle modalità con cui tale diritto può concretamente essere esercitato, i limiti a cui è soggetto e, soprattutto, quali esiti ci si può ragionevolmente attendere con gli strumenti attuativi al momento disponibili.

In ottemperanza alla menzionata sentenza della Corte di giustizia[20],

[20] V. *supra* par. 2.

Google è stato messo nella posizione di dover prendere in considerazione le numerose istanze di rimozione di contenuti "indesiderati". In risposta a tale necessità, il motore di ricerca ha predisposto un'apposita pagina *web*[21] attraverso la quale è possibile, per ciascun soggetto interessato, richiedere la cancellazione di dati che si considerano lesivi al fine di ripristinare "una reputazione digitale integra".

Nondimeno, come si evince dalle statistiche che lo stesso motore di ricerca ha pubblicato all'interno del "Rapporto sulla trasparenza"[22], la percentuale di richieste che vengono effettivamente processate ed accolte si attesta ampiamente al di sotto del 50%. L'Italia peraltro si pone come fanalino di coda in Europa visto che la percentuale non supera il 33% (ciò implica che solo un terzo delle richieste viene evaso e il relativo contenuto viene rimosso). La percentuale risulta un po' più alta per gli altri Paesi ma, comunque, anche nel caso più virtuoso, che secondo le statistiche sarebbe quello francese, non si va oltre il 49%.

Occorre però evidenziare un altro aspetto. Oltre alla esiguità delle domande evase con esito positivo, il punto più rilevante che emerge dalle statistiche riguarda il contenuto delle richieste di cancellazione. I dati per cui si chiede la rimozione il più delle volte riguardano non tanto l'esercizio del diritto all'oblio quanto la tutela della privacy.

In altre parole, i contenuti dei quali si richiede la rimozione interessano dati la cui pubblicazione è avvenuta da parte dello stesso soggetto che ne richiede in seguito la cancellazione. Basti pensare che uno dei domini su cui vi è il maggior numero di richieste di rimozione è *Facebook*, dove notoriamente, salvo casi eccezionali di violazione dell'*account*, è lo stesso titolare del profilo a condividere i contenuti che desidera rendere pubblici.

Come evidenziato, però, e come si evince dalla giurisprudenza della

[21] Disponibile al seguente indirizzo https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636263708229058035-652807212&rd=1&pli=1.

[22] Disponibile al seguente indirizzo https://www.google.com/transparencyreport/?hl=it.

Corte di Giustizia, il caso vero del diritto all'oblio riguarda i fatti di cronaca attinenti alla vita delle persone raccontati, *rectius* pubblicati, da soggetti terzi. Prendendo a riferimento questo specifico segmento, che poi rappresenta l'essenza vera del diritto all'oblio, volendo dare una percentuale indicativa di riferimento, non essendocene al momento una ufficiale, le rimozioni si attestano ad una percentuale particolarmente esigua, che non supera il 5/8%.

Se ne deve concludere che, attualmente, la forza sottrattiva del diritto all'oblio, attraverso questi strumenti specifici di rimozione, risulta molto bassa.

Ciò posto, è evidente che oltre al rimedio in forma specifica fornito dai vari motori di ricerca – *Google* per primo ma anche gli altri *provider* si sono adeguati o, comunque, si stanno adeguando –, devono necessariamente essere previsti altri rimedi esperibili, nel caso in cui il motore di ricerca non dovesse dare seguito alla richiesta ovvero dovesse respingerla.

In Italia, in particolare, sono previsti due ulteriori rimedi: l'opposizione all'Autorità Garante per la Privacy e la tutela civile in sede giurisdizionale.

5. La Carta dei diritti Internet

Circa un anno dopo la sentenza della Corte di giustizia, in Italia è stata approvata una vera e propria Carta dei diritti e doveri della Rete[23]

[23] La Presidenza della Camera dei deputati ha promosso la costituzione di una Commissione di studio per l'elaborazione di principi in tema di diritti e doveri relativi ad Internet all'indomani della sentenza della Corte di giustizia. La Commissione, composta dai deputati attivi sui temi dell'innovazione tecnologica e dei diritti fondamentali studiosi ed esperti, ha iniziato i suoi lavori il 28 luglio 2014. Per la prima volta in Italia è stata istituita in sede parlamentare una Commissione su questi temi. L'iniziativa è nata in coincidenza con altre iniziative analoghe, assunte in questo ambito negli ultimi anni, con una recente accelerazione a livello internazio-

con l'obiettivo di focalizzare l'attenzione su un uso consapevole del *web*, al fine di garantire un adeguato bilanciamento dei diritti in gioco. La carta si focalizza soprattutto su temi quali il *copyright*, la cultura, il *digital divide* (ovvero il c.d. divario digitale tra coloro che hanno effettivo accesso alla tecnologia ICT e coloro a cui invece risulta ancora preclusa) e i diritti di coloro che utilizzano la Rete per gli scopi più disparati (lavoro, divertimento, fare impresa, "dialogare con lo Stato", esercizio dei diritti di cittadinanza).

La Carta si spinge fino al punto di definire, all'interno dell'articolo 2, l'accesso a *Internet* come un diritto fondamentale, o meglio come condizione necessaria per assicurare l'esercizio di tutti gli altri diritti previsti.

All'interno della stessa sono raccolti un insieme di principi e valori, che fanno riferimento, attingendovi in qualche modo, alla Dichiarazione Universale dei Diritti dell'Uomo, che riconosce e tutela la dimensione individuale del soggetto. La Carta è per lo più rivolta al legislatore, il quale potrà legiferare in maniera più consapevole, ma è pensata anche per i cittadini, in modo da garantirgli adeguata consapevolezza del loro "diritto di avere diritti", così come ha evidenziato Stefano Rodotà, che ha coordinato il comitato in seno al quale la Carta è stata elaborata. In base a quanto si legge all'interno dell'articolo 3, infatti, «ogni persona ha diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare *Internet* in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali».

Nondimeno, la grande risonanza attorno ai temi del diritto all'oblio ha suggerito l'opportunità di prevedere alcune innovazioni quali il "diritto all'autodeterminazione informativa" – ovvero il diritto di gestire il

---

nale. Tra queste, l'approvazione in Brasile della legge cosiddetta *"Marco civil"* nell'aprile 2014, le sentenze della Corte di giustizia dell'Unione europea dell'8 aprile *(Google-Spain)* e del 13 maggio 2014 *(Digital rights Ireland)*, la raccomandazione del Consiglio d'Europa anch'essa del 16 aprile 2014 (sulla protezione dei diritti umani su *Internet*) e la sentenza della Corte Suprema Usa del 25 giugno 2014 (sulla *privacy* relativa ai telefoni cellulari).

proprio profilo digitale e a costruire liberamente la propria identità all'interno di rapporti sociali che nella rete diventano sempre più complessi – o il diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici (articolo 7).

Il diritto all'oblio viene espressamente considerato all'interno dell'articolo 11, ed è definito come il diritto ad ottenere la cancellazione di dati e notizie personali non più attuali ai fini dell'informazione o della ricerca storica. L'articolo 12 tutela il rapporto con i *provider* del web nei confronti dei quali i fruitori della rete rappresentano sempre la controparte debole. L'articolo 13, invece, ribadisce il tema della sicurezza online e la descrive sia come tutela delle infrastrutture sia come difesa degli individui da fenomeni quali *cyberbullismo*, *stalking*, razzismo, xenofobia e *hate-speech*.

Nella Carta si arriva a parlare di un Governo di *Internet*, inteso come il «rispetto complessivo dei diritti dei cittadini in un ecosistema digitale che supera i confini statuali» e che di *Internet* ribadisce «il carattere aperto e democratico, volto a impedire ogni forma di discriminazione ed evitare che la sua disciplina dipenda dal potere esercitato da soggetti dotati di maggiore forza economica»[24].

6. La posizione del Garante per la Privacy sul diritto all'oblio

Il Garante per la privacy a più riprese è intervenuto per cercare di fornire validi elementi che contribuissero a connotare l'essenza del diritto all'oblio in accordo con quella che è la normativa italiana.

[24] Cfr. A. Di Corinto, *Carta dei Diritti in internet*, approvata alla Camera la mozione in vista dell'Internet Governance Forum, in Repubblica.it http://www.repubblica.it/tecnologia/2015/11/03/news/diritti_in_internet_approvata_alla_camera_la_mozione_in_vista_dell_igf-126558837/ e anche Id., *Internet, ecco la Carta dei diritti e doveri della rete*, in Repubblica.it, http://www.repubblica.it/tecnologia/sicurezza/2015/07/28/news/internet_ecco_la_carta_dei_diritti_e_dei_doveri_della_rete-119963206/.

Interessante appare, al riguardo, il contenuto dei chiarimenti emanati nel 2004, in risposta ad alcuni quesiti posti dall'Ordine dei giornalisti[25].

In quella occasione, il Garante ha chiarito che generalmente la pubblicazione su *Internet* di dati personali di soggetti menzionati in articoli giornalistici è da considerarsi di per sé lecita. Nondimeno, il trattamento dei dati per finalità giornalistiche – anche in assenza del consenso degli interessati (la cui raccolta peraltro contrasterebbe con gli altri diritti fondamentali di cronaca e di informazione) – deve comunque rispettare «i principi di proporzionalità e non eccedenza, di indispensabilità rispetto all'esercizio del dovere giornalistico di cronaca, di veridicità dei fatti, di reale interesse del pubblico ad essere informato su aspetti di dettaglio».

Il Garante ha però tenuto a sottolineare che le finalità informative e/o giornalistiche *vanno comunque contemperate con il diritto all'oblio degli interessati*. Per di più, con specifico riguardo al trattamento dei dati personali su reti di comunicazione elettronica, stante l'accessibilità planetaria alle informazioni *online*, il Garante ha altresì specificato che il diritto all'oblio, in tale contesto, deve intendersi come il diritto degli interessati ad evitare che l'indefinita permanenza su *Internet* di dati e informazioni risalenti nel tempo – magari incompleti e non aggiornati in quanto privi dei successivi resoconti giornalistici circa l'evoluzione della notizia originariamente riportata – determini una lesione dei diritti che il Codice della Privacy tende complessivamente a proteggere[26].

Ciò può accadere in occasione della riproposizione di una informazione personale a distanza di tempo, mediante la ripubblicazione di vecchi articoli contenenti dati personali resi disponibili *online,* la cui

[25] Cfr. Autorità Garante per la protezione dei dati personali, Privacy e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti, 6 Maggio 2004, 1007634 disponibile al seguente indirizzo http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1007634.

[26] Cfr. Art. 2 che garantisce che «il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali».

reperibilità è facilitata attraverso motori di ricerca esterni. Inoltre, la lesione del diritto all'oblio (e l'impossibilità dell'interessato di tornare nell'anonimato) è resa ancor più grave quando le informazioni riprodotte o disponibili in maniera permanente, sebbene in origine legittimamente pubblicate, risultino poi nel tempo incomplete. Un esempio è il caso di un soggetto menzionato in un articolo giornalistico in quanto indagato ma successivamente assolto senza che di questa positiva evoluzione venga data notizia.

Ciò posto, il Garante ha evidenziato che il discrimine per pubblicare o meno una notizia è l'esistenza dell'interesse pubblico. Pertanto chiunque voglia successivamente riproporre e ripubblicare (o semplicemente far permanere) su *Internet* articoli giornalistici contenenti dati personali di terzi, è tenuto a verificare, a maggior ragione quando l'intendimento è quello di dare diffusione planetaria della notizia sul *web*, che tale interesse sussista al momento della ripubblicazione. Sarà dunque necessaria una nuova valutazione, altra rispetto a quella svolta dal giornalista autore della originaria pubblicazione, che tenga in debito conto – nell'ottica del diritto all'oblio – il fatto che la persona coinvolta sia o meno un personaggio pubblico.

A tale riguardo, particolarmente interessante appare il contenuto del provvedimento adottato dal Garante nel 2008 nell'accoglimento di un reclamo presentato da un privato cittadino[27]. Nel caso di specie, il ricorrente richiedeva che non restassero associate perennemente al proprio nome in rete, per mezzo delle "scansioni" operate automaticamente dai motori di ricerca esterni al sito dell'editore, le notizie oggetto di un determinato articolo, considerato lesivo. Nella specie, il Garante ha ritenuto che i motivi prospettati apparissero meritevoli di specifica tutela tenuto conto del-

[27] Cfr. Autorità Garante per la protezione dei dati personali «Archivi storici online dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni – 8 aprile 2009 – [1617673]» disponibile al seguente indirizzo http://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/1617673.

le peculiarità del funzionamento di *Internet,* che può comportare la diffusione di un gran numero di dati personali riferiti ad un medesimo soggetto. In particolare, il Garante, evidenziando quella che, in definitiva, deve considerarsi l'essenza stessa del diritto all'oblio, ha posto l'accento sul fatto che deve essere garantita ad un soggetto, che ha intrapreso nuovi percorsi di vita personale e sociale, la possibilità di allontanarsi da vicende pregiudizievoli risalenti nel tempo. Tale diritto viene ostacolato per mezzo della rappresentazione istantanea e cumulativa derivante dai risultati delle ricerche operate mediante i motori di ricerca che «rischiano di riverberare comunque per un tempo indeterminato i propri effetti sugli interessati come se fossero sempre attuali».

Sonora appare la conclusione a cui è giunto il Garante in tale occasione. All'editore, infatti, è stato imposto di adottare ogni misura necessaria affinché le generalità del ricorrente non risultassero più direttamente rinvenibili attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito *Internet*.

7. La posizione della giurisprudenza italiana sul diritto all'oblio

In tema di diritto all'oblio, l'orientamento sviluppato dai giudici italiani appare meritevole di approfondimento. In particolare, la Cassazione è intervenuta sul tema statuendo che «il soggetto titolare dei dati personali oggetto di trattamento deve ritenersi titolare del diritto all'oblio anche in caso di memorizzazione nella rete Internet, mero deposito di archivi dei singoli utenti che accedono alla rete e, cioè, titolari dei siti costituenti la fonte dell'informazione»[28]. La Corte ha esplicitamente chiarito che sebbene l'interesse pubblico sotteso al diritto all'informazione, previsto dall'articolo 21 della Carta costituzionale, costituisca un limite al diritto fondamentale alla riservatezza, al sogget-

[28] Cass. Civ., Sez. III, 5 aprile 2012, n. 5525, in *Nuova giur. civ. comm*., 2012, 10,1.

to a cui appartengono i dati utilizzati deve essere correlativamente attribuito il diritto all'oblio.

Sebbene tale pronuncia, almeno parzialmente, si configuri come un *obiter dictum*[29], il riconoscimento espresso in capo al soggetto di uno specifico diritto all'oblio, anche al di fuori del classico paradigma diritto di cronaca/diritto di riservatezza, conferisce alla sentenza una portata innovativa.

La Suprema Corte, infatti, con tale pronuncia ha sancito e riconosciuto il diritto del soggetto a richiedere che non vengano ulteriormente divulgate notizie che, per il trascorrere del tempo, risultino ormai dimenticate o ignote alla generalità dei consociati.

In una pronuncia più risalente[30], la Corte di Cassazione aveva fornito alcune precisazioni al riguardo. Atteso che il trattamento dei dati personali può avere ad oggetto anche dati pubblici o già pubblicati, ha chiarito la Corte, il diritto all'oblio funge da limite per salvaguardare la *proiezione sociale dell'identità personale*, ovvero l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita – stante il lasso di tempo intercorso dall'accadimento del fatto che ne costituisce l'oggetto – di attualità delle stesse. La Suprema Corte, infatti, ha evidenziato che il trattamento di determinate informazioni può risultare non più giustificato o addirittura di ostacolo per il soggetto nell'esplicazione e nel godimento della propria personalità, in ragione del trascorrere del tempo.

Peraltro, già in una delle prime pronunce[31], la Corte aveva precisato che, in materia di trattamento di informazioni, il soggetto cui l'informazione si riferisce ha diritto al rispetto della propria identità personale o morale. In altre parole, l'interessato ha diritto a non vedere «travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale e, pertanto, alla verità della propria immagine nel momento storico attuale».

[29] Cass. Civ., Sez. III, 9 aprile 1998, n. 3679, in *Giust. Civ., Mass.,* 1998, 778.
[30] Cass. Civ., Sez. I., 25 giugno 2004, n. 11864, in *Giust. Civ.,* 2005, f. 11, I, p. 2731.
[31] Cass., Civ., Sez. I., 22 giugno 1985, n. 7769, *inedita*.

Più di tutto però, in materia, non può non essere ricordata la sentenza che la Suprema Corte ha emanato recentemente[32]. La questione, esaminata in primo grado dal Tribunale di Chieti, riguardava una condanna al risarcimento del danno per violazione del diritto all'oblio che aveva coinvolto sia il direttore sia l'editore di una testata giornalistica telematica, a motivo della permanenza di un articolo su una vicenda giudiziaria di natura penale che aveva coinvolto i ricorrenti per un fatto avvenuto tempo prima e che non si era ancora conclusa. Nella specie, i ricorrenti lamentavano che tale permanenza risultava pregiudizievole non solo per la propria reputazione personale ma anche per il danno di immagine arrecato all'attività commerciale dagli stessi gestita.

Giunta la questione dinanzi alla Suprema Corte, quest'ultima ha confermato la condanna al risarcimento del danno a carico del direttore e dell'editore della testata giornalistica. Nella specie, la Corte ha evidenziato che l'illecito trattamento di dati personali era stato correttamente ravvisato dal giudice di prime cure non già nel contenuto e nelle originarie modalità di pubblicazione e diffusione *on line* dell'articolo di cronaca e nemmeno nella conservazione e archiviazione informatica di esso, ma nel mantenimento del diretto ed agevole accesso a quel risalente servizio giornalistico pubblicato molto tempo prima e della sua diffusione sul web, anche in data successiva al ricevimento di specifica diffida da parte degli interessati. In particolare, secondo la Suprema Corte, il Tribunale aveva giustamente rilevato che risultava incontestato che digitando (tramite il motore esterno di ricerca *Google*) il nominativo dei ricorrenti si accedeva alla prima pagina del sito *web* che includeva, affiancato e associato alla reclamizzata attività del locale da loro gestito, anche il *link* sull'articolo di cronaca redatto tempo prima. Tale

[32] Cass. Civ., Sez. I., 24 giugno 2016, n. 13161, in Persona e Danno, con nota di F. Sassano, *Diritto all'oblio. Fissato un tempo perché gli accadimenti siano cancellati dagli archivi online,* al seguente indirizzo: https://www.personaedanno.it/riservatezza- privacy/diritto-all-oblio-fissato-un-tempo-perche-gli-accadimenti-siano-cancellati-dagli-archivi-on-line-cass-civ-13161-16-francesca-sassano.

consultazione risultava di facile accessibilità e consultabilità, di molto superiore a quelle dei quotidiani cartacei, tenuto conto dell'ampia diffusione locale del giornale *on line*. Inoltre, secondo quanto rilevato dal giudice di prime cure, indubbiamente, il persistere del trattamento dei dati personali aveva determinato una lesione del diritto dei ricorrenti alla riservatezza ed alla reputazione, soprattutto in relazione alla peculiarità dell'operazione di trattamento, caratterizzata dalla capillarità della divulgazione dei dati trattati e dalla natura degli stessi, particolarmente sensibili attenendo ad una vicenda giudiziaria penale.

La Suprema Corte, nell'ambito di tale vicenda giudiziaria, ha evidenziato come il diritto all'oblio si spinga oltre la mera tutela della *privacy* e come sia un diritto di derivazione perlopiù giurisprudenziale e di elaborazione dottrinale, grazie anche alle posizioni assunte dalle Autorità Garanti europee. Esso, secondo la Corte, è da intendersi proprio quale diritto dell'individuo ad essere dimenticato; diritto che mira a salvaguardare il riserbo imposto dal tempo ad un notizia già resa di dominio pubblico.

Il fondamento normativo in Italia del diritto all'oblio, secondo la Suprema Corte, è da rinvenire nel Codice della Privacy laddove prevede che il trattamento di dati non risulti legittimo qualora gli stessi siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o trattati (articolo 11 del decreto legislativo 196/2003). Inoltre, in base a quanto specifica ulteriormente l'articolo 7 del medesimo decreto, l'interessato ha il diritto di conoscere in ogni momento chi possiede i suoi dati personali e come li adopera, nonché di opporsi al trattamento dei medesimi, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettifica, l'aggiornamento o l'integrazione.

La pronuncia risulta particolarmente rilevante in quanto la Corte evidenzia come il diritto all'oblio non sia altro che la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca. Così come non va reso pubblico il fatto la cui diffu-

sione (lesiva) non risponda ad un reale interesse della collettività, allo stesso modo non va riproposta la vecchia notizia (anch'essa lesiva) quando ciò non sia più rispondente ad una attuale esigenza informativa.

La portata innovativa di tale sentenza è, inoltre, da ravvisarsi in due ulteriori profili. In primo luogo, la Corte evidenzia come l'attualità o meno della notizia vada valutata non già con riferimento al procedimento giudiziario, il quale, se ancora in corso, rischierebbe di dilatare i tempi del diritto all'oblio, subordinandolo ai ritardi della giustizia italiana e, peraltro, differenziandolo da soggetto a soggetto, bensì al fatto storico. In secondo luogo, la Corte ha riconosciuto la possibilità di esercitare il diritto all'oblio, con la conseguente rimozione delle informazioni pregiudizievoli, anche in corso di processo.

Nella direzione tracciata dalla Suprema Corte si è mossa anche la giurisprudenza di merito.

In una recente pronuncia[33], ad esempio, il Tribunale di Roma ha concretamente applicato i principi elaborati dalla Corte di giustizia dell'Unione Europea nella decisione *"Google Spain"* riconoscendo, però, la prevalenza dell'interesse pubblico sul diritto all'oblio dell'interessato. Il caso riguardava un avvocato, che nel 2014 aveva richiesto a *Google* di deindicizzare alcuni URL risultanti da una ricerca concernente il proprio nominativo con riferimento a vicende giudiziarie in cui risultava implicato. Si trattava, nella specie, di notizie di cronaca relative a una vicenda giudiziaria risalente agli anni 2012/2013 che lo vedeva coinvolto, insieme ad altri personaggi romani, esponenti del clero e soggetti riconducibili alla c.d. "banda della Magliana" in presunte truffe e guadagni illeciti. Il professionista si doleva che tali informazioni riferite dai risultati del motore di ricerca, oltre ad essere false, facevano riferimento a una risalente vicenda giudiziaria nella quale era rimasto coinvolto senza che fosse mai stata pronunciata alcuna condanna. Nondimeno, il Tribunale ha respinto la domanda, chiarendo che

[33] Trib. Roma, Sez. I, 3 dicembre 2015, n. 23771, *inedita.*

seppure essa risultava riconducibile al trattamento dei dati personali e al diritto all'oblio, quale parte essenziale del diritto alla riservatezza, i dati trattati risultavano da un lato recenti e dall'altro di interesse pubblico.

Il Tribunale, infatti, ha evidenziato che il trascorrere del tempo dall'accadimento dei fatti, ai fini della lesione del diritto all'oblio, si configura come elemento costitutivo essenziale. Invero, i dati di cui il ricorrente richiedeva la cancellazione risultavano recenti e dotati di una loro innegabile attualità, soprattutto in considerazione del ruolo pubblico del ricorrente, professionista esercente l'attività di avvocato in Svizzera.

Il Tribunale ha aggiunto poi un tassello ulteriore, discostandosi però da quanto la Corte di giustizia aveva precedentemente statuito nel caso *Google Spain*. Relativamente alle doglianze sulla falsità delle notizie riportate dal motore di ricerca, infatti, a parere del Tribunale, l'interessato è tenuto ad agire a tutela della propria reputazione e riservatezza esclusivamente nei confronti dei siti terzi che abbiano pubblicato notizie infedeli o non aggiornate con i successivi sviluppi, eventualmente a lui favorevoli, ma non nei confronti del gestore del motore di ricerca, poiché questo opera meramente quale *caching provider* ai sensi dell'articolo 15 del decreto legislativo 70/2003.

Il giudice di merito ha dunque chiarito che, nel bilanciamento tra diritto alla riservatezza e l'interesse pubblico a rinvenire sul *web* notizie relative a persone che svolgono ruoli pubblici, il diritto di informazione prevale su quello all'oblio. Degna di nota appare, in questo senso, la conclusione del Tribunale che ha evidenziato come in ogni caso il diritto all'oblio non possa e non debba essere utilizzato per abbellire o smacchiare la reputazione di un soggetto che svolge ruoli di rilevanza pubblica.

Interessante sul tema appare anche una recente sentenza del Tribunale di Milano[34]. Con tale pronuncia è stato imposto a *Google* di provvedere alla rimozione dei risultati connessi ad un articolo

[34] Trib. di Milano, Sez. I, 28 settembre 2016, n. 10374, *inedita*.

giornalistico riguardante una componente dell'Autorità Garante per l'Energia e il Gas (AEEG), la quale veniva apostrofata come la "raccomandata di Bersani".

Nella specie, il Tribunale di Milano, annullando il rigetto opposto dal Garante per la Privacy sul reclamo presentato dalla ricorrente, ha ordinato a *Google* di deindicizzare una pagina web in cui permaneva l'articolo del quotidiano "Il Giornale", dell'8 dicembre 2010, intitolato *"L'energia? Un affare di famiglia. Vince la raccomandata di Bersani"*.

Il Tribunale, al riguardo, ha evidenziato che a prescindere dal carattere diffamatorio o meno, i medesimi dati personali, che magari nell'immediato potevano essere trattati lecitamente dai mezzi di informazione nel nome di un prevalente «interesse pubblico», possono poi perdere quell'interesse se, circolando sul *web* a distanza di tempo, «risultano non aggiornati, non pertinenti, non completi». Il Tribunale, in questo caso, specifica che l'interesse alla pubblicazione delle informazioni contenute nell'articolo non prevale, non tanto su un diritto all'oblio, quanto su un diritto al «ridimensionamento della propria visibilità telematica», perché l'interesse collettivo alla pubblicazione di una notizia deve essere verificato nel tempo.

8. Conclusioni

Come evidenziato, i contorni del diritto all'oblio sono stati ora definitivamente tracciati attraverso il nuovo regolamento "*Data Protection*" adottato dal legislatore europeo. A partire dal 2018, si renderà necessario valutare gli effetti e le problematiche che sorgeranno dall'applicazione della nuova regolamentazione.

Per ciò che attiene al momento presente in Italia, la tutela in forma specifica messa a disposizione in seguito alla sentenza della Corte di giustizia, che si risolve in un *format* che consente di richiedere direttamente al motore di ricerca la rimozione dei contenuti ritenuti pregiudi-

zievoli, come chiarito, riguarda per lo più la *privacy* e non strettamente il diritto all'oblio. Ciononostante, la percentuale delle domande che trova positivo accoglimento si aggira intorno al 33%. Questo dato pone l'Italia come fanalino di coda in Europa.

Occorre invece rilevare che tanto l'Autorità Garante per la Privacy quanto la giurisprudenza si sono mostrate piuttosto propense a riconoscere e, in taluni casi ad implementare, il diritto all'oblio e i suoi contenuti, già prima della sentenza della Corte di giustizia. A maggior ragione, dopo la pronuncia della Corte, questa tendenza favorevole è stata ampiamente riconfermata.

Da quanto emerge dai provvedimenti e dalle pronunce esaminate, sono eminentemente due i fattori che occorre tenere in considerazione perché il diritto all'oblio possa essere esercitato con successo: il fattore tempo e il venir meno dell'interesse generale della collettività ad essere informato in merito a determinati accadimenti. Se entrambe le condizioni sono verificate, ovvero è trascorso un ragionevole lasso di tempo tale da rendere la conoscenza di quella notizia non più rispondente ad un interesse pubblico, il diritto all'oblio potrà essere esercitato con successo consentendo così all'interessato di ristabilire quella che viene definita una "reputazione digitale integra".

Laura Marchegiani
Università degli Studi di Macerata

Le licenze multiterritoriali per l'uso *online* di opere musicali nella disciplina comunitaria della gestione collettiva dei diritti d'autore: profili concorrenziali[1]

Sommario: 1.Premessa – 2. La disciplina delle licenze multiterritoriali, tra regolazione e concorrenza – 3. Segue. Le decisioni "Cisac" e "Osa". Verso il recupero della territorialità nell'intermediazione dei diritti *online*? – 4. L'ambito soggettivo di applicazione della disciplina comunitaria delle licenze multiterritoriali – 5. Lo statuto concorrenziale degli organismi di gestione collettiva che concedono licenze multiterritoriali per i diritti *online* – 6. Conclusioni

1.Premessa

Dare nuovo slancio all'economia europea attraverso il mercato unico digitale, da considerarsi come *locus artificialis* ove l'incontro tra domanda e offerta è costruito, governato, orientato e controllato dalla legge[2] e le potenzialità insite nel mercato unico potranno raggiungere una compiuta realizzazione, pure attraverso la promozione e lo sviluppo

[1] Il testo riprende, con il corredo delle indicazioni bibliografiche e tenendo conto dell'evoluzione *medio tempore* del quadro normativo di riferimento, le considerazioni esposte nel corso del convegno dal titolo "Il mercato unico digitale", tenuto nel Dipartimento di Giurisprudenza dell'Università di Macerata il 26 ottobre 2016.

[2] Una particolare suggestione esercita infatti la notissima definizione di N. Irti, *L'ordine giuridico del mercato*, Bari, 2001, p. 112, se applicata alla materia antimonopolistica, ove la regolazione rappresenta in effetti il "significante" del concetto di mercato. In senso convergente, si veda l'ampia analisi di M. Libertini, voce *Concorrenza*, in *Enc. dir.*, *Annali*, III, 2011, pp. 191 ss.

della distribuzione online delle opere dell'ingegno[3], rappresenta uno degli obiettivi-cardine della Agenda digitale europea[4], che puntualmen-

[3] Sottolinea le connessioni tra la promozione di una società digitale e la costruzione di un quadro regolatorio che favorisca lo sviluppo di nuovi modelli di distribuzione *online* delle opere dell'ingegno, allo scopo di stimolare le risorse creative e innovative presenti in ambito comunitario e promuoverne l'imprenditorialità nel settore culturale, M.L. Montagnani, *Il diritto d'autore nell'era digitale. La distribuzione online delle opere dell'ingegno*, Milano, 2012, pp. 77 ss.

[4] COM (2010) 245 del 26 agosto 2010, di cui si veda in particolare l'Azione fondamentale 1. Ma il sostrato politico dell'iniziativa può essere più compiutamente compreso alla luce della strategia Europa 2020 per una crescita intelligente, sostenibile e inclusiva [COM (2010) 2020], che evidenzia la necessità di realizzare un mercato unico per i contenuti e i servizi *online*, attraverso "mercati europei sicuri e senza frontiere per i servizi web e i contenuti digitali, caratterizzati da alti livelli di fiducia, un quadro normativo equilibrato con regimi chiari in materia di diritti, promozione delle licenze multi-territoriali, tutela e remunerazione adeguate per i titolari dei diritti".
La traiettoria evolutiva orientata al superamento delle limitazioni connesse alla territorialità delle legislazioni nazionali in tema di diritto d'autore è stata intrapresa fin dal Libro verde del 1988 "Il diritto d'autore e le sfide tecnologiche", 7 giugno 1988, COM (88) 172 def.: tra i documenti di maggiore rilievo, possono utilmente consultarsi la Comunicazione della Commissione "Un mercato unico dei diritti di proprietà intellettuale", 24 maggio 2011, COM(2011) 287 def., in ordine alla creazione di un quadro globale per il diritto d'autore nel mercato unico digitale, ed alla previsione di un quadro di *governance* europeo promotore dell'uso efficiente delle tecniche di tutela per creatori e utilizzatori delle opere; il Libro verde sulla distribuzione *online* di opere audiovisive nell'Unione europea del 13 luglio 2001, COM (2011) 427 def., che pone l'accento sull'esigenza di semplificazione dei processi di concessione delle licenze relative al diritto d'autore". Più di recente, la modernizzazione della legislazione comunitaria in tema di diritto d'autore ha insistito sull'individuazione delle modalità tecniche di superamento della frammentazione territoriale dei diritti, che persiste pure a fronte di "sistemi di regolazione giuridica regionali" (P. Spada, *Parte generale*, in Auteri e al., *Diritto industriale. Proprietà intellettuale e concorrenza*, Torino, 2016, 40) per lo più agendo a favore di una maggiore connettività, della facilitazione all'accesso dei servizi in linea, del potenziamento della portabilità transnazionale dei contenuti protetti e dei servizi che li utilizzano, ma anche usando gli strumenti di armonizzazione delle legislazioni degli Stati membri: si vedano, in particolare, la Comunicazione della Commissione "Verso un quadro normativo moderno e più europeo sul diritto d'autore", 9 dicembre 2015, COM (2015) 626 *final* e la Proposta di Regolamento del Parlamento europeo e del Consiglio che garantisce la portabilità transfrontaliera dei servizi di contenuti online nel mercato interno COM (2015) 627 *final*, nonché, principalmen-

te individua, nel descrivere le Azioni fondamentali all'uopo necessarie, l'esigenza di semplificare le procedure di autorizzazione e di gestione dei diritto d'autore per concedere licenze transfrontaliere, da un lato, e l'opportunità di rafforzare le regole di *governance*, di trasparenza e di capacità di trattare licenze paneuropee sui diritti online, dall'altro[5].

Una simile cornice regolatoria, secondo la Commissione Europea, attenuerebbe gli effetti deterrenti allo sviluppo di un mercato dei prodotti culturali che sono insiti nella frammentazione territoriale della disciplina sostanziale dei diritti d'autore[6] contribuendo alla creazione di un "mercato unico pienamente funzionante", ove creatività degli autori e capacità di promuovere servizi transfrontalieri innovativi da parte degli utilizzatori delle opere, potrebbero definitivamente espandersi[7].

Nel quadro programmatico così delineato, si inserisce la nuova disciplina della concessione di licenze multiterritoriali per l'uso *online*

---

te, la Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme relative all'esercizio del diritto d'autore e dei diritti connessi applicabili a talune trasmissioni online degli organismi di diffusione radiotelevisiva e ritrasmissioni di programmi televisivi e radiofonici, COM (2016) 594 e la Proposta di Direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale COM (2016) 593. Per una revisione critica dell'approccio sotteso al c.d. "copyright package" del 14 settembre 2016, comprensivo anche dell'implementazione del Marrakesh Treaty (Proposta di Regolamento COM (2016) 595 *final*), si vedano le osservazioni generali di MAX PLANCK INSTITUTE, *Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules*, al sito *www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Position_Statement_Part_A_Update24022017.pdf*

[5] Comunicazione della Commissione del 26 agosto 2010 COM (2010) *final* "Un'agenda digitale europea", p. 10.

[6] Si veda, ad esempio, la Comunicazione della Commissione "Verso un quadro normativo moderno e più europeo sul diritto d'autore", cit.

[7] L'attività di distribuzione online autorizzata di opere musicali si confronta, in Europa, con evidenti criticità, soprattutto dovute alla complessità delle transazioni in ambiente digitale ed alla non costante possibilità di accedere, sul territorio europeo, ad un ampio repertorio di opere per una vasta gamma di servizi musicali, Commission Staff Working Document, Impact Assessment 11 luglio 2012, SWD(2012) 204 *final*, p. 21

delle opere musicali, introdotta, in un'apposita sezione[8], con la Direttiva di riordino del sistema di gestione collettiva dei diritti d'autore[9]. Il percorso regolatorio della materia è tuttavia più risalente, potendosene individuare l'atto introduttivo, almeno per quanto concerne il profilo di disciplina delle licenze multiterritoriali per gli usi online delle opere musicali, nella Raccomandazione della Commissione dell'ottobre 2005 in tema di gestione transfrontaliera dei diritti d'autore e dei diritti connessi[10] che aveva già tentato di imprimere una spinta modernizzatrice ai

[8] Secondo il Parere del comitato economico e sociale europeo, COM (2012) 372 *final* – 2012/0180 (COD), in G.U. dell'Unione europea, 13 febbraio 2013, § 3.4, "sarebbe forse stato preferibile presentare due progetti di direttiva, una di portata generale sulle società di gestione collettiva e l'altra relativa alle licenze multiterritoriali per la distribuzione della musica online". Tuttavia, la stretta connessione tra le regole poste a presidio della trasparenza della gestione e della contabilità delle *collecting societies* e i meccanismi di ricerca dell'efficienza nella gestione delle licenze paneuropee si evidenzia nelle previsioni in materia di capacità di trattamento elettronico dei dati (art. 24), di trasparenza e correttezza delle informazioni sui repertori (artt. 25-26) e di correttezza e puntualità nelle comunicazioni sull'uso e sulle fatturazioni (art. 27) e nel pagamento dei titolari dei diritti (art. 28), che compongono lo statuto delle *collecting* dotate di *passport* per la concessione di licenze paneuropee. Inoltre, la combinazione di più intensi requisiti di trasparenza nell'azione delle società intermediarie con la previsione di condizioni abilitanti per la concessione del *passport* per la concessione di licenze paneuropee consentirebbe ai titolari dei diritti di avere una chiara rappresentazione, comprese le implicazioni di carattere finanziario, dell'opportunità che la loro società gestisca direttamente o tramite un accordo di rappresentanza la concessione multiterritoriale delle licenze, scegliendo, di caso in caso, la soluzione più appropriata e coerente con gli interessi dei titolari medesimi, *Impact of Assessment*, cit., pp. 190 ss.

[9] Il riferimento è al Titolo III della Direttiva 2014/26/UE del 26 febbraio 2014 sulla gestione collettiva dei diritti d'autore e dei diritti connessi e sulla concessione di licenze multiterritoriali per i diritti su opere musicali per l'uso *online* nel mercato interno ed al "corrispondente" capo III del D.Lgs. 15 marzo 2017, n. 35, (in G.U. n. 72 del 27 marzo 2017), che ne ha dato attuazione nell'ordinamento italiano.

[10] Raccomandazione della Commissione, del 18 ottobre 2005, sulla gestione transfrontaliera dei diritti d'autore e dei diritti connessi nel campo dei servizi musicali *on line* autorizzati, in G.U. dell'Unione europea, 21 ottobre 2005, n. L 276/54. Tra gli antecedenti di tale innovativa posizione (J. Drexl, *Competition in the Field of Collecting Management: Preferring "Creative Competition" to Allocate Efficiency in European Copyright Law*, in P. Torremans, (ed.), *Copyright Law*, *A Handbook of Contemporary Re-*

sistemi di licenze territorialmente universali, comprensive di tutti i diritti necessari alle attività di produzione professionale dei nuovi servizi introdotti dalla società dell'informazione, in particolare il *downloading* e la diffusione interattiva, ma anche il *webcasting* e il *simulcasting* non interattivi[11].

2. La disciplina delle licenze multiterritoriali tra regolazione e concorrenza

Tali istanze di modernizzazione, si inseriscono in un percorso ultraventennale di armonizzazione del diritto d'autore, alla ricerca di un difficile punto di equilibrio tra la natura statale e nazionale dell'esclusiva, so-

---

search, Edward Elgar, Cheltenham, 2007, pp. 256 ss., vanno segnalati, in ordine di prossimità decrescente, *Commission Staff Working Document*, *Study on a Community Initiative on the Cross-Border Collective Management of Copyright*, 7 luglio 2005, disponibile al sito http://ec.europa.eu/internal_market/copyright/docs/management/study-collectivemgmt_en.pdf e Comunicazione della Commissione al Consiglio, al Parlamento Europeo e al Comitato economico e sociale europeo "Gestione dei diritti d'autore e diritti connessi nel mercato interno", 16 aprile 2004, COM(2004) 261 definitivo.

[11] È probabilmente superfluo sottolineare che i fornitori dei servizi musicali online abbisognano, per la fornitura dei servizi innovativi - interattivi e non - introdotti dalla società dell'informazione, quali il download dei contenuti musicali e/o i servizi in streaming, (T. Lueder, *First Experience with EU Wide Online Music Licensing*, in *GRUR Int.*, 2007, pp. 649 ss.) dell'autorizzazione relativa ad una combinazione di diritti meccanici e di esecuzione per le applicazioni *online*, cui corrisponde una nozione unitaria di "diritti online" già delineata da Commissione, 19 aprile 2012, Case No COMP/M.6459 – Sony/Mubadala Development/Emi Music Publishing e poi ripresa dall'art. 3, Direttiva 2014/26/UE.
Il riferimento congiunto all'art. 2 - Diritto di riproduzione e all'art. 3 - Diritto di comunicazione di opere al pubblico, compreso il diritto di mettere a disposizione del pubblico altri materiali protetti, conferma la natura (anche) oggettivamente composita dei diritti online. Per la definizione dei servizi online la Direttiva richiama le disposizioni di un'altra Direttiva, la 98/34/CE, individuando tra i servizi della società dell'informazione individuati dall'art. 1.2, quelli oggetto del regime di licenze multi-territoriali qualora richiedano la concessione di licenze per opere musicali protette.

lo lambita dalla regolazione giuridica regionale dell'Unione, e l'ubiquità degli interessi sottesi alla proprietà intellettuale, enormemente potenziata dall'ambiente digitale, a seguito dell'evoluzione tecnologica[12].

L'architettura tradizionale del sistema di gestione, come è noto, si fonda(va) su una riserva di intermediazione – di fatto o di diritto[13] – a favore di un singolo ente o associazione per ciascun territorio nazionale[14].

[12] Sulla tendenza alla "disintermediazione" determinata dall'influsso delle nuove tecnologie, A.M. Gambino-A. Stazi, *Diritto dell'informatica e della comunicazione*, Torino, 2009, pp. 1 ss., e, per una visione prospettica del nuovo ruolo istituzionale delle *collecting*, sempre più orientato alla realizzazione dell'ottimalità allocativa, M. Ricolfi, *Figure tecniche di gestione, del diritto d'autore e dei diritti connessi*, in AA.VV., *Gestione collettiva dell'offerta e della domanda di prodotti culturali*, cit., pp. 6 ss., a pp. 24 ss. Si è osservato che l'attività di produzione professionale esercitata nel campo del diritto d'autore, ed in particolare nella distribuzione dei contenuti digitali ha perduto il carattere della intermediazione per acquisire quello della "organizzazione e della "aggregazione" E. Prosperetti, *L'opera digitale tra regole e mercato*, Torino, 2017, secondo una tendenza già emersa in ambito analogico, come osserva V. Falce, *Gestione dei diritti, disintermediazione e Collecting Societies. La modernizzazione del diritto d'autore*, in *AIDA*, 2012, pp. 97 ss, e destinata ad eliminare il ruolo intermediario delle *collecting*, V. Falce, *Copyright Societies Under Scrutiny: form the EU Approach to the Italian Solution*, in *World Competition*, 2014, pp. 121 ss.

[13] Esemplare, dell'ipotesi di monopolio di fonte legale, la posizione della Società Italiana degli Autori ed Editori, ente pubblico economico a cui, in base all'art. 180 L. 633/1942, è riservata in via esclusiva "l'attività di intermediario, comunque attuata". Vale la pena al riguardo di osservare che la natura imprenditoriale dell'attività della SIAE e la sua qualificazione di "soggetto rilevante per la normativa interna in materia di concorrenza" non si ritiene possano ricadere nell'ambito di operatività dell'eccezione indicata dall'art. 8, comma 2, L. 287/90, laddove consente di escludere dall'applicazione della disciplina antitrust nazionale alcune imprese che operano in regime di monopolio: così, M. Libertini, *Gestione collettiva dei diritti di proprietà intellettuale e concorrenza*, in AA.VV., *Gestione collettiva dell'offerta e della domanda di prodotti culturali*, cit., pp. 103 ss., spec. p. 117. Poiché i mercati nazionali dell'intermediazione tendono naturalmente ad assumere un assetto monopolistico, la previsione di un monopolio legale può fungere da meccanismo di selezione dell'operatore più efficiente: J. Drexl, *Competition in the Field of Collective Management*, p. 263 s.

[14] Per una descrizione della parabola evolutiva dei sistemi di gestione e dei soggetti ivi emergenti, D. Sarti, *Gestione collettiva e modelli associativi*, in AA.VV., *Gestione collettiva*, cit., pp. 30 ss., M. Ricolfi, *Figure tecniche*, cit., pp. 20 ss.

In un sistema di gestione collettiva costruito su base territoriale, con la diffusa previsione di regole di appartenenza obbligatoria ed esclusiva alla società di gestione dello Stato membro di residenza dell'autore, e la conseguente aggregazione dei repertori su base nazionale, le esigenze di autorizzazione transfrontaliera si realizzavano attraverso gli accordi di reciproca rappresentanza, che consentivano a ciascuna società nazionale di autorizzare l'esecuzione, sul proprio territorio, delle opere appartenenti ai repertori delle "consorelle" straniere[15], ma anche di concedere agli utilizzatori residenti licenze estese a tutti i territori nazionali degli enti parte degli accordi di rappresentanza volontaria.

L'introduzione nel modello convenzionale di clausole di residenza economica permetteva dunque di mantenere una delineazione territoriale pure in un sistema orientato alla creazione di uno sportello unico (c.d. *one-stop-shop*), tale da ridurre costi di transazione, altrimenti eccessivamente ingenti, per gli operatori dell'ambiente digitale[16].

La Commissione, agendo come garante della concorrenza, ha sotto-

---

[15] Per una rassegna delle numerose decisioni della giurisprudenza comunitaria sugli accordi di rappresentanza reciproca, E.J. Mestmäcker, *Collecting Societies*, in C.D. Ehlermann-I. Athanasiu (eds.), *The Interaction between Competition Law and Itellectual Property Law*, Oxford, 2005, pp. 343 ss.
Da segnalare, in particolare, la Decisione della Commissione, 71/224/CEE, *GEMA* in cui si vietava alle società di gestione collettiva di discriminare i titolari dei diritti in base alla nazionalità, sia con riguardo alle royalties corrisposte, sia con riguardo alla possibilità di affiliazione, negando anche la legittimità di contratti esclusivi su scala mondiale che vincolassero a lungo termine i titolari dei diritti. Nello stesso senso, Corte di giustizia, Causa 7/82, *GVL*, in *Raccolta*, 1983, 483.
Sulla restrittività dei contratti di rappresentanza reciproca, laddove prevedessero l'obbligo della società di gestione collettiva a non dare accesso al proprio repertorio agli utilizzatori di musica registrata stabiliti in altro Stato membro si pronunciano CGUE, Causa 395/87, *Tournier*, in *Raccolta*, 1989, 2521 e CGUE, Cause riunite 110/88, 241/88 e 242/88, *Lucazeau*.

[16] Il modello convenzionale di rappresentanza multiterritoriale si è sviluppato in tal senso per rispondere ai bisogni degli utilizzatori, P.M. Sanfilippo, *La gestione collettiva*, cit., p. 450. Al vantaggio per gli utlizzatori delle opere protette si aggiungerebbe il beneficio per i consumatori di poter accedere ad un più ampio repertorio, F. Gotzen, *Les licences multiterritoriales entre le juge et le législateur. Des affaires "Cisac" à la Directive 2014/26*, in *RIDA*, 2014, pp. 94 ss., spec. p. 137.

posto a scrutinio gli accordi di rappresentanza promossi in seno alle federazioni di società di gestione dei diritti d'autore e connessi, in due importanti pronunce. Nella decisione sul caso *Trasmissioni in simulcast*[17], ha affrontato il tema delle relazioni tra società e utilizzatori in ambito transfrontaliero, con riguardo alla utilizzazione *online* delle opere, esaminando l'esentabilità dell'accordo-quadro elaborato nell'ambito della Federazione Internazionale delle Industrie Fonografiche: come si è già accennato, il modello di accordo realizzava un unico sportello di acquisto delle autorizzazioni relative a repertori multipli aggregati su base monoterritoriale, estesi a livello paneuropeo in virtù degli accordi di rappresentanza reciproca[18]. Una volta eliminata la clausola di residenza economica[19], l'attenzione della Commissione si è incentrata sulla

[17]Il riferimento è alla Commissione, 8 ottobre 2002, caso COMP/C2/38.014, IFPI "Trasmissioni in *simulcast*" (2003/300/CE), in GUCE, 30 aprile 2003, L 107/58, avente ad oggetto l'esentabilità dell'accordo quadro elaborato dalla Federazione Internazionale delle Industrie Fonografiche e promosso come modello per i rapporti di rappresentanza reciproca tra le organizzazioni nazionali dei produttori fonografici, per favorire la concessione di licenze multi territoriali e multi repertorio alle emittenti radio e televisive per la trasmissione in *simulcast* delle riproduzioni fonografiche incluse nelle loro trasmissioni. Se ne veda un commento in L. Guibault-S. van Gompel, *Collective Management in the European Union*, in D. Gervais (editor), *Collective Management of Copyright and Related Rights*, 2^ ed., The Netherlands, 2010, pp. 144 ss. Sul tema, in dottrina, Riccio G. M., *Copyright Collecting Societies e regole di concorrenza. Un'indagine comparatistica*, Torino, 2012, pp. 128 ss.; Ercolani, S., *Dalla gestione collettiva*, cit., pp. 241 ss., Lamandini, M., *Televisioni, nuove tecnologie*, cit., p. 142.

[18] Lo stesso tipo di funzione economica concreta si riconnetteva all'accordo noto come Santiago Agreement, anch'esso censurato dalle autorità antitrust nella misura in cui, prevedendo una clausola di residenza economica della controparte, era incompatibile con il divieto delle intese.

[19] Le società di gestione dei diritti connessi dei produttori discografici avevano infatti rapidamente emendato il modello di accordo, disponendo che " le emittenti in *simulcast* stabilite nello Spazio economico europeo potranno rivolgersi a qualsiasi società di gestione collettiva stabilite nel SEE … per richiedere ed ottenere una licenza multi territoriale per la trasmissione in *simulcast* nei territori delle società partecipanti all'accordo" Commissione, 8 ottobre 2002, *Trasmissioni in simulcast*, cit., p. 2. La clausola di residenza economica, agevolmente soppressa dalle società rappresentative dei produttori discografici, è stata invece tenuta in maggior conto

composizione dei corrispettivi richiesti agli utilizzatori, considerando esentabile la fissazione dei compensi dovuti agli autori secondo le tariffe del paese di destinazione della trasmissione, ma non ammettendo che la residua area di concorrenza nella fissazione dei corrispettivi dei servizi di gestione fosse ulteriormente limitata[20].

Nella decisione sul caso CISAC[21], riguardante alcune clausole del modello di contratto di rappresentanza reciproca elaborato dalla Confederazione Internazionale delle Società di Autori e Compositori, e le pratiche concordate in materia di delimitazione dei territori che gli intermediari nazionali realizzavano sui mercati dei servizi amministrativi e della concessione di licenze, ha ritenuto che le clausole di affiliazione, le restrizioni territoriali bilateralmente convenute e le pratiche concordate di delineazione territoriale, pur realizzando l'obiettivo di offrire in ciascun territorio uno sportello unico per la gestione mondiale ed assicurando alcuni vantaggi in termini di efficienza, "non possono essere considerate indispensabili", se si valuta che i diritti interessati, di ese-

---

dalle società degli editori, tanto da impedire il rinnovo dell'accordo promosso dalla confederazione delle società dei autori, noto come Santiago Agreement, proprio per le perplessità sollevate dalla ritenuta contrarietà al divieto delle intese. L'accordo avrebbe invece meritato l'esenzione centralizzata, secondo F. Gotzen, *Les licences multiterritoriales*, cit., pp. 115 ss.

[20] La tariffa globale, imposta agli utilizzatori per la autorizzazione alla trasmissione in *simulcast* sarebbe comunque stata ampiamente predeterminata, poiché risultante dalla aggregazione di tutte le tariffe nazionali dei soggetti partecipanti all'accordo. Per sfuggire alla criticità concorrenziale della fissazione di prezzo, la Commissione svolge un articolato procedimento logico e argomentativo basato sulla scomposizione del prezzo in due elementi fondamentali, che le società di gestione collettiva si impegnavano a specificare: attraverso tale "isolamento" della componente corrispondente ai costi amministrativi, da quella relativa al compenso dovuto ai titolari dei diritti, ogni società di gestione collettiva avrebbe potuto prevedere uno sconto rispetto alla tariffa globale, in ragione dei propri minori costi di gestione. Nello stesso senso, la decisione della Commissione, 4 ottobre 2006, decisione 2007/735/CE, *Accordo di proroga di Cannes*.

[21] Commissione, 16 luglio 2008, C(2008) 3435 def, (Caso COMP/C2/38.698) *Cisac*, p. 51.

cuzione pubblica per le trasmissioni satellitari, via cavo e via Internet[22] sono caratterizzati da una spiccata "natura" e "vocazione" transfrontaliera, oltre che da procedimenti e costi di monitoraggio in larga misura indipendenti dalla vicinanza territoriale, essendo il controllo dell'utilizzazione delle opere realizzabile a distanza e con modalità telematica[23].

Che l'obiettivo perseguito dalla Commissione fosse quello di favorire il superamento dello sportello unico, in cui multiterritorialità e completezza dei repertori sono garantiti dalla combinazione di monopoli nazionali e accordi bilaterali di rappresentanza, e di promuovere un modello di gestione "liberalizzato", reso possibile dalle attuali infrastrutture tecnologiche, idonee a supplire efficacemente al ruolo locale degli intermediari (almeno per le ritrasmissioni via internet, via satellite e via cavo) con il controllo a distanza delle utilizzazioni, era ben chiaro anche dall'attività frattanto intrapresa, dalla Commissione medesima, nel ruolo di regolatore antimonopolistico.

La Raccomandazione del 2005[24] segna infatti un evidente scostamento dai modelli spontanei sviluppati dal mercato dell'intermediazione in ambito transfrontaliero, assegnando valore di pietra angolare del futuro sistema di concorrenza tra le società di gestione collettiva alla *autonomia negoziale* del titolare dei diritti, declinata in una triplice libertà di scelta: del soggetto cui affidare la gestione; dell'ambito oggettivo delle facoltà esclusive affidategli; dell'ambito territoriale della gestione[25]. È evidente la derivazione di una simile fisionomia dall'*acquis communautaire* in

[22] Sui contenuti della decisione, ampiamente, G.M. Riccio, *Copyright Collecting Societies e regole di concorrenza. Un'indagine comparatistica*, Torino, 2012, p. 133; S. Ercolani, *Dalla gestione collettiva alla gestione "à la carte". Licenze online a geometria variabile per la musica in Europa*, in *Dir. aut.*, 2009, pp. 232 ss.

[23] Il controllo a distanza della utilizzazione online delle opere musicali è in effetti reso possibile, limitatamente alle utilizzazioni *autorizzate*, dalla "identità elettronica" dell'opera e dall'unicità dell'indirizzo IP che identifica il personal computer: F. Gotzen, *Les licences multiterritoriales*, cit., pp. 105 ss.

[24] Citata *supra*, nota 10.

[25] Raccomandazione, 18 ottobre 2005, cit., § 3).

tema di applicazione delle regole antimonopolistiche alla gestione collettiva, con il divieto di ogni discriminazione dei titolari dei diritti per la nazionalità e la illegittimità di contratti esclusivi di lunga durata, tra autori e società, comprensivi di ogni prerogativa patrimoniale riveniente dall'attività creativa, anche futura[26]. Lo svolgimento della attività tipica delle società di gestione collettiva, pure in un regime di monopolio di fatto o di diritto[27] non le esonera dunque dal rispetto delle regole concorrenziali nelle diverse, ma funzionalmente convergenti, prospettive dell'accesso dei titolari dei diritti alla gestione collettiva, dell'accesso degli utilizzatori ai servizi transfrontalieri di intermediazione[28], del divieto

[26] Si vedano riferimenti *supra*, nota 15.

[27] Da segnalare, con riguardo alla posizione di monopolista di diritto assegnata alla Società Italiana Autori ed Editori dall'art. 180, l. aut., che la recente attuazione della Direttiva 2014/26, da parte del D.Lgs. 35/2017, non ha intaccato lo *status quo*. L'art. 2, dedicato alle definizioni, nel comma 1 riconduce la SIAE alla categoria degli organismi di gestione collettiva e, nel comma 2, introducendo la figura delle "entità di gestione indipendente", precisa che tale previsione lascia fermo quanto previsto dall'articolo 180 della legge sul diritto d'autore: dunque sembrerebbe che la presenza di altri operatori sul mercato dell'intermediazione non consenta in ogni caso agli utilizzatori di effettuare i pagamenti a soggetti diversi dalla SIAE. Al riguardo è forse opportuno rammentare che l'Autorità Garante della Concorrenza e del Mercato ha formulato, in alcuni pareri resi ex art. 22, L. 287/1990 in ordine alla proposta di direttiva prima (AS1009, del 24 dicembre 2012, in Boll.) ed alla relativa attuazione poi (AS 1281, 1 giugno 2016, in Boll. 19/2016 e AS1303, 19 ottobre 2016, in Boll. n. 37 del 24 ottobre 2016), alcune osservazioni critiche sull'ambito soggettivo di applicazione della disciplina: in primo luogo, pronunciandosi sul testo della proposta della Commissione, aveva ritenuto che la limitazione dei destinatari della direttiva alle sole società costituite su base associativa potesse produrre effetti discriminatori, determinando "criticità concorrenziali" nell'attività di intermediazione; in secondo luogo aveva osservato che il mantenimento della previsione dell'art. 180 l. aut., "una disposizione ormai isolata nel panorama degli ordinamenti degli Stati membri", avrebbe escluso la possibilità che organismi alternativi potessero operare sul territorio nazionale, raccomandando al legislatore di selezionare criteri attuativi della legislazione comunitaria tali da garantire un livello concorrenziale adeguato nel mercato interno, in modo analogo a quanto è accaduto nell'ambito dei diritti connessi. In fine, nelle considerazioni espresse sullo schema di decreto legislativo, sottolineava l'opportunità di stabilire l'alternatività dei requisiti fissati nell'art. 3, lett. *a)* e di ridimensionare, per sfuggire ad effetti restrittivi della concorrenza, il livello di patrimonializzazione necessario per l'accesso al mercato.

[28] Da cui deriva la affermazione di illiceità delle clausole di residenza economica,

di abuso di posizione dominante attraverso l'imposizione di prezzi non equi[29].

La fisionomia dell'attività di intermediazione e la selezione dei modelli di organizzazione della gestione collettiva sono sensibilmente influenzate dal sistema concorrenziale[30] e dai valori che vi sono coinvolti: è dunque necessario che nell'interpretazione della Direttiva di riordino dell'attività di intermediazione si tenga presente la prospettiva antimonopolistica, muovendo dall'enunciato, non di mera prassi linguistica, bensì evocativo della diffidenza comunitaria verso le "legificazioni" del mercato[31], del cinquantaseiesimo considerando, secondo cui "(l)e disposizioni della presente direttiva non pregiudicano l'applicazione del diritto in materia di concorrenza". E sebbene non possa revocarsi in dubbio la prevalenza della legge dell'Unione sulle decisioni delle Corti in materia di antitrust[32], la compatibilità concorrenziale delle condotte degli intermediari nell'ottica della valutazione concreta delle autorità preposte ai diversi livelli di controllo, appare indispensabile corollario

---

invece considerate essenziali, per la funzionalità del sistema di intermediazione transfrontaliera, soprattutto dalle società di autori, probabilmente nel timore di una *race to the bottom* nel mercato dei corrispettivi per i servizi di intermediazione, con evidente pregiudizio della vocazione solidaristica delle società generaliste: sul punto, attentamente, P.M. Sanfilippo, *La gestione collettiva*, cit., p. 452. Il potenziamento dei diritti connessi e lo sviluppo in tale ambito di modelli di intermediazione maggiormente orientati al mercato è peraltro considerato uno dei fattori determinanti la crisi dei tradizionali modelli associativi utilizzati nella gestione collettiva, D. Sarti, *Gestione collettiva e modelli associativi*, in AA.VV., *Gestione collettiva dell'offerta e della domanda di prodotti culturali*, cit., pp. 30 ss., a p. 46.

[29] Tale classificazione è proposta da E. J. Mestmäcker, *Collecting Societies*, cit., pp. 343 ss.

[30] Con l'avvertenza tuttavia che l'applicazione della disciplina antimonopolistica ed in particolare l'imposizione di obblighi di contrarre alle società in posizione dominante non sono sufficienti ad allineare il modello *market oriented* a quello solidaristico, né a rappresentare il denominatore comune di tipologie organizzative caratterizzate da strutturale disomogeneità degli interessi coinvolti: D. Sarti, op. loc. ult. cit.

[31] Sulla tutela della concorrenza come principio generale del diritto europeo, M. Libertini, *Diritto della concorrenza dell'Unione Europea*, Milano, 2014, pp. 57 ss.

[32] F. Gotzen, *Les licences multiterritoriales*, cit., p. 135.

dei principi generali di diritto europeo, pure nel quadro del nuovo statuto regolamentare disegnato dalla Direttiva[33].

3. Segue. Le decisioni "CISAC" e "OSA". Verso il recupero della territorialità nell'intermediazione dei diritti *online*?

È a questo punto utile verificare la compatibilità del modello di sviluppo concorrenziale del mercato della gestione collettiva delineato dalla regolazione, orientato a promuovere una maggiore competizione tra intermediari – non più protetti dalle delineazioni territoriali – sul mercato della fornitura di licenze agli utilizzatori[34], con le tendenze emergenti da alcune significative decisioni che hanno avuto occasione di vagliare la "sostenibilità" del sistema di gestione pluralista.

Nelle 23 sentenze gemelle rese nell'aprile 2013[35], il Tribunale dell'Unione europea, ha parzialmente annullato la decisione della Commissione sul contratto tipo degli accordi di rappresentanza reciproca elaborato dalla Confederazione Internazionale delle Società di Autori e Compositori e sulle pratiche concordate di cui si è prima discusso. Il Tribunale sembra contestare gli stessi postulati della liberalizzazione, discutendo uno dei fondamenti della superabilità del modello territoriale di rappresentanza, l'assunto per cui il controllo delle utilizzazioni delle opere *online* possa essere effettuato a distanza[36]: tale deduzione non è desti-

[33] La direttiva comunitaria dovrebbe colmare le carenze regolatorie lasciate intatte dalla applicazione del diritto antitrust e creare una base normativa uniforme che realizzi una "sintesi tra il diritto antitrust e i diritti d'autore", M. Libertini, *Gestione collettiva dei diritti,* cit., pp. 120 ss.

[34] Che potranno quindi rivolgersi ad una pluralità di rappresentanti del medesimo repertorio per ogni territorio, F. Gotzen, *Les licences multiterritoriales*, cit., p. 95.

[35] Di cui si prende in considerazione Tribunale UE, 12 aprile 2013, causa T-442/08, resa nei confronti della Confederazione Internazionale delle Società di Autori e Compositori.

[36] Commissione, 16 luglio 2008, *Cisac*, § 189 "ogni opera musicale ha un'identità elettronica, mentre ogni personal computer ha un indirizzo internet. Grazie a tali in-

nata a valere per il monitoraggio degli usi illeciti della musica, che non potrebbe efficacemente svolgersi se non su base territoriale[37].

Non sussisterebbero, per le società di gestione, incentivi economici idonei a supportare una simile attività di controllo sugli usi non autorizzati nel territorio dello Stato di residenza, se gli utilizzatori fossero poi liberi di richiedere la licenza legittimante a qualsiasi concorrente, diverso da chi ha operato in concreto la sorveglianza.

Secondo aspetto, non meno rilevante, sottolineato dal Tribunale, è quello degli effetti della "liberalizzazione" sulla composizione dei repertori, e dunque l'inevitabile tendenza alla loro frammentazione[38]. Con l'abbandono della delineazione territoriale dello sportello di accesso, le società titolari di repertori diversi non avrebbero interesse a porre in atto una cooperazione per aggregarli, essendo ciascuna in concorrenza

---

formazioni, le società di gestione collettiva sono in grado di garantire, al momento in cui rilasciano la licenza, che l'utilizzatore commerciale possa sapere con precisione quale opera musicale viene utilizzata, da quale computer e per quale finalità". Con la comunicazione di tali informazioni dall'utilizzatore all'intermediario, sarebbe poi agevole per quest'ultimo corrispondere le *royalties* ai titolari dei diritti. Analogamente, Commissione, 8 ottobre 2002, *Trasmissioni in simulcast*, §61: "(l)a concessione di licenze di diritti d'autore e diritti connessi in un contesto "on line" differisce in modo significativo dalla concessione di licenze tradizionale "off line" in quanto non è necessario alcun controllo fisico dei locali che detengono la licenza. Le funzioni di controllo devono necessariamente svolgersi direttamente su internet. I requisiti essenziali per poter controllare l'uso dei diritti d'autore e dei diritti connessi sono per tanto un computer e una connessione a Internet".

[37] Tribunale UE, 12 aprile 2013, T-442/08, cit., par. 156 s.

[38] Gli interpreti sono concordi nel ritenere che la frammentazione dei repertori produca conseguenze sfavorevoli alla preservazione della diversità culturale, in contrasto con il presupposto di intervento del legislatore comunitario indicato nel terzo considerando della Direttiva 2014/26: stabiliscono in particolare un nesso di proporzionalità diretta tra causa ed effetto L. Guibault-S. van Gompel, *Collective Management in the European Union*, in D. Gervais (ed.), *Collective Management of Copyright and Related Rights*, 2^ ed., Kluwer Law International, 2011, p. 141, mentre più sfumata è la posizione di E. Arezzo, *Competition and Itellectual Property*, cit., che ravvisa nella frammentazione uno dei fattori, insieme all'indebolimento delle piccole società intermediarie, idonei a pregiudicare il valore della diversità culturale.

con le altre per la concessione di licenze sui singoli repertori loro affidati in ogni territorio nazionale[39].

In una seconda importante pronuncia, la Corte di giustizia[40], ha affrontato la questione della compatibilità del sistema di monopoli nazionali combinati con gli accordi di rappresentanza reciproca, con il divieto di restrizioni alla libera prestazione dei servizi formulato dall'art. 56 TFUE. La Corte, dopo aver definito l'attività di facilitazione nell'ottenimento da parte dell'utilizzatore dell'autorizzazione all'uso delle opere protette e nel conteggio e versamento delle *royalties* dovute ai titolari dei diritti come prestazione di un "servizio", ai sensi della Direttiva 123 del 2006, ne ha giustificata la restrizione su base territoriale in ragione del perseguimento di uno scopo di interesse pubblico, rappresentato dalla tutela dei dritti di proprietà intellettuale. La restrizione alla libera prestazione di servizi in concreto realizzata con l'attribuzione di un monopolio legale sulla gestione, è infatti funzionale ad una gestione efficace dei diritti d'autore, la cui tutela, per essere effettiva, non può prescindere da un "controllo territorializzato". Non esistono infatti, allo stato attuale del diritto dell'Unione, metodi alternativi che possano consentire il raggiungimento di un omologo livello di tutela implicando minori effetti restrittivi[41].

Pare dunque che la tensione tra la domanda di efficienza caratteristica dei mercati concorrenziali e il dato ineludibile della territorialità della gestione dei diritti[42], rimanga cifra caratteristica di una materia fin

[39] Tribunale, 12 aprile 2013, cit., §§ 151 e 159.
[40] CGUE, 27 febbraio 2014, causa C-351/12. Per un commento, M.L. Bixio, *Ancora una* chance *per il sistema monopolistico delle* collecting societies. *Osservazioni sulla decisione della Corte di Giustizia dell'Unione Europea del 27 febbraio 2014 caso OSA*, in *Riv. dir. ind.*, 2015, II, pp. 83 ss.
[41] CGUE, caso OSA, par. 76.
[42] Tensione costantemente presente nella riflessione sulla promozione di un modello pluralista di gestione collettiva dei diritti d'autore: osserva molto bene la duplice tendenza delle linee riformatrici nel dibattito in materia, P.M. Sanfilippo, *La gestione collettiva*, cit., p. 445.

dall'origine connotata da una forte componente regolatoria[43] e da "posizioni di esclusività" positivamente riconosciute[44], e che dell'insieme di tali tratti caratterizzanti si debba essere avvertiti nella definizione delle regole[45] funzionali al raggiungimento di un assetto competitivo sostenibile sui due versanti del mercato di prestazione dei servizi: di gestione ai titolari dei diritti e di concessione di licenze agli utilizzatori[46].

Nel quadro così delineato, si possono tentare alcune osservazioni su due profili della Direttiva che assumono particolare rilievo nella definizione dello statuto concorrenziale degli intermediari multiterritoriali: l'ambito soggettivo di applicazione del Titolo III e la previsione di specifici obblighi a contrarre in capo ai soggetti che professionalmente producono il servizio di concessione di licenze su base transfrontaliera.

4. L'ambito soggettivo di applicazione della disciplina comunitaria delle licenze multiterritoriali

Destinatari della disciplina sulla concessione delle licenze multiterritoriali, secondo gli artt. 23 e 24 della direttiva, sono gli organismi di

[43] Lo sottolinea P.M. Sanfilippo, *La gestione collettiva dei diritti d'autore e connessi tra regolazione e concorrenza*, in *AIDA*, 2007, p. 443.

[44] Che non ne contraddice le origini privatistiche, considerando il percorso evolutivo delle tecniche di protezione degli interessi di particolare rilevanza generale nel nostro ordinamento, P. Rescigno, *Introduzione*, in AA.VV., *Gestione collettiva dell'offerta*, cit., 4.

[45] Propone di valorizzare le sfumature di significati diffusamente presenti nella Direttiva 2014/26 e nelle decisioni degli organi comunitari, F. Gotzen, *Les licences multiterritoriales*, cit., pp. 135 ss.

[46] Il contesto competititvo in cui operano el società di gestione appartiene, come è noto, alla categoria dei *two-sided markets*: J. Drexl - S. Nérisson - F. Trumpke - R.M. Hilty, *Comments of the Max Planck Institute for Intellectual Property and Competition Law on the Proposal for a Directive of the European Parliament and of the Council on Collective Management of Copyright and Related Rights and Multi-Territorial Licensing of Rights in Musical Works for Online Uses in the Internal Market COM (202)372*, disponibile al sito http://ssrn.com/abstract=2208971, p. 4.

gestione collettiva operanti nel territorio dell'Unione che svolgano il servizio di intermediazione dei diritti per gli usi *online*. Come è stato evidenziato nella valutazione di impatto che ha accompagnato il testo legislativo, sul mercato delle licenze paneuropee operano cinque organizzazioni principali, tutte caratterizzate da una composizione mista di *collecting societies* ed editori. Per effetto della Raccomandazione del 2005, infatti, i maggiori editori musicali hanno ritirato i propri diritti dalle società di gestione locali per affidarli a soggetti dedicati, come CELAS, GmbH partecipata da due storiche società di gestione nazionali (la tedesca GEMA e la britannica PRS for Music), nonché gestore dei diritti di riproduzione meccanica dell'editore EMI, e PAECOL, società interamente controllata dall'intermediario nazionale tedesco o ancora ARMONIA, Gruppo Europeo di Interesse Economico costituito, tra gli altri intermediari nazionali, dall'italiana SIAE, dalla francese SACEM e cui partecipano gli editori Sony e Universal Peer Music[47].

Si pone quindi la questione di qualificare tali soggetti, che si sono affermati sul mercato come produttori professionali[48] del servizio di concessione di licenze paneuropee, al fine di considerare se, ed eventualmente in quali limiti, siano destinatari delle regole che la Direttiva impone agli organismi di gestione collettiva per l'esercizio di attività intermediaria sui diritti *online* in ambito transfrontaliero[49].

---

[47] PAECOL gestisce i diritti meccanici dell'editore Sony: per un prospetto dei principali enti fornitori di licenze paneuropee, si veda l'*Impact Assessment*, cit., p. 105.

[48] Secondo l'argomento *a minori ad maius* il requisito della natura "unica o principale" della finalità di gestione dei diritti d'autore indicata nell'art. 3 lett. *a)* e *b)* direttiva e testualmente ripresa nell'art. 2, commi 1 e 2, D.Lgs. 35/2017, ben si inscrive nel requisito della professionalità caratteristico dell'impresa nel diritto italiano, di cui può dunque verificarsi la ricorrenza con riguardo alle entità titolari del *passport* paneuropeo. Peraltro, la definizione del carattere "unico" o "principale" dell'attività di amministrazione dei diritti d'autore e connessi risale alla Direttiva 93/83/CEE, pur non illustrandone adeguatamente "i dati tipologici", come osserva M. Libertini, *Gestione collettiva dei diritti*, cit., p. 103.

[49] La possibilità di ricondurre le figure soggettive dedicate alla gestione transfrontaliera alla categoria delle *collecting societies* è dibattuta: per una efficace sintesi

Le fattispecie di gestori collettivi delineate dalla direttiva sono principalmente due: gli organismi di gestione collettiva, cui è destinata la regolazione nel suo complesso, organizzati in forma non lucrativa, controllati dai titolari di diritti o da enti rappresentativi di titolari di diritti (organismi di gestione collettiva e/o associazioni di categoria); e le entità di gestione indipendenti, organizzate secondo un programma lucrativo, cui non partecipano, nemmeno indirettamente, i titolari di diritti[50], invece ampiamente esonerate sia dalle regole di *governance* che dallo statuto dei licenzianti multiterritoriali. Occorre quindi innanzi tutto domandarsi se gli operatori che si sono affermati sul mercato della gestione transfrontaliera dei diritti *online*, almeno nei casi in cui assumano una forma organizzativa con fini lucrativi, possano qualificarsi come "entità di gestione indipendenti" e ritenersi per tal via esonerati dall'applicazione della disciplina del Titolo III[51].

Se è corretto ritenere che l'*indipendenza* delle entità di gestione di cui alla lett. *b)* dell'art. 3 debba predicarsi con riguardo ai titolari dei diritti – e il tenore della lett. *i)* pare confermarlo – non sembra che le entità di gestione indipendente possano essere partecipate dagli organismi di gestione di cui alla lett. *a)*, che annoverano, tra i propri membri, i titolari dei diritti. Se pure si volesse dare un significato assoluto

---

dei termini della questione, si vedano D. Sarti, *La categoria delle collecting*, cit., p. 5, nt. 5) e R. Vuckovic, *Implementation of Directive 2014/26/EU on Collective Management and Multi-Territorial Licensing of Musical Rights in Regulating the Tariff-Setting Systems in Central and Eastern Europe*, in *IIC* 2016, pp. 28 ss., spec. p. 46, nt. 76.

[50] Entrambe le figure soggettive si caratterizzano, sul piano dell'oggetto, per l'esercizio di un'attività autorizzata "per legge o in base ad una cessione di diritti, una licenza o qualsiasi altro accordo contrattuale a gestire i diritti d'autore o i diritti connessi ai diritti d'autore per conto di più di un titolare dei diritti, a vantaggio collettivo di tali titolari, come finalità unica o principale".

[51] Il tema della individuazione della tipologia di *collecting* sottoposte alla direttiva non appare di agevole definizione, particolarmente di fronte alle nuove figure di gestione funzionali all'aggregazione di "soggetti specificamente individuati": D. Sarti, *La categoria delle collecting societies soggette alla direttiva*, in *AIDA*, 2013, pp. 3 ss.

all'esclusione degli organismi di gestione collettiva dalla nozione di titolari dei diritti di cui all'art. 3, lett. *c)* e quindi ritenere che la partecipazione di questi ad un organismo di gestione indipendente non implichi una partecipazione *indiretta* ad esso dei titolari dei diritti[52], le conseguenze di una simile interpretazione letterale non paiono da condividersi. Vi è infatti che, se si ammettesse che tali entità di gestione indipendente possano organizzare organismi di gestione collettiva in un programma con finalità lucrative, realizzando una *collecting* di *collecting* caratterizzata dalla autodestinazione dei risultati, ne deriverebbe una ingiustificata disparità di trattamento tra le *collecting* di secondo grado organizzate senza scopo di lucro, che sarebbero destinatarie dell'intera disciplina della direttiva, come si evince dal combinato disposto delle definizioni di cui all'art. 3, lett. *a)* e *d)*[53], e le prime, cui sarebbero applicate solo alcune disposizioni, tra le quali si segnalano la previsione del dovere di condurre in buona fede le negoziazioni per la concessione di licenze[54] e la sottoposizione ad una comune area di con-

[52] In questo senso, invece, sulla scorta della esclusione testuale degli organismi di gestione dalla definizione di "titolare di diritti" di cui all'art. 3, lett. *c)*, E. Arezzo, *Competition and Intellectual Property Protection*, cit., 546, nota 62. È peraltro opportuno sottolineare come la questione della sottoposizione alla disciplina delle entità di gestione indipendenti del Gruppo Europeo di Interesse Economico denominato ARMONIA possa escludersi sulla base della mancanza, nella forma organizzativa prescelta, dello scopo di lucro.

[53] Sull'ammissibilità delle *collecting* di secondo grado, D. Sarti, *La categoria*, cit., p. 31.

[54] Il significato della previsione, con il mancato richiamo del par. 2 dell'art. 16, ove si prescrive che la condizioni di concessione delle licenze siano basate su condizioni oggettive e non discriminatorie, rischia di divenire puramente pleonastico, in considerazione della clausola generale della buona fede in materia (pre)contrattuale: R. Sacco, *Il contratto*, in *Trattato di dir. civ.* diretto da R. Sacco, 3^ ed., Torino, 2004, pp. 233 ss.; V. Roppo, *Il contratto*, in *Trattato di dir. priv.* diretto da G. Iudica e P. Zatti, Milano, 2001, pp. 175 ss. Non sembra, almeno stando alla interpretazione letterale, che dall'applicazione parziale dell'art. 16 alle entità di gestione indipendenti possa farsi derivare quell'"obbligo di contrarre a condizioni ragionevoli" che rappresenta il tradizionale bilanciamento, in termini di autonomia contrattuale, alla situazione di monopolio delle *collecting*: dubitativo, sul punto, D. Sarti, *Appunti in tema di legittimità ed estensione del monopolio SIAE*,

trollo da parte delle autorità competenti designate dagli Stati membri[55].

Che la disciplina dell'attività di gestione collettiva dei diritti d'autore, quale insieme di regole che discende dall'individuazione della corrispondenza ad un certo modello di comportamento positivamente individuato non debba dipendere dal codice organizzativo prescelto, ma debba applicarsi sulla base della consistenza oggettiva del fenomeno produttivo, è peraltro chiarito nel quattordicesimo considerando, ove si demanda agli Stati membri la predisposizione delle misure atte ad evitare "che la scelta della forma giuridica permetta di aggirare gli obblighi previsti dalla … direttiva". Sul punto mette solo conto di osservare che la questione dell'ambito soggettivo di applicazione della disciplina armonizzata, e dunque anche di quella sulle licenze multiterritoriali, aveva indotto l'Autorità Garante a sottolineare le "potenziali criticità concorrenziali derivanti dalla scelta di individuare quali destinatari della direttiva esclusivamente le società di gestione a base associativa", affermando che "al fine di evitare discriminazioni con potenziali implicazioni anticompetitive nell'attività di intermediazione interessata dalla normativa in discussione" è auspicabile che si giunga ad una "applicazione generalizzata dei requisiti soggettivi previsti dalla direttiva a tutti i soggetti che intendono esercitare l'attività di gestione dei diritti d'autore e dei diritti connessi, con le eventuali differenziazioni del caso idonee a salvaguardare le specificità dei singoli soggetti interessati. Ciò al fine di garantire parità di condizioni ai diversi operatori presenti nel mercato".

Escluso dunque che gli organismi ibridi possano avvantaggiarsi della qualificazione in termini di entità di gestione indipendenti ai fini di un ampio esonero dalle disposizioni della Direttiva, occorre valutare se essi siano invece destinatari della previsione dell'art. 2, comma 3, se-

---

Nota a Trib. Milano, 12 settembre 2014, (ord.), in *AIDA*, 2015, III, pp. 2 ss.

[55] L'art. 2.4 della Direttiva richiama infatti l'articolo 16 par. 1, gli articoli 18 e 20 e l'articolo 21 par. 1, lettere *a)*, *b)*, *c)*, *e)*, *f)*, e *g)* e gli articoli 36 e 42 che si applicheranno a tutte le entità di gestione indipendente stabilite nell'Unione.

condo cui le disposizioni *pertinenti* "si applicano alle entità direttamente o indirettamente detenute o controllate, integralmente o in parte, da un organismo di gestione collettiva purché tali entità svolgano un'attività che, se condotta da un organismo di gestione collettiva", vi sarebbe soggetta[56]. L'aggettivo *pertinente*[57] assume così portata decisiva al fine di stabilire quali regole dello statuto speciale previsto dalla direttiva per gli organismi di gestione collettiva, possano essere estese ai gestori c.d. ibridi[58].

Al riguardo va osservato che la clausola di salvezza così delineata prende il posto, attenuandone sensibilmente il contenuto precettivo, dell'art. 31 della proposta di direttiva, ove si disponeva che i soggetti controllati o partecipati da società di gestione collettiva fossero sottoposti a parte della disciplina in materia di concessione di licenze multiterritoriali[59]. È significativo, però, che, anche nella versione in cui più forte appariva l'intento di sottoporre a regolazione l'attività dei gestori ibridi, si escludesse l'applicazione delle norme in tema di obbligo di rappresentanza e di accesso alle licenze multiterritoriali, di cui tra poco si dirà[60].

---

[56] Subentra all'abrogato art. 31 della proposta, ove si prevedeva che le regole su capacità trasparenza e correttezza imposte ai gestori di licenze multiterritoriali si applicassero anche alle entità controllate o partecipate da organismi di gestione collettiva, che svolgessero la medesima attività.

[57] L'esistenza di una relazione di immediata reciprocità (tra disposizione espressiva della norma di comportamento e l'attività esercitata dal soggetto controllato o partecipato dall'organismo di gestione) sembra caratterizzare in modo univoco il significato della clausola di apertura così delineata, almeno a tenore delle parole utilizzate nelle principali traduzioni del testo della direttiva ("relevant", "pertinentes" "einschlagigen" "pertinentes").

[58] Che il quadro delineato dalla direttiva non abbia intaccato la legittimità dei monopoli nazionali, né abbia segnato l'abbandono di un piano competitivo a forte connotazione regolatoria, è sottolineato da D. Sarti, *Appunti*, cit., p. 9.

[59] Sull'*iter* della disposizione, riflesso di differenti percezioni del ruolo degli enti di gestione indipendente sul mercato dei diritti *online*, E. Arezzo, *Competition*, cit., p. 14.

[60] L'art. 31 della Proposta, infatti, rubricato "Concessione di licenze multiterritoriali da parte di controllate di società di gestione collettiva" richiamava gli articoli 18

5. Lo statuto concorrenziale degli organismi di gestione collettiva che concedono licenze multiterritoriali per i diritti *online*

Il sistema di gestione delineato dalla direttiva si basa sulla previsione di speciali "capacità" di trattare per via elettronica, in modo trasparente ed efficace, i dati necessari alla gestione delle licenze transfrontaliere e dunque della disponibilità di risorse di elaborazione e di amministrazione elettronica dei dati che consentano di identificare i repertori rappresentati e di controllare le utilizzazioni, allo scopo di permettere una tempestiva e accurata fatturazione e distribuzione delle somme dovute ai titolari dei diritti.

Ciò significa che solo le organizzazioni dotate dei requisiti organizzativi necessari – e soprattutto delle infrastrutture tecnologiche idonee – a realizzare le condizioni di attività indicate nell'art. 24 della Direttiva[61] potranno operare sul relativo mercato, secondo le condizioni di accesso determinate dagli Stati membri.

Già all'indomani della Raccomandazione del 2005 è stato osservato come l'adozione della prospettiva dei titolari dei diritti, con il riconoscimento di una ampia libertà di scelta in ordine a soggetto, oggetto e territorio coinvolti nell'attività autorizzata di concessione di licenze, avrebbe promosso nel mercato dei servizi loro dedicati l'emersione di un monopolio naturale, anche in quegli ordinamenti in cui non fosse

---

[par. 1, lett. *a)* e *c)*], 22, 23, 24, 25, 26, 27, 32 e 36, omettendo dalla serie dei richiami le disposizioni degli artt. 29 e 30. Ora, sebbene l'omissione del richiamo non necessariamente debba significare divieto di applicare il contenuto precettivo della norma attraverso diverse tecniche interpretative (sul punto, R. Guastini, *L'interpretazione dei documenti normativi*, in *Trattato Cicu-Messineo*, Milano, 2004, pp. 103 ss.) certamente è indicativo dell'intento del legislatore di non prevedere limitazioni dell'autonomia contrattuale dei gestori ibridi a prescindere dalla valutazione del potere di mercato degli stessi.

[61] In senso contrario alla previsione di requisiti patrimoniali minimi per l'esercizio dell'attività di intermediazione dei diritti connessi, che non siano rigorosamente proporzionati alla natura, alla complessità e alla dimensione dell'attività medesima, Autorità Garante della Concorrenza e del Mercato, *Parere* AS 1303, cit., p. 32.

prevista una riserva legale di attività[62]. Una predizione analoga si può a ragione formulare con riguardo al mercato della concessione di licenze transfrontaliere. Da un lato, infatti, la sussistenza dei requisiti postulati dal *passport* paneuropeo non sarà predicabile a tutte le società di gestione collettiva strutturate su base nazionale, ma più probabilmente si realizzerà in (pochi) organismi del tipo di quelli già esistenti, siano essi *collecting* di *collecting*[63] o, più probabilmente, forme organizzative a composizione mista[64]; d'altra parte, è noto che per gli utilizzatori, ossia per i fornitori dei servizi musicali *online*, i repertori sono tutt'altro che sostituibili, essendovene alcuni – quale quello Anglo-Americano - essenziali per la fornitura di servizi musicali: l'esito della concorrenza sui repertori potrebbe facilmente determinare una posizione di vantaggio nel mercato *downstream*, ove i gestori esclusivi delle opere maggiormente apprezzate dal pubblico sarebbero favoriti[65].

---

[62] J. Drexl, *Competition in the Field of Collective Management*, cit., p. 270.

[63] Secondo D. Sarti, *La categoria delle collecting societies*, cit., pp. 27 ss., le *collecting* di secondo grado potrebbero rientrare nella nozione di organismo di gestione armonizzata a condizione che siano caratterizzate dalla funzione associativa di tutela dell'interesse di categoria dei titolari dei diritti intermediati, non, invece, qualora agiscano quali meri gestori di interessi individuali.

[64] E. Arezzo, *Competition*, cit., p. 551. Anche negli Stati Uniti la liberalizzazione ha condotto ad un assetto oligopolistico, R. Pardolesi-A.Giannaccari, *Gestione collettiva e diritto antitrust: figure in cerca d'autor(i)?*, in AA.VV., *Gestione collettiva*, cit., pp. 49 ss., a pp. 99 ss.

[65] Chiaramente sul presupposto che una clausola di esclusiva a favore della società di gestione per l'intermediazione dei diritti *online* sia ammissibile nell'ordinamento attuale: così, E. Arezzo, *Competition*, cit., p. 552, osservando che solo gli accordi di reciproca rappresentanza tra *collecting* debbono avere natura "non esclusiva".

La misurazione del valore economico dei repertori mostra la posizione dominante detenuta nel mercato mondiale dal repertorio Anglo-Americano, G. Mazziotti, *New Licensing Models for Online Music Services in the European Union: From Collective to Customized Management*, in *Columbia Journal of Law and the Arts*, 2011, vol. 34 (4), pp. 757 ss. spec. pp. 770 ss. Così anche R. Vuckovic, *Implementation of Directive 2014/26/EU on Collective Management and Multi-Territorial Licensing of Musical Rights in Regulating the Tariff-Setting Systems in Central and Eastern Europe*, in *IIC* 2016, pp. 28 ss., spec. p. 5

Proprio per evitare che le piccole società di gestione collettiva rimangano ai margini del sistema della gestione di licenze multiterritoriali e che tale marginalità si ripercuota sulla preservazione della diversità culturale degli Stati membri, che è pure tra gli interessi protetti dalla Direttiva[66], gli articoli 30 e 31, di valore centrale nel sistema di gestione paneuropea promosso dal legislatore comunitario[67], definiscono un meccanismo, detto di *tag-on*, con un duplice obiettivo: da un lato consentire anche alle *collecting* minori di (far) accedere (i propri repertori) al sistema delle licenze multiterritoriali, così che le opere degli autori meno conosciuti siano offerte agli utilizzatori alle stesse condizioni alle quali viene offerto il resto dei repertori rappresentati dall'organismo paneuropeo (considerando 46, e art. 30 par. 4 "l'organismo di gestione collettiva interpellato include il repertorio rappresentato dell'organismo di gestione collettiva richiedente in tutte le offerte che trasmette ai fornitori di servizi online"). Ciò contrasterebbe, almeno in parte, il monopolio, anche culturale, dei grandissimi editori musicali, favorendo la possibilità di accesso alle licenze transfrontaliere di opere non (ancora) appetite dal mercato[68]. D'altro lato, il sistema dell'obbligo di rappresentanza è funzionale alla aggregazione dei repertori, che dovrebbe agevolare gli utilizzatori riducendo il numero di entità licenzianti cui rivolgersi per poter conseguire le autorizzazioni relative al repertorio mondiale, e quindi riprodurre i risultati pratici cui si perveniva grazie alla rete di accordi di reciproca rappresentanza in cui la delineazione territoriale riguardava il punto di accesso per la concessione della licenza transfrontaliera.

[66] Si è già fatto cenno al terzo considerando, ove si precisa che l'Unione "deve tenere conto della diversità culturale nell'azione che svolge e contribuire al pieno sviluppo delle culture degli Stati membri nel rispetto delle loro diversità nazionali e regionali".

[67] "*The most important provisions of Title III*", secondo J. Drexl-S. Nérisson-F. Trumpke-R.M. Hilty, *Comments*, cit., p. 28.

[68] Sottolinea il rischio della sostituzione di una valutazione tipicamente imprenditoriale a quella del pubblico, che dovrebbe invece fungere da effettivo stimolo alla innovazione estetica, J. Drexl, *Competition in the Field of Collective Management*, cit., p. 266.

Ora, una delle critiche più convincenti alla proposta di direttiva, nella sua connotazione orientata al mercato, era proprio quella di non prevedere – a fronte di un'amplissima libertà di scelta del titolare dei diritti – il supporto di limitazioni dell'autonomia privata, e talvolta di chiari e univoci obblighi a contrarre, idonei a riequilibrare i differenti ordini di rapporti tra *collecting*, titolari dei diritti ed utilizzatori[69], è dunque alle previsioni di tali obblighi che debbono dedicarsi alcune considerazioni più puntuali.

Le condizioni degli accordi bilaterali di rappresentanza per la gestione di licenze multiterritoriali sono definite dall'art. 29, ove l'autonomia delle parti è limitata dal divieto di prevedere una clausola di esclusiva. Sembrerebbe derivarne la facoltà, per ogni organismo di gestione collettiva, di affidare il proprio repertorio a più di un'entità paneuropea per la concessione transfrontaliera dei diritti *online* agli utilizzatori: sebbene una simile disposizione promuova una apertura più ampia del mercato della concessione di licenze, non ne vanno sottaciuti gli effetti negativi, in termini di efficacia del controllo sulle utilizzazioni illecite dei contenuti e di frammentazione dei repertori rappresentati, che la giurisprudenza comunitaria ha posto in evidenza[70]. Un'interpretazione più coerente con le tendenze emerse in sede europea, invece, condurrebbe ad intendere il divieto di esclusiva nel senso di riservare al mandante la facoltà di concedere licenze dirette extraterritoriali sul proprio repertorio a qualsiasi utilizzatore, ovunque stabilito, secondo una soluzione già formulata dall'antitrust europeo, per gli

[69] La titolarità di una posizione di monopolio delle *collecting* nei due versanti del mercato avrebbe dovuto implicare la illiceità del rifiuto di contrattare con i titolari dei diritti e con gli utilizzatori, tuttavia sarebbe stato auspicabile prevedere precise obbligazioni in tale senso, J. Drexl-S. Nérisson-F. Trumpke-R.M. Hilty, *Comments of the Max Planck Institute for Intellectual Property and Competition Law on the Proposal for a Directive of the European Parliament and of the Council on Collective Management of Copyright and Related Rights and Multi-Territorial Licensing of Rights in Musical Works for Online Uses in the Internal Market COM (202)372*, disponibile al sito *http://ssrn.com/abstract=2208971*.

[70] Vedi *supra*, par. 3.

usi *offline*, ma con analoghe argomentazioni giustificative in termini di ritorno degli investimenti in strutture localizzate di monitoraggio, nel caso *Tournier*[71]. Vale infatti la pena di osservare che, pure a seguito della creazione di nuove figure di gestione delle licenze multiterritoriali per gli usi *online*, successivamente alla Raccomandazione del 2005, il regime non esclusivo della rappresentanza degli organismi di gestione ibridi non abbia prodotto effetti apprezzabili sul pluralismo degli enti licenzianti: sebbene infatti i contratti non contengano più clausole di esclusiva, l'apparenza di esclusività della gestione transfrontaliera in capo ad alcune figure soggettive mandatarie di importanti editori musicali rimane ben radicata nello stato soggettivo degli utilizzatori[72].

L'art. 30 impone all'organismo dotato di *passport* paneuropeo, un "obbligo di rappresentare" gli altri organismi di gestione collettiva, privi dei requisiti necessari per svolgere l'attività di gestione transfrontaliera, se questi "già concede o offre la concessione di licenze multiterritoriali per la stessa categoria di diritti su opere musicali *online* del repertorio di uno o più altri organismi di gestione collettiva". La previsione dell'obbligo a contrarre in capo all'organismo paneuropeo, lo si è già accennato, dovrebbe consentire a tutti i repertori – ed in particolare a quelli gestiti dai piccoli intermediari – di accedere al sistema delle licenze multiterritoriali, e tuttavia esso non opera se l'organismo offre licenze multiterritoriali limitate al proprio repertorio[73]. La funzione precipua di tale eccezione è quella di consentire alle *collecting* che lo vogliano di specializzarsi su particolari categorie di opere musicali mantenendo l'unicità e la specificità del repertorio, a favore della promozione della diversità culturale[74]. La preservazione della diversità cultu-

[71] CGUE, 13 luglio 1989, C-395/87, *Tournier*.
[72] Illustra molto bene queste dinamiche, G. Mazziotti, *New Licensing Models*, cit., pp. 22 ss.
[73] La disposizione solleva altre perplessità, in ordine.
[74] Commission Staff Working Document, 7 luglio 2005, cit., par. 3.3 e 4.1. Il senso della disposizione è anche chiarito dal quarantaseiesimo considerando, ove il riferimento è agli organismi di gestione che si limitano a gestire in ambito transfronta-

rale rappresenta dunque la *ratio* che accomuna la previsione del meccanismo c.d. di *tag-on*, e la norma che esclude l'obbligo di contrarre per i gestori di un unico repertorio. Mi pare dunque da escludere che di una simile eccezione possano avvalersi gli organismi di gestione che partecipano alle figure soggettive ibride di cui si è parlato – a prescindere dalla discussa possibilità di qualificare queste ultime, con pienezza di effetti, quali organismi di gestione collettiva[75] – anche qualora gestiscano i diritti online di un unico titolare[76]. Per questa via mi sembra sostenibile l'ipotesi che alla *collecting* partecipante ad un gestore multiterritoriale, possa applicarsi l'obbligo di far accedere il repertorio di una società di gestione priva di *passport* che ne faccia richiesta, al sistema di concessione di licenze organizzato su base paneuropea[77]. A voler diversamente ritenere, si determinerebbe una ingiustificata disparità di trattamento, nel mercato dei servizi di intermediazione transfrontaliera dei diritti *online*, in base alla forma di aggregazione che è stata prescelta nel mercato della raccolta dei diritti. Il che mi pare in contra-

---

liero "il proprio repertorio".

[75] Il punto, come si è visto, è dibattuto, ma per la negativa, efficacemente, D. Sarti, *La categoria*, cit., pp. 43 ss.

[76] È il caso di organizzazioni come CELAS e PAECOL, su cui diffusamente, G. Mazziotti, *New Licensing Models*, cit., pp. 12 ss.

[77] In questa ipotesi l'obbligo di contrarre prescinderebbe dall'accertamento del potere di mercato e potrebbe apparire una restrizione ingiustificata dell'autonomia contrattuale dell'organismo di gestione, tuttavia vanno segnalati due argomenti che possono in parte confortare una simile soluzione: in primo luogo, la tendenza del mercato della gestione collettiva ad assumere un assetto fortemente concentrato, non solo per effetto della regolazione; dall'altro la previsione di una struttura dei corrispettivi per i servizi di gestione (art. 30.5) che, sebbene possa determinare un aumento complessivo dei costi di gestione, certamente evita il pericolo della produzione di diseconomie di scala in capo agli enti licenzianti. Preconizzano la tendenza al monopolio europeo di un unico organismo di gestione transfrontaliera, come effetto dell'applicazione degli artt. 31 e 31, J. Drexl-S. Nérisson-F. Trumpke-R.M. Hilty, *Comments*, p. 30.

Vale comunque la pena di osservare che, nell'ipotesi del probabile conseguimento di una posizione dominante da parte di una o più entità licenzianti diverse dalle *collecting societies*, si aprirebbe la strada ad una applicazione rigorosa delle regole a tutela della concorrenza, D. Sarti, *La categoria*, cit., pp. 42 ss.

sto con i corollari applicativi che derivano dal quattordicesimo considerando, per cui gli Stati membri devono "evitare che la scelta della forma giuridica permetta di aggirare gli obblighi previsti dalla presente direttiva".

Gli obiettivi delle norme in materia di licenze multiterritoriali non potrebbero essere raggiunti interamente, e la formazione di un piano comune di competizione per le società di gestione collettiva nella prestazione dei servizi ai propri membri non potrebbe avvenire, se questi ultimi non fossero posti in condizione di accedere al sistema della concessione di licenze multiterritoriali anche nelle ipotesi in cui le società cui hanno affidato la gestione non concedano, né direttamente, né attraverso la rappresentanza da parte di altre società, licenze paneuropee per l'utilizzazione *online* dei diritti esclusivi[78].

[78] Alcuni commentatori hanno osservato che la creazione di un vero punto unitario di accesso alle autorizzazioni multiterritoriali e multirepertorio si sarebbe potuto avere optando per il sistema di licenze collettive estese, eventualmente integrata con il principio del paese di origine, avrebbe funzionato secondo un meccanismo presuntivo per cui ogni società di gestione collettiva avrebbe potuto concedere una licenza multiterritoriale per tutti gli usi online dei diritti ricompresi nel proprio repertorio, purché fosse dotata di rappresentatività e quindi incaricata di fornire i servizi di gestione – direttamente da parte dei titolari dei diritti e indirettamente in virtù di accordi di rappresentanza reciproca con altre società di gestione collettiva – di una quota significativa delle opere utilizzate sul mercato (*Impact Assessment*, cit., pp. 45 ss.).
In tale modello sarebbe rimasta intatta la possibilità che i titolari dei diritti e gli editori esercitassero i diritti esclusivi direttamente o attraverso altre entità per la concessione di licenze, previo passaggio volontario e attivo per un "opt out" di tali diritti dall'effetto estensivo, diversamente presunto, mediante una notifica alla locale società di gestione collettiva. La combinazione con il principio del paese di origine, secondo cui un servizio *online* originato in uno degli Stati membri necessiterebbe, in mancanza di "opt out" da parte dei titolari dei diritti, di un solo atto di autorizzazione all'utilizzazione *online* dei diritti coinvolti (riproduzione e comunicazione al pubblico), i cui effetti si estenderebbero a tutti gli Stati membri, realizzerebbe un risultato pratico di superamento dei problemi legati alla territorialità del diritto, in quanto in base al criterio del paese di origine si determinerebbe anche il diritto applicabile. Un possibile adattamento del principio del paese di origine alla realtà dei servizi musicali *online* - peraltro già applicato dalla Direttiva 93/83 in materia di diritto d'autore e diritti connessi applicabili alla radiodiffusione via sa-

La disposizione dell'art. 31, completa il quadro della *freedom of contract* assicurata ai titolari dei diritti[79], prevedendo che "se entro il 10 aprile 2017", un organismo di gestione collettiva non concede o offre la concessione delle licenze multiterritoriali per i diritti *online*, e non conclude un accordo di rappresentanza *ex* art. 29, essi possano ritirare da tale organismo i diritti ali fini della concessione di licenze multiterritoriali senza dover ritirare i diritti per la concessione di licenze monoterritoriali. I titolari dei diritti hanno dunque facoltà di concedere licenze transfrontaliere sui diritti per opere musicali *online* "direttamente o tramite qualsiasi terzo da loro autorizzato o qualsiasi altro organismo di

---

tellite e alla ritrasmissione via cavo, individuando il diritto applicabile in quello del paese di emissione (ma si veda, in senso contrario rispetto all'estensione ai diritti d'autore, R. Matulionyté, *Cross Border Collective Management and Principle of Territoriality: Problems and Possible Solutions in the EU*, 11, *World Intell. Prop.*, 2009, pp. 467, 475 ss.), e dalla Direttiva 2010/13 [sost. della Direttiva 2007/65] sui servizi di media audiovisivi, che ravvisa il paese di origine nel luogo di stabilimento del *provider* nel caso dei servizi televisivi *online* interattivi e non interattivi - avrebbe potuto essere quello del luogo in cui è avvenuto l'*upload* del contenuto protetto dal diritto d'autore sul *server* connesso alla rete Internet, o il paese di stabilimento del *service provider* o addirittura di quello della residenza dell'autore nel momento in cui l'opera è stata per la prima volta comunicata al pubblico. Per tali due ultime soluzioni si vedano riferimenti rispettivamente in G. Mazziotti, *New Licensing Models for Online Music Services in the European Union: From Collective to Customized Management*, in *Columbia Journal of Law and the Arts*, 2011, vol. 34 (4), pp. 757 ss. e in J. Ginsburg, *Berne without Borders: Geographic Indiscretion and Digital Communication*, (November 2001) Col. Law School, Pub Law Research Paper No. 01-30, disponibile al sito http://ssrn.com/abstract=29210.

[79] Il diritto di assegnare e di ritirare liberamente i diritti dalla gestione collettiva rappresenta la pietra angolare del sistema nella prospettiva adottata dal legislatore comunitario, come risulta dal quindicesimo e dal diciannovesimo considerando e dall'art. 5. Anche in Italia, l'art. 4, D.Lgs. 35/2017, stabilisce che "(i) titolari dei diritti possono affidare ad un organismo di gestione collettiva o ad un'entità di gestione indipendente di loro scelta la gestione dei loro diritti, delle relative categorie o dei tipi di opere e degli altri materiali protetti per i territori da essi indicati, indipendentemente dallo Stato dell'Unione europea di nazionalità, di residenza o di stabilimento dell'organismo di gestione collettiva, dell'entità di gestione indipendente o del titolare dei diritti, *fatto salvo quanto disposto dall'articolo 180, della legge 22 aprile 1941, n. 633, in riferimento all'attività di intermediazione dei diritti d'autore*" (enfasi aggiunta).

gestione collettiva che si attenga alle disposizioni del presente titolo". In questo caso la società potrà proseguire nella gestione nazionale dei diritti *online* sulle opere musicali, e si realizzerà una segmentazione territoriale della concessione di licenze.

Sempre discorrendo della fisionomia assunta dalla autonomia contrattuale nell'ambito della gestione delle licenze transfrontaliere si può notare che non è previsto, a favore del titolare dei diritti, un obbligo dell'organismo dotato di *passport* paneuropeo di accettare il mandato: certamente una previsione in tal senso potrebbe essere introdotta in fase di attuazione secondo la previsione dell'art. 7, comma 2, che consente agli Stati membri di applicare ai titolari dei diritti "altre disposizioni della presente direttiva" e quindi anche di prevedere, a loro favore, l'obbligo di rappresentanza riconosciuto dall'art. 30 agli organismi di gestione collettiva privi dei requisiti per la concessione transfrontaliera delle licenze[80].

6. Conclusioni

Il sistema di gestione collettiva delineato dall'armonizzazione comunitaria, pur essendo ispirato ad una logica di liberalizzazione, mantiene intatta una significativa componente regolatoria, tanto da consentire che in Italia sia preservato, pure nel quadro dell'attuazione della direttiva europea, il monopolio legale della Società Italiana Autori ed Editori.

Le soluzioni adottate dalla direttiva, in generale, paiono la sintesi del

[80] Ma una simile opzione non sembra aver trovato applicazione nelle principali trasposizioni nazionali della Direttiva: si veda ad esempio *l'Ordonnance n. 2016-1823 du 22 décembre 2016 portant transposition de la directive 2014/26/UE du Parlement européen et du Conseil du 26 février 2014 concernant la gestion collective du droit d'auteur et des droits voisins et l'octroi de licences multiterritoriales de droits sur des œuvres musicales en vue de leur utilisation en ligne dans le marché intérieur*, in *JO*, 23 décembre 2016.

dualismo tra regolazione e concorrenza, che da sempre caratterizza la materia della gestione collettiva dei diritti d'autore.

Da un lato vi sono le ragioni della gestione tradizionale, basata su monopoli territoriali e rappresentanza volontaria, che, a fronte di inefficienze in tema di governo, di trasparenza e di amministrazione dei compensi agli autori, assicuravano un accesso unitario e certo agli utilizzatori dei contenuti ed un efficace controllo delle utilizzazioni illecite delle opere, realizzando gli incentivi per una effettiva cooperazione che la disciplina comunitaria si limita ad auspicare. Dall'altro si segnalano le spinte alla realizzazione di un mercato più contendibile, reso possibile dalla evoluzione tecnologica, stimolato dalle nuove possibilità di sfruttamento e (forse) dalla prospettiva del passaggio ad una gestione disintermediata.

Sullo sfondo, ma non per importanza, i valori fondamentali della cultura europea, declinati nella promozione della creatività, nella protezione della diversità culturale e nella aggregazione associativa in senso forte, anche in contrapposizione all'industria culturale, tratto genetico delle *collecting societies* tradizionali.

La soluzione europea rappresenta dunque un compromesso, o meglio segna il cammino alla transizione verso nuovi modelli di mercato e di gestione, probabilmente consapevole che nella società dell'informazione e della tecnologia l'evoluzione normativa non può che avere anch'essa natura provvisoria ed incedere tipicamente "incrementale".

Marco Capone
Masterlex Palermo

"Nuovi media, vecchi problemi: il giornalismo nell'era dei *social network*"

Abstract: Il giornalismo ai tempi dei *social network* è radicalmente cambiato. Su *Facebook*, infatti, le notizie vengono condivise ad una velocità impressionante: i nostri profili, le nostre bacheche, i gruppi, possono essere fonte di informazione. Per non parlare poi di *Twitter*, che è diventato il principale canale di informazione.

La tecnologia ha rivoluzionato il mondo del giornalismo: certamente, in positivo.

Le fonti si sono moltiplicate, molti cittadini si informano sui *social network*, attraverso i *device* mobili. Il 90% delle notizie sui *social* proviene dai giornali, il restante 10% costituisce un problema perché pone il lettore e anche lo stesso giornalista a rischio bufale. Come fa un giornalista a mettersi in guardia da queste "cantonate"? Il giornalista deve innanzitutto verificare la veridicità della notizia e, quindi, comprendere la fonte. La verifica della notizia è uno dei capisaldi della professione giornalistica e sul *web* questa operazione non sempre è facile. Proprio con il *web*, il compito del giornalista diventa ancora più difficile e la tutela della persona diventa assai più complessa. Pensate alle recenti notizie di video *hard* e foto postate su internet: il *web* è una vera e propria jungla all'interno della quale è veramente difficile muoversi. Tra le recenti creazioni del mondo dell'*online* troviamo anche il triste fenomeno degli *hate speech*. Lo *hate speech* è un tema che alimenta un dibattito molto attuale e ancora più controverso nel caso della libertà di espressione su internet, dove non esistono specifiche normative internazionali condivise.

Journalism in the times of social networks is radically changed. On Facebook, in fact, the news will be shared at an impressive speed: our profiles, our message boards, groups, can be a source of information. To say nothing of Twitter, which has become the main channel of information.

Technology has revolutionized the world of journalism: certainly, positively. The sources have multiplied, many citizens are informed on social networks through mobile devices. 90% of the news in the social network comes from the newspapers, the remaining 10% is a problem because it puts the reader and also the same journalist with the risk of hoaxes.

How does a journalist to put themselves on guard against these "blunders"? The journalist must first verify the veracity of the news, and thus understand the source. The verification of the news is one of the cornerstones of the journalistic profession and on the web this is not always easy. Just with the web, the journalist's task becomes even more difficult and the protection of the person becomes much more complex. Think about the recent reports of hardcore videos and photos posted on the Internet: the web is a real jungle inside which is really hard to move.

Among the recent creations of the online world we are also the sad phenomenon of hate speech. The hate speech is an issue that feeds a very timely debate and even more controversial in the case of freedom of expression on the Internet, where there are no specific shared international standards.

Sommario: 1. Il nuovo giornalismo con MasterLex.it – 2. I *social network*, il giornalismo e l'evoluzione della professione – 3. Il magma digitale e le insidie del *web* – 4. Il rispetto della *privacy* e il diritto di cronaca – 5. *Facebook* e la *privacy*, confini molto labili. Gli *hate speech* – 6. La diffamazione a mezzo *Facebook* – 7. Una riflessione doverosa e un problema ancora in attesa di concrete soluzioni

1. Il nuovo giornalismo con MasterLex.it

MasterLex è un nuovo quotidiano di informazione giuridica, *online* dal 13 settembre. L'idea di dar vita ad un nuovo progetto in realtà è nata lo scorso anno, ma per realizzare il portale e formare la redazione è passato un po' di tempo. Il nostro è un progetto ambizioso, innovativo, certamente non facile: cambiare l'informazione giuridica. Ci siamo resi conto, infatti, di come nel corso del tempo i vari siti che trattavano l'argomento giuridico lo facevano con modalità a nostro avviso obsolete, e soprattutto quasi restringendo l'ambito di pubblico al quale si rivolgevano. Peraltro, utilizzando un linguaggio prettamente elitario, che rendeva difficile la lettura degli articoli ad un qualsiasi soggetto non laureato in giurisprudenza. Ed è così che è nato il progetto MasterLex, un nuovo giornale capace di raccontare il diritto, in tutte le sue molteplici forme, ai cittadini: tutti i cittadini. Chiaramente, *in primis* il pubblico dei professionisti, senza dimenticare però che c'è una vasta gamma di soggetti che magari non riesce sempre a comprendere concretamente la materia giuridica. È così sul nostro portale sono nati i *focus*, gli approfondimenti, le inchieste, le rubriche. Spazi appositi dedicati al mondo del condominio, dei consumatori, dei disabili e così via. Un'informazione totale che ha come perno centrale il mondo del diritto. E la nostra filosofia, cioè il diritto alla portata di tutti, in un certo senso è stata condivisa e portata avanti anche dal palco del XXXIII Congresso Nazionale Forense, svoltosi a Rimini il 6-7-8 ottobre. Gli avvocati che prendevano la parola durante gli interventi sostenevano come la professione dell'avvocato sia una professione di servizio ai cittadini e gli stessi non possono non interessarsi alle novità presenti nel settore. Certo, un conto è raccontare i cambiamenti seguendo un linguaggio tecnico, un conto è farlo diversamente. E così abbiamo colto la sfida, e abbiamo deciso di effettuare delle selezioni interattive, sul *web*. Abbiamo voluto evitare ai potenziali candidati lunghe e costose trasferte, abbiamo deciso di farli restare comodamente seduti da casa e rispondere al nostro test. Su

telegram, quindi, circa 400 candidati hanno redatto un articolo di giornale e fornito titoli per farci comprendere, realmente, le capacità di scrittura. Un metodo innovativo che si è coniugato perfettamente con la nostra filosofia di lavoro. E infatti, viviamo in un'era che ha profondamente rivoluzionato il mondo dell'informazione. I nuovi media, infatti, sono profondamente influenzati dalle avanguardie della tecnologia.

2. I *social network*, il giornalismo e l'evoluzione della professione

Il giornalismo ai tempi dei *social network* è radicalmente cambiato. Su *Facebook*, infatti, le notizie vengono condivise ad una velocità impressionante: i nostri profili, le nostre bacheche, i gruppi, possono essere fonte di informazione. Per non parlare poi di *Twitter*, che è diventato il principale canale di informazione. Per farvi un esempio, negli Stati Uniti molte società sportive twittano ancor prima di diramare i comunicati ufficiali alla stampa. Oppure è realmente accaduto che alcune band musicali annunciassero il loro scioglimento o una loro tournée in 140 caratteri e poi dessero la notizia sul sito ufficiale. Un sistema rapido e immediato che consente di essere informati molto facilmente. Peraltro adesso ci sono state delle modifiche ai 140 caratteri e si è cercato di togliere dal conteggio i *file* multimediali per lasciare più spazio al testo. Prima di analizzare come i *social network* abbiano influenzato il sistema occorre però capire come la tecnologia ha cambiato il settore dei media.

La tecnologia ha rivoluzionato il mondo del giornalismo. Certamente, in positivo. Pensiamo al rapporto lettore-giornalista: un tempo si scriveva una lettera indirizzata al giornale, si attendeva che il postino consegnasse la lettera al giornale e il redattore la trovava sulla propria scrivania. Passavano, però, almeno 6-7 giorni prima che il messaggio del lettore giungesse al giornalista. Oggi con i *social network* la situazione è assolutamente cambiata. Ma questi sono esempi, se vogliamo, banali. Pensate agli inviati in guerra, coloro che seguono gli sviluppi per esempio in Si-

ria. In passato i corrispondenti dovevano recarsi all'ambasciata e adempiere una serie di obblighi abbastanza noiosi e lunghi. Ora, con i computer, il tutto è immediato. La tecnologia ci mette a disposizione una serie di strumenti che hanno radicalmente cambiato il modo di fare notizia. Anche la formazione del giornalista è cambiata, la professione veniva trasmessa spesso di generazione in generazione. I taccuini, gli appunti, sono ormai solo un ricordo. I tempi sono profondamente nuovi: il nuovo avanza continuamente e la tecnologia è la novità costante e crescente che anima la professione e i suoi cambiamenti. Ormai andiamo verso una produzione multipiattaforma, non esiste più solo il cartaceo. Per renderci conto di questi cambiamenti dobbiamo necessariamente analizzare un aspetto, che è quello connesso alla crisi della carta stampata.

Vero è che c'è una crisi della carta stampata ma inevitabile è il fattore connesso alle diverse modalità di reperire informazioni. Le fonti si sono moltiplicate, molti cittadini si informano sui *social network*, attraverso i *device* mobili. Il 90% delle notizie sui social proviene dai giornali, il restante 10% costituisce un problema perché pone il lettore e anche lo stesso giornalista a rischio bufale. Anche su *Twitter*, per esempio, la bufala è dietro l'angolo visto che spesso i *followers* prendono qualche cantonata dai profili falsi. Il modo di condividere la notizia è cambiato, anche la figura dell'addetto stampa ha subito questa evoluzione. Come fa un giornalista a mettersi in guardia da queste "cantonate"? Il giornalista deve innanzitutto verificare la veridicità della notizia e, quindi, comprendere la fonte. La verifica della notizia è uno dei capisaldi della professione giornalistica e sul *web* questa operazione non sempre è facile. Mentre in passato era spesso il giornalista a dover reperire la notizia, oggi sono le notizie ad arrivare al giornalista. E questo perché il *web* porta le notizie. Ma, come detto, è un flusso incontrollato e incontrollabile. Adesso, il giornalista ha l'importante compito di filtrare le notizie, selezionarle e verificarle.

La professione è, quindi, cambiata. Bisogna misurarsi con le nuove fonti dell'informazione. Non esiste un mezzo comparabile al digitale, e questo è assolutamente oggettivo. Il digitale, per sua natura, è molto più competi-

tivo rispetto al cartaceo. Premendo un tasto otteniamo l'informazione in tempo reale, con foto, commenti, video, tutto.

Ma chiaramente l'informazione non è gratis, questo è un messaggio che deve assolutamente passare. È soltanto cambiato il modo di condividere la notizia, ma l'indipendenza dei giornali è garantita dal fatto che la gratuità delle notizie non sia assoluta. La pubblicità, infatti, non basta a coprire le spese di una grande redazione. Il cartaceo offre una linea editoriale molto sofisticata, e contenuti che per loro natura devono essere pagati. I giovani leggono sui cellulari, sugli ipad, al pc. Non è che non si informano, anzi, condividono spesso le notizie che apprendono. Il pubblico del digitale è destinato ad aumentare.

3. Il magma digitale e le insidie del *web*

Ma le notizie sul *web* vanno "controllate": esiste un magma digitale, ma non tutte le notizie che passano sul *web* sono degne di nota. Un giornale *online* seleziona le notizie più importanti e le pubblica; il cartaceo invece da questo punto di vista è, ovviamente, limitato. La capacità di aggiornare un portale *web*, in tempo reale, offre la possibilità di decidere immediatamente la gerarchia delle notizie. La bravura del giornalista sta nel "pesare" le notizie, decidendo quali sono più importanti e attraenti e quali no. Una scala di valori è assolutamente fondamentale, ogni sito internet presenta dei parametri nello stabilire un palinsesto.

Sul *web* cambia anche la velocità con cui si scrive: è chiaro che i tempi di lavoro del giornalista *online* sono diversi da quelli di un collega che lavora per la carta stampata. Le regole che sovrintendono un portale *web* sono le medesime di quelle che sorreggono una redazione di un giornale cartaceo ma diverso è il modo di proporre le notizie.

Quali sono le insidie che il *web* può proporre, oltre il pericolo bufale? Il problema principale, a fronte di una notizia immediata che rischia di poter diventare virale è quello legato alla *privacy*. Il rispetto della *privacy* e il diritto di cronaca: come contemperare i due aspetti?

4. Il rispetto della *privacy* e il diritto di cronaca

La *privacy* è stata introdotta in Italia con legge 675/1996, emanata nel nostro ordinamento per adeguarsi ad una direttiva europea, la 46 del 24 ottobre 1995, che aveva imposto agli Stati membri di darsi delle norme per disciplinare la circolazione dei dati personali e sensibili. Un *diktat* proveniente dall'ordinamento dell'UE per tutti gli Stati membri. Questa legge distingue dati personali e dati sensibili: i primi quelli che compaiono nei nostri documenti di identità e che quindi consentono l'identificazione del soggetto; i dati sensibili sono, invece, dati più intimi, che consentono di tracciare un profilo più specifico e particolareggiato di un soggetto (condizioni di salute, credo religioso, orientamento politico ecc). Questa distinzione, per i giornalisti, assume una rilevanza decisiva. Come lavorare nel trattamento dei dati personali? La Corte di cassazione si è più volte pronunciata sulla questione, fornendo dei parametri, se così possiamo dire, al giornalista.

Il diritto di cronaca è costituzionalmente garantito, trovando esplicazione nell'articolo 21 Cost. nella libertà di manifestazione del pensiero, che infatti ricomprende ogni prodotto dell'intelletto e ogni estrinsecazione di opinione.

L'articolo 21, dunque, come diritto ad informare e diritto ad essere informati. I limiti c.d. interni del diritto in questione sono: interesse sociale del contenuto, verosimiglianza alla realtà, riproduzione autentica e trasparente della notizia.

È necessario, quindi, che la notizia sia conforme al criterio della "continenza", ossia correlazione e proporzione tra il fatto, che sta a fondamento del giudizio critico, e il contenuto della critica stessa. Limite esterno al diritto di cronaca è quello del rispetto della *privacy* del soggetto coinvolto nella notizia.

Si evidenzia così il conflitto tra interessi di pari rango. Infatti il diritto alla riservatezza si annovera tra i diritti della personalità, che secondo alcuni trovano piena copertura costituzionale, secondo altri

rinvengono nella Costituzione il loro referente ordinario, dovendo rinviare tuttavia alle altre fonti di diritto per la loro puntuale definizione. In realtà la tutela della vita privata del soggetto deve essere garantita in quanto espressione necessaria della rilevanza costituzionale che la persona ha acquisito nel sistema costituzionale, in forza dell'articolo 2 Cost., dando garanzia ad ogni proiezione della persona nella realtà sociale ed ogni esplicazione della sua personalità.

Se quindi il diritto alla riservatezza non può essere catalogato tra i diritti espressamente coperti da garanzia costituzionale, tuttavia non sembra potersi contestare la riconducibilità di tale diritto ai principi espressi dagli articoli 2 e 3 della Costituzione.

Ergo la tutela della *privacy* deriva dalla tutela della persona, fulcro dell'intero *corpus* normativo, ed ancor più della Carta costituzionale.

Recentemente, purtroppo, non sempre queste regole vengono seguite. Peraltro, proprio con il *web*, il compito del giornalista diventa ancora più difficile e la tutela della persona diventa assai più complessa. Pensate alle recenti notizie di video *hard* e foto postate su internet: il *web* è una vera e propria jungla all'interno della quale è veramente difficile muoversi. Per muoversi è necessario predisporre delle importanti tutele e dei meccanismi che possano concretamente evitare problemi di qualsiasi tipo.

5. *Facebook* e la *privacy*, confini molto labili. Gli *hate speech*

E arriviamo, in questo senso, ai *social network*. Come *Facebook* può diventare strumento pericoloso? Beh è molto semplice. Postare o condividere qualcosa di riservato è facilissimo, immediato appunto, tutto ciò senza che il consenso dell'interessato sia realmente prestato. Infatti dall'America gli sviluppatori di *Facebook* stanno cercando di predisporre nuovi algoritmi di protezione dei dati personali. A ciò si aggiunga anche che recentemente *Facebook* ha acquistato il servizio di messaggistica istantanea, *whatsapp*, con tutta una serie di problemi

connessi alla *privacy* di cui certamente avrete sentito parlare. Alcuni dati statistici che devono certamente farci riflettere: *Facebook* ha abbondantemente superato un miliardo di utenti registrati: i quali, tutti insieme, pubblicano circa due miliardi e mezzo di messaggi al giorno. Su *Twitter* gli utenti attivi sono circa 200 milioni e la media di *tweet* in un giorno è di 400 milioni. Su *YouTube* vengono caricati filmati a una media di 48 ore di nuovi contenuti ogni minuto. Per i *social network* e i grandi gruppi del *web* è evidentemente impossibile valutare ogni singolo contenuto caricato dagli utenti, ed è anche tecnicamente difficile sviluppare sistemi automatici efficienti di blocco preventivo dei contenuti offensivi o violenti.

Jeffrey Rosen – un giurista statunitense molto popolare e molto attento alle cose di internet – fu invitato l'anno scorso a un convegno organizzato dalla Facoltà di Legge di Stanford sulla libertà di espressione in rete, a cui parteciparono anche i giovani rappresentanti di grande aziende del *web* come *Google* e *Facebook*. Rosen **ha ora raccontato** del loro contributo alla discussione e di come si regolano con i contenuti offensivi o pericolosi, e con le espressioni che nella tradizione anglosassone rientrano o potrebbero rientrare nella categoria dello *hate speech*.

Cos'è lo *hate speech*

Lo *hate speech* – espressione spesso tradotta in italiano con la formula "incitamento all'odio" – è una categoria elaborata negli anni dalla giurisprudenza americana per indicare un genere di parole e discorsi che non hanno altra funzione a parte quella di esprimere odio e intolleranza verso una persona o un gruppo, e che rischiano di provocare reazioni violente contro quel gruppo o da parte di quel gruppo. Nel linguaggio ordinario indica più ampiamente un genere di offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale) ai danni di un gruppo. La condanna dello *hate speech* – sia sul piano giuridico che nelle

conversazioni al bar – sta in un equilibrio elastico ma spesso problematico con la libertà di parola, principio tutelato dal Primo emendamento della Costituzione degli Stati Uniti (e fondante, con le sue regole, di ogni democrazia).

Come la risolvono i *social network*

Lo *hate speech* è un tema che alimenta un dibattito molto attuale e ancora più controverso nel caso della libertà di espressione su internet, dove non esistono specifiche normative internazionali condivise. Le grandi aziende come *Google* e *Facebook* affidano la compilazione delle norme di utilizzo dei servizi a un gruppo di lavoro specifico, che chiamano scherzosamente i *Deciders*, "quelli che decidono" (dal nomignolo dato al direttore del settore legale di *Twitter*, Nicole Wong, quando lavorava per *Google*).

YouTube (che fu acquistata da *Google* nel 2006) **vieta** esplicitamente lo *hate speech*, inteso secondo la definizione generale di linguaggio offensivo di tipo discriminatorio. *Facebook* allarga un po' le maglie: lo vieta ma **aggiunge** che sono ammessi messaggi con «chiari fini umoristici o satirici», che in altri casi potrebbero rappresentare una minaccia e che molti potrebbero comunque ritenere «di cattivo gusto». *Twitter* è il più "aperto": non vieta esplicitamente lo *hate speech* e neppure lo cita, eccetto che in una **nota** sugli annunci pubblicitari (in cui peraltro specifica che le campagne politiche contro un candidato «generalmente non sono considerate *hate speech*»).

Alcuni studenti di cartografia della *Humboldt State University* in California hanno elaborato una "mappa dello *hate speech*" su *Twitter* selezionando manualmente i contenuti inequivocabilmente offensivi da un campione di 150 mila *tweet* contenenti parole dispregiative come *nigger* ("negro"), *cripple* ("storpio") *owetback* ("clandestino"). Il campo di ricerca è limitato al territorio degli Stati Uniti e al periodo da giugno 2012 ad aprile 2013, e il risultato – per quanto parziale – può avere chiavi di lettura significative per quel paese. Ma la definizione di *hate speech* non è

univoca in tutto il mondo (a volte non lo è neanche negli Stati Uniti) e solleva un problema più articolato se si considera che la maggior parte degli utilizzatori di *social network* e portali *web* non sono americani.

Le tecniche e le regole usate da *Facebook*

Il capo dei *Deciders* di *Facebook* si chiama Dave Wilner: ha ventotto anni, ha scritto lui le norme d'uso del servizio ed è sposato con una collega del *team* Sicurezza dell'utente, che si occupa di protezione dei bambini e prevenzione dei suicidi (chissà che conversazioni a cena, si chiede Rosen). Il genere di domanda a cui Wilner e il suo *team* devono cercare di dare risposta ogni giorno è questo: «questa persona in foto è nuda? questa foto di Hitler è razzismo o commento politico? postare una foto di qualcuno alterata tramite *Photoshop* è bullismo? postare la foto di una pistola è una minaccia credibile? e se la pistola è quella della copertina di un album rap?».

Le difficoltà teoriche ma anche tecniche legate alla valutazione dei contenuti offensivi o critici – quelli che potrebbero provocare incidenti o reazioni violente – hanno spinto aziende come *Facebook* e *YouTube* ad affidare una parte importante del lavoro alla comunità di utenti, tramite il sistema delle segnalazioni. Questo serve a elaborare un algoritmo sviluppato in parte tramite l'apprendimento meccanico di questi dati e in parte tramite il lavoro umano di supervisione da parte dei *Deciders*, che aggiustano il tiro laddove ritengano che una segnalazione sia ingiustificata o condizionata da fattori non rilevanti secondo le norme di utilizzo. Primo emendamento e Libertà di parola sono due concetti rilevantissimi nelle valutazioni finali.

Il Primo emendamento e internet

Il Primo emendamento della Costituzione degli Stati Uniti – che garantisce e tutela la libertà di culto, di parola e di stampa, e a cui diversi commentatori di lingua inglese si appellano spesso in difesa della libertà di espressione in rete – è un argomento molto presente

nella giurisprudenza statunitense, e anche oggetto di lunghe controversie. La libertà di espressione è considerata un diritto fondamentale e generalmente non ammette l'interferenza dello Stato: in una **sentenza** del 1988 molto citata (*Boos* contro *Barry*) i giudici ribadivano che «nel dibattito pubblico i cittadini dovrebbero tollerare le parole offensive, e perfino quelle oltraggiose, per fornire spazio sufficiente alle libertà protette dal Primo emendamento».

Ma la libertà di espressione non è un diritto assoluto – conosce ovvie e meno ovvie regolazioni – e non tutte le espressioni individuali sono considerate materia da Primo emendamento: quelle che non riguardano temi di interesse pubblico e da cui la società non potrebbe trarre beneficio non hanno alcuna tutela costituzionale (*unprotected speech*). Viene spesso citato un caso del 1942: un tale Chaplinsky diede in pubblico del "maledetto fascista e delinquente" a un agente dello Stato del *New Hampshire*, la Corte lo condannò – non per il bersaglio dell'offesa ma per l'offesa in sé – e lui si appellò inutilmente al Primo emendamento.

6. La diffamazione a mezzo *Facebook*

Un ultimo passaggio, infine, non può non essere dedicato alla possibilità di diffamare qualcuno a mezzo *Facebook*. Fino a qualche anno fa sembrava quasi impensabile una ipotesi del genere. Invece, oggi, tutto ciò è possibile. Diffamare un soggetto attraverso l'utilizzo dei *social network*. Postare un commento offensivo sulla bacheca di *Facebook* della persona offesa integra il reato di diffamazione a mezzo stampa. La Corte di cassazione, già lo scorso anno con la sentenza 24431/2015, ha stabilito che inserire un commento su una bacheca di un *social network* significa dare al suddetto messaggio una diffusione che potenzialmente ha la capacità di raggiungere un numero indeterminato di persone, sicché, laddove questo sia offensivo, deve ritenersi integrata la fattispecie aggravata del reato di diffamazione.

La Corte di cassazione si confronta con l'utilizzo illecito e smodato dei cosiddetti *social network*, e sottolinea la diffusività delle affermazioni che compaiono su tali siti. Proprio in ragione del fatto che i commenti che compaiono su tali *social network* hanno una diffusione capillare e potenzialmente illimitata, i Giudici di ultima istanza ritengono che le offese espresse in tal modo debbano ritenersi aggravate, come se commesse a mezzo stampa. Anche quest'anno la Corte ha affrontato ancora il problema, ritenendo possibile su *Facebook* anche la diffamazione aggravata. Tutto ciò si inserisce, inevitabilmente, nel circuito pocanzi descritto e inevitabilmente si raccorda a quel magma incontrollabile che il *web* ha generato.

7. Una riflessione doverosa e un problema ancora in attesa di concrete soluzioni

Chiaramente, le questioni sono ancora aperte e certamente in questo mio breve intervento non troveremo soluzioni ma spunti. Ciò su cui occorre riflettere, a mio avviso, è che i *social network* vanno utilizzati con grande cura e soprattutto i giornalisti devono fare molta attenzione a quelle che sono le notizie che reperiscono sui *social* e che poi, successivamente, vanno a postare in questa mostruosa piattaforma.

Prezzo e codice a barre

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

Il convegno del 26 ottobre 2016 si inserisce nel Progetto Nazionale dei CDE Italiani dal titolo "Un Mercato Unico Digitale per l'Europa", promosso dalla Rappresentanza in Italia della Commissione Europea.

Hanno patronicato al convegno

macerata
comune di macerata

Camera di Commercio
Macerata

Ordine degli Avvocati di Macerata

In collaborazione con

IAIC
ITALIAN ACADEMY OF
THE INTERNET CODE

CREDA
Centro di Ricerca
di Eccellenza per
il Diritto d'Autore

scuola di dottorato
SDA
UNIVERSITÀ DI MACERATA