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

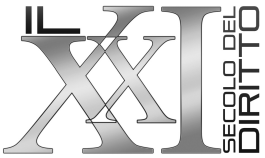
IL MERCATO UNICO DIGITALE

A CURA DI GIANLUCA CONTALDI

UNIVERSITÀ DI MACERATA — 26 OTTOBRE 2016

ATTI DEL CONVEGNO

NUOVA EDITORIALE UNIVERSITARIA



Via Colonnello Tommaso Masala, 42 - 00148 Roma
e-mail: nuovaeditriceunivers@libero.it
web: www.nuovaeditriceuniversitaria.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.
È recente l'intervento del Garante della Privacy che ha segnalato la ne-

[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.

cessità 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, si collocano gli *smart contracts* o contratti intelligenti, ossia quei contratti

[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.

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 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

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

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.) 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

[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.

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.

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

[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). È previsto inoltre il divieto per i fornitori di rete broadband di interferire con il libero accesso ad internet degli utenti.

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,

[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,

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.

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

---

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).

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 générele 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, pp. 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, pp. 40 ss.; in proposito, tra gli altri, A. Dickinson, *The Rome II Regulation. The Law Applicable to Non-Contractual Obligations*, Oxford, 2008, pp. 295 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali nel diritto internazionale privato*, Milano, 2013, pp. 108 ss..

[4] La letteratura in materia è molto vasta. Ci si permette di rinviare a F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 15 ss., spec. pp. 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, pp. 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, pp. 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, pp. 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, pp. 255 ss., spec. pp. 257 ss.; L. Mari, *Il diritto processuale civile della convenzione di Bruxelles*, I, *Il sistema della competenza*, Padova, 1999, pp. 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, pp. 345 ss., spec. pp. 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, pp. 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, pp. 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, pp. I-6009 ss., punti 18 ss. della motivazione.
[10] Si vedano in proposito A. Davì, *La responsabilità extracontrattuale*, cit., pp. 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, pp. 484 ss.; M. Lehmann, *Where Does Economic Loss Occur?*, in *Journal of Private International Law*, 2011, pp. 527 ss., spec. pp. 538 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 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, pp. I-415 ss.. Si vedano in proposito, tra gli altri, A. Davì, *La responsabilità extracontrattuale*, cit., p. 31 e pp. 111 ss.; L. Mari, *Il diritto processuale civile*, cit., pp. 378 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 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"), pp. 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, pp. 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, pp. 201 ss.; S. Marino, *La violazione dei diritti della personalità nella cooperazione giudiziaria civile europea*, in *Rivista di diritto internazionale privato e processuale*, 2012, pp. 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, pp. 271 ss., spec. pp. 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, pp. I-3961 ss., par. 33.
[24] Si rimanda a quanto osservato in proposito in F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 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., pp. 348 ss. e, con riferimento al caso in esame, in ID., *Le obbligazioni non contrattuali*, cit., pp. 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, pp. 9 ss., spec. pp. 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, pp. 183 ss., spec. pp. 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, pp. 5 ss.; R. Geimer, *Verfassung, Völkerrecht und internationales Zivilverfahrensrecht*, in *Zeitschrift für Rechtsvergleichung*, 1992, pp. 321 ss. e 401 ss.; Th. Pfeiffer, *Internationale Zuständigkeit und prozessuale Gerechtigkeit*, Frankfurt am Main, 1995, pp. 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, pp. 441 ss.; J. Bertele, *Souveränität und Verfahrensrecht. Eine Untersuchung der aus dem Völkerrecht ableitbaren Grenzen staatlicher extraterritorialer Jurisdiktion im Verfahrensrecht*, Tübingen, 1998, pp. 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, pp. 501 ss., nota di H. Muir-Watt, ivi, pp. 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., pp. 202 ss.; S. Marino, *La violazione dei diritti della personalità*, cit., pp. 366 ss.; nonché quanto osservato in F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 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., pp. 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, pp. 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, pp. 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 e 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, pp. 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, pp. 879 ss., spec. pp. 884 ss.; F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 28 ss.; in senso positivo, valutando con favore in un'ottica di prevedibilità della competenza giurisdizionale la soluzione accolta dalla Corte di giusti-

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-

---

zia, M. Köhler, *Der fliegende Gerichtsstand. Die Bestimmung des zuständingen Gerichts bei ubiquitäre Rechtsverletzungen*, in *WRP – Wettbewerb im Recht und Praxis*, 2013, pp. 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., pp. 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., pp. 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, pp. 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, pp. 472 ss., con nota di E. Treppoz, ivi, pp. 479 ss.; si veda anche F. Marongiu Buonaiuti, *Le obbligazioni non contrattuali*, cit., pp. 39 ss..

[59] Accordo su un Tribunale unificato dei brevetti, in *GUUE*, C 175 del 20 giugno 2013, pp. 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, pp. 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, pp. 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., pp. 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, pp. 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, pp. 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, pp. 81 ss., spec. pp. 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 da-*

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

---

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

[64] Si veda in proposito Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., pp. 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., pp. 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, pp. 377 ss., con nota di B. Haftel, ivi, pp. 378 ss.; si veda anche Ch. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation*, cit., pp. 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 ss.. 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., pp. 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., pp. 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., pp. 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., pp. 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., pp. 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, pp. 560 ss..