

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

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

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

Il tema della raccolta, utilizzo e trasferimento dei dati personali costituisce una argomento particolarmente delicato e complesso per il diritto, sia interno che sovranazionale, soprattutto in rapporto al necessario equilibrio con la protezione dei diritti di libertà che il loro utilizzo impone¹.

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

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

Se quindi dal punto di vista economico, la diffusione pervasiva e globale dell'interazione digitale ha il merito di generare nuovi e forse inaspettati profitti, è innegabile che, dal punto di vista giuridico, tali scambi di informazioni tra imprese, anche appartenenti al medesimo gruppo aziendale ma a diversi ordinamenti giuridici, pongono crescenti questioni, soprattutto in considerazione della tutela di quei valori e diritti che, seppur sempre più comuni (si pensi alla salvaguardia dei diritti e delle libertà fondamentali), continuano a ricevere differenti livelli di protezione nei diversi ordinamenti giuridici nazionali³.

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

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

³ Su questi temi si veda, fra gli altri, O. Bassini, M. Pollicino, *Reconciling right to be forgotten and freedom of information in the digital age: past and future of personal data protection in the EU*, in *Diritto pubblico comparato europeo*, 2014, pp. 640 ss.; C. Gayrel, J. Herveg, J-M. Van Gyseghem, *La protection des données à caractère personnel en droit européen*, in *Journal européen des droits de l'homme*,

D'altra parte, è necessario poi considerare che la velocità e la quantità di dati disponibile nelle comunicazioni digitali ha certamente accentuato e favorito le attività di controllo e sorveglianza sugli individui degli Stati che, soprattutto sotto la minaccia del terrorismo internazionale, hanno talvolta travalicato e violato gli stessi limiti delle libertà personali⁴. A tal proposito, ad esempio, è innegabile che la vicenda “PRISM” – legata al programma statunitense di sorveglianza delle comunicazioni rivelato nel giugno 2013 da Edward Snowden – oltre ad aver evidenziato i contrasti tra Unione europea e Stati Uniti in materia di protezione e trasferimento dei dati personali, ha finito per riaccendere l'allarme “sorveglianza globale” di orwelliana memoria⁵.

n° 16/1, 2016, pp. 98 ss.; E. De Busser, *Private Companies and the Transfer of Data to Law Enforcement Authorities: Challenges for Data Protection*, in *Maas-tricht Journal of European and Comparative Law*, vol. 23, n. 3, 2016, pp. 478 ss..

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

⁵ Le rivelazioni di Edward Snowden, pubblicate per la prima volta il 5 giugno 2013 da parte del giornale britannico *The Guardian* hanno dato origine allo scandalo “Datagate”, nel corso del quale è venuta alla luce la raccolta di metadati da parte dell'Agenzia per la sicurezza nazionale statunitense sulle telefonate dei clienti dell'operatore *Verizon*. A ciò ha seguito tutta una serie di rivelazioni circa un vero e proprio sistema di controllo e monitoraggio gestito dalla medesima agenzia go-

Proprio tali circostanze, da un lato di natura privatistica, con riferimento alle attività delle imprese piattaforma, e dall'altra pubblicista, con riferimento ai programmi di sorveglianza e intelligence statale, hanno fatto da teatro per la nota vicenda Schrems⁶, che in Europa ha contribuito a rianimare l'annoso dibattito sul trasferimento dei dati personali verso i Paesi extra-europei. Ciò ha, dunaque, accelerato la necessaria riformulazione della disciplina europea a protezione dei dati personali, nonché la "demolizione" del c.d. "Safe Harbour" e l'adozione di

vernativa, in collaborazione con le più importanti compagnie telefoniche e operatori Internet. Si veda sul A. Di Corinto, L. Reitano, *Digito ergo spio, le armi del mestiere*, in *Limes*, luglio 2014; F. Pizzetti, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it*, n. 13, 2013.

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

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

Il 2016, dunque, ha segnato in Europa l'entrata in vigore di un pacchetto di norme in materia: il regolamento n. 679⁸, che il 6 maggio 2018 andrà a sostituire la direttiva n. 46 del 1995⁹, la direttiva n. 680¹⁰, che sostituirà il 25 maggio dello stesso anno la decisione quadro GAI n. 977 del 2008¹¹, e la direttiva n. 681 (c.d. direttiva PNR)¹², primo intervento in materia del legislatore europeo che dovrà essere recepita entro il maggio 2018.

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

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

⁸ Cfr. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GU L 119 del 4 maggio 2016, pp. 60-65.

⁹ Cfr. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GU L 281 del 23 novembre 1995, p. 31-39.

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

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

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

sonali dei cittadini europei continuano a beneficiare di un elevato standard di protezione, anche nell'ipotesi in tali dati siano trasferiti al di fuori del territorio degli Stati membri, in un'ottica di applicazione extraterritoriale della normativa europea¹³.

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

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

È innegabile, infatti, che al di là delle enunciazioni di principio, l'attenzione del legislatore europeo si sia piuttosto concentrata sull'esigenza di evitare che il trasferimento di dati tra Stati sia intralciato dall'esistenza di difformità normative ed incertezze giuridiche, piuttosto che garantire un effettiva e concreta protezione dei diritti di libertà (e quindi a volte il divieto di trasferimento). Ciò in una duplice prospettiva: a livello interno, al fine di assicurare la libera circolazione dei dati per un migliore funzionamento del mercato comune europeo¹⁴, mentre all'esterno, al fine di rafforzare i rapporti commerciali con i Paesi terzi. È indubbio, dunque, che la possibilità concreta di impedire il flusso frontaliero dei dati viene di fatto esclusa nell'applicazione della normativa europea, soprattutto se si vuole evitare l'isolamento commerciale

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

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

dell'Europa¹⁵. Tale atteggiamento, definito da taluni “progressista”¹⁶, forse in maniera troppo ottimistica, appare inoltre confermato dal considerando n. 101 del regolamento, secondo il quale i flussi dei dati verso e da Paesi al di fuori dell'Unione sono “necessari” per l'espansione del commercio internazionale e della cooperazione internazionale.

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

In particolare, ciò che appare particolarmente rischioso in tema di garanzia dei diritti di libertà è proprio l'obiettivo “di appianare le divergenze” tra ordinamenti, piuttosto che ostacolare o controllare il flusso di dati transfrontalieri. Ciò soprattutto ove si consideri la nozione ormai pacifica e restrittiva di trasferimento¹⁷, secondo la quale non costituisce trasferimento l'inserimento di dati personali da parte di un soggetto stabilito nell'Unione, in una pagina internet, caricata presso un *web hosting provider* stabilito nell'Unione, anche quando i dati così inseriti divengano accessibili da Paesi terzi, nonché le criticità nell'applicazione un po' troppo indulgente delle decisioni di adeguatezza e le altre deroghe espresse al divieto di trasferimento, presenti nel regolamento: dalle clausole contrattuali standard alle norme vincolanti d'impresa.

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

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

¹⁶ D. Pittella, *Trasferimento verso Paesi terzi*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Cedam, 2016.

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

A completamento di questa prima disamina sul trasferimento dei dati personali verso Paesi extraeuropei e a conferma del quadro piuttosto critico sin qui offerto, è infine utile ricordare che simili e congenite compressioni dei diritti di libertà sono altresì previste nella Direttiva PNR, giacché la stessa finisce in definitiva per autorizzare una raccolta indiscriminata e generalizzata di dati personali, trasferiti anche verso Stati extra-europei, permettendo una notevole ingerenza nella privacy di qualsiasi individuo¹⁸.

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

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

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

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

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

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

Tuttavia, anche se la decisione di adeguatezza, nell'attuale riforma, viene meglio delineata, resta il problema del fondamento stesso di tale strumento. Il requisito dell'adeguatezza, infatti, nella volontà del legislatore europeo, non implica un raffronto tra sistemi di protezione dei diritti di ordinamenti diversi, ma si ferma piuttosto alla cosiddetta "equivalenza" che, sempre in quest'ottica piuttosto ottimista, consentirebbe agli Stati di utilizzare diverse vie per garantire l'effettiva protezione dei dati personali. In altri termini, la prova diabolica che si chiede alla Commissione è quella di operare una valutazione *ex ante* dell'ordinamento del Paese terzo (*rectius* dell'effettività *ex ante* dell'ordinamento dello Stato terzo in materia di tutela dei diritti), nonché la facoltà di operare un successivo controllo e un eventuale riesame periodico del provvedimento adottato²⁰.

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

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

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

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

Quest'ultime possono essere distinte in due categorie, a seconda che sia necessaria o meno un'autorità di controllo. Nel primo caso, il trasferimento avviene senza specifica autorizzazione a condizione che lo Stato terzo (o l'organizzazione) offra garanzie adeguate che possono consistere in: i) uno strumento vincolante che sia stato approvato dall'autorità nazionale di controllo, ii) norme vincolanti d'impresa, iii) clausole standard di protezione dei dati, adottate dalla Commissione o iv) da un'autorità di controllo nazionale e approvate dalla Commissione, v) codice di condotta con l'impegno vincolante del destinatario dei dati ad applicare le garanzie adeguate, vi) il c.d. sigillo europeo di protezione dei dati, un contrassegno concesso a soggetti appartenenti a stati terzi da parte di organismi di certificazione a livello nazionale ai sensi dell'art. 43 del regolamento²¹. Nel secondo caso, costituiranno garanzie

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

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

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

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

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

Ad oggi il numero degli Stati per i quali la Commissione ha adottato le decisioni di adeguatezza alla luce della vecchia normativa è esiguo²². Inoltre, gli strumenti adottati sono destinati a rimanere in vigore sino

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

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

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

Per quanto attiene al primo profilo, si tratta generalmente di una serie di atti unilaterali adottati dalla Commissione e (talvolta) dalla Commissione e dagli Stati terzi, diretti a regolare il traffico transfrontaliero di dati. Con riferimento a quest'ultima ipotesi, tuttavia, è evidente, che tali atti, anche quando sottintendono obbligazioni sinallagmatiche tra Unione e Stati terzi, non possano in ogni caso essere considerati alla stregua di accordi in forma semplificata. Infatti, né l'Unione né gli Stati terzi, in alcuno degli atti menzionati, hanno mai espresso la volontà di concludere un accordo internazionale²³, né è utilizzata la procedura di cui all'art. 218 TFUE, che prevede peraltro la previa approvazione del Parlamento europeo²⁴. Essi rimangono, dunque, in entrambi i casi atti secondari dell'Unione vincolanti per gli Stati membri (o persone fisiche e giuridiche degli Stati membri)²⁵, con una (ovvia) scarsa incidenza all'esterno, verso i Paesi terzi.

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

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

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

Per quanto attiene al secondo profilo, cioè quello dei contenuti, tra le decisioni di adeguatezza, la più nota è quella n. 520 del 26 luglio 2000, fondata sui *Safe Harbour Principles*, che ha consentito il trasferimento dei dati tra Unione europea e Stati Uniti, fino alla sentenza “Schrems” della Corte di giustizia del 2015, decisione poi sostituita nel 2016 dal EU-US Privacy Shield²⁶.

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

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

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

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

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

La Corte ha rilevato, dunque, che la previsione – contenuta nel Safe Harbour – di una semplice adesione volontaristica a principi relativi alla protezione dei dati da parte di soggetti con sede negli Stati Uniti ha reso non solo possibile la compressione di diritti fondamentali da parte delle autorità pubbliche americane, come di fatto è accaduto, ma ha mancato anche di prevedere effettive tutele giurisdizionali che potessero evitare tali interferenze²⁷.

Nella ricostruzione della Corte, è ben chiaro, tuttavia, che la protezione del diritto fondamentale al rispetto della vita privata impone che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario²⁸. Nel caso specifico, tali deroghe non erano certamente strettamente necessarie dal momento che consentivano alle autorità pubbliche statunitensi di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche, in contrasto con il contenuto essenziale del diritto fondamentale al rispetto della vita privata, garantito dall’articolo 7 della Carta dei diritti fondamentali²⁹.

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

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

²⁷ Le medesime preoccupazioni emergevano in due Comunicazioni della Commissione UE: la Comunicazione “Ricostruire la fiducia UE-USA nello scambio dei dati personali” (COM2013/846 del 27 Novembre 2013) e la Comunicazione della Commissione europea al Parlamento europeo sul funzionamento del Safe Harbour dalla prospettiva dei cittadini europei e delle imprese con sede nell’Unione Europea (COM2013/847 del 27 Novembre 2013).

²⁸ Cfr. la sentenza Schrems, punto 92 e la giurisprudenza ivi citata.

²⁹ *Ibidem*, punto 94.

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

Dal punto di vista dei contenuti, nel *Privacy Shield* permangono alcune criticità, sia considerato come sistema complessivo che riguardo alle singole ipotesi di deroga al divieto di trasferimento previste³⁰.

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

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

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

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

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

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

Quanto alle singole ipotesi di deroga espressamente previste, quella che desta particolare perplessità è la possibilità di ricorrere a strumenti di sorveglianza di massa da parte agenzie di *intelligence* statunitensi, ipotesi questa già consentita dal Privacy Harbour, ma in questo caso ristretta a specifiche ipotesi. Tale deroga appare particolarmente problematica ove si consideri la possibilità di fare ricorso alla c.d. *bulk collection of data*, vale a dire la raccolta e la conservazione indiscriminata su larga scala di dati e informazioni personali. Tale pratica, allorché sia assimilabile a *mass surveillance*, appare di per sé stessa incompatibile con il principio di proporzionalità³². In tale circostanza, il fatto che ad essa si faccia ricorso in circostanze eccezionali è del tutto irrilevante ai fini dell’inammissibilità o quantomeno della criticità della deroga.

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

Altra questione irrisolta è poi quella della compatibilità di intercettazioni massive con i principi di necessità e proporzionalità, come recentemente interpretati nella sentenza *Schrems*³³. Se tale forma di intercettazione appare astrattamente legittima anche allo sguardo della Corte di Strasburgo, proprio in considerazione della necessità della lotta al terrorismo internazionale³⁴, dubbi affiorano invece ove si consideri che la legislazione statunitense basa proprio la legittimità delle intercettazioni sulla raccolta di dati indiscriminata di cui sopra³⁵.

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

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

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

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

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

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

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

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

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

4. Le clausole contrattuali standard

Le clausole contrattuali standard, così come le norme vincolanti d'impresa, sono ulteriori strumenti, previsti dal legislatore europeo, che consentono il trasferimento dei dati verso Stati terzi, anche in assenza di una decisione di adeguatezza, ma a costi transattivi più elevati³⁷.

Si tratta di clausole-tipo, di natura contrattuale, approvate dalla Commissione europea, che derogano al divieto di trasferimento dei dati personali tra soggetti privati non appartenenti allo stesso gruppo economico. Tali clausole, inserite nel contratto utilizzato per il trasferimento, hanno la finalità di garantire che importatore ed esportatore siano vincolati al rispetto dei principi e degli obblighi che la normativa europea individua in tema di dati personali quando il Paese extra europeo non offra garanzie “adeguate” ai sensi della normativa europea³⁸. La loro previsione non esclude, infine, che gli operatori possano formulare altre clausole contrattuali *ad hoc* (quindi non standard), che in ogni caso dovrebbero garantire un livello adeguato di protezione dei dati.

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

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

³⁷ Così in G.M. Riccio, cit., p. 24.

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

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

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

Tra le clausole contrattuali approvate dalla Commissione, quest'ultima (decisione 2010/87/UE) merita particolare attenzione, in quanto disciplina i trasferimenti dal titolare del trattamento europeo al soggetto che li elabora stabilito in un Paesi terzo³⁹.

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

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

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

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

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

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

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

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

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

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

5. Le norme vincolanti d'impresa

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

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

Tale strumento non può essere considerato come l'unico od il migliore per il trasferimento di dati personali tra le società partecipanti al gruppo, ma come uno strumento in aggiunta a quelli già esistenti. A tale scopo, la normativa europea richiede l'indicazione della struttura del gruppo societario, dei trattamenti e dei trasferimenti dei dati, con precisazione delle finalità dei trattamenti che verranno effettuati fuori dall'Unione ed identificazione dei Paesi terzi in cui i dati saranno trattati, nonché un'approvazione da parte dell'autorità di controllo nazionale competente⁴⁰, che deve verificare la sussistenza dei requisiti minimi previsti dalla lunga lista contenuta nell'art. 46 del regolamento.

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

Anche in tema di responsabilità, in caso di eventuali violazioni commesse in Paesi terzi il regime presenta delle fragilità, dal momento che quest'ultima incombe sulla società prescelta, salvo che il gruppo societario abbia proposto al Garante nazionale un criterio di ripartizione delle responsabilità di tipo diverso. In altri termini, può accadere che il titolare del trattamento stabilito nell'Unione possa essere esonerato anche completamente da tale responsabilità, a condizione che dimostri che l'evento dannoso non è a lui imputabile⁴¹. Tale possibilità – in evidente contrasto con gli obiettivi della normativa europea in materia –

⁴⁰ V. artt. 63 ss..

⁴¹ V. art. 47, par. 2, lett. f).

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

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

Infine, quanto alla eventuale modifica delle norme vincolanti d'impresa, sembra che la modificazione delle possa essere soggetta a mera comunicazione all'autorità di controllo, senza necessità di preventiva autorizzazione⁴², circostanza questa che non consentirebbe di prevedere *ex ante* le regole che dovranno sovrintendere al trattamento dei dati⁴³.

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

⁴² Cfr. art. 47, par. 2, lett. k).

⁴³ Di diversa opinione, G.M. Riccio, cit., p. 878.

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

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

Per PNR, in sostanza, si intendono i dati identificativi che i passeggeri forniscono ai vettori aerei, che questi ultimi utilizzano per scopi e finalità di tipo commerciale⁴⁴. In particolare, tutti i dati che contengono una serie di informazioni che attengono al singolo passeggero – fra cui il nome, l'indirizzo dell'abitazione e quello di posta elettronica, i recapiti telefonici, le modalità di pagamento, la data di prenotazione, il numero del posto, l'informazione sulle precedenti assenze all'imbarco, ecc.⁴⁵ – sono utilizzati sin dagli anni Cinquanta dagli Stati o dalle autorità a ciò preposte come strumento di lotta al terrorismo e alla criminalità organizzata e, dunque, per finalità connesse alla sicurezza e alla salvaguardia degli interessi nazionali.

La prassi degli Stati di adottare strumenti unilaterali in tale materia, ha poi trovato ulteriore sostegno dopo l'attacco terroristico dell'11 Settembre 2001 in territorio statunitense, che ha richiesto una più stringente sicurezza dei voli aerei⁴⁶. A livello internazionale, invece,

⁴⁴ F. Rossi Dal Pozzo, *EU Legal Framework for Safeguarding Air Passenger Rights*, Cham-Heidelberg-New York- Dordrecht-London, 2015, pp. 99 ss..

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

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

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

Ad oggi, l'Unione europea ha concluso accordi in materia con tre Stati terzi: gli Stati Uniti⁴⁸, l'Australia⁴⁹, il Canada⁵⁰ e nel 2015 sono

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

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

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

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

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

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

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

Degli accordi menzionati, di stretta attualità è tra Unione europea e Canada, che è stato recentemente oggetto di una parere della Corte di giustizia secondo la quale l'accordo non può essere concluso nella sua forma attuale a causa dell'incompatibilità di varie sue disposizioni con i diritti fondamentali riconosciuti dall'Unione⁵¹.

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

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

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

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

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

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

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

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

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

nonostante i progressi fatti in materia di controllo e tutela dei diritti che possono (facilmente) essere violati in materia di dati PNR, permangono alcune criticità strutturali⁵². Infatti, nulla è cambiato rispetto alla mole di dati che possono essere acquisiti ai sensi della direttiva. Ciò indubbiamente resta, come osservato, un'interferenza piuttosto seria, a largo spettro e soprattutto tale da ingenerare negli individui interessati la sensazione che le proprie vite private siano oggetto di sorveglianza costante⁵³.

7. Osservazioni conclusive

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

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

⁵² Sul punto si veda, F. De Benedetti, *Privacy, il Garante Ue: Il pnr misura invasiva e inefficace*, disponibile su www.repubblica.it del 14.4.2016.

⁵³ Cfr. Corte di giustizia, sentenza dell'8 aprile 2014, *Digital Rights Ireland e Seilinger e altri*, cause riunite C-293/12 e C-594/12.

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

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

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

Cristina Grieco¹

Università degli Studi di Macerata e Università di Colonia

L'attuazione in Italia del diritto all'oblio

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

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

Sommario: 1. Introduzione – 2. La consacrazione del diritto all'oblio nella sentenza della Corte di Giustizia nel caso *Google Spain* – 3. Il regolamento UE n. 679/2016 “*Data Protection*” e la positivizzazione del

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

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

1. Introduzione

Quello del diritto all'oblio è un tema particolarmente attuale viste le tragiche vicende che, con frequenza sempre più allarmante, sono balzate agli onori della cronaca negli ultimi tempi. Quanto accaduto offre uno spaccato di quella che è la realtà sociale nell'era di *Internet* e dei *social network*, dove, sempre più di frequente, si assiste ad episodi di sovraesposizione della vita del singolo individuo².

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

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

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

È proprio in questa dimensione della realtà, che non può dirsi poi così distante da quella che Orwell ha descritto nel suo celebre 1984, alla presenza di strumenti tanto pervasivi, che nasce la necessità di intervenire per limitare gli effetti indesiderati. In questo modo, come sosteneva Betti, il diritto tipizzando una determinata fattispecie ed effettuando una selezione degli interessi da proteggere e dei valori da tutelare, riesce a dominare e strutturare la realtà "estranea al diritto" collegando determinati effetti giuridici ad aspetti rilevanti tratti dalla realtà sociale⁴.

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

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

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

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

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

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

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

l’utilizzo di Internet e delle reti telematiche, per le modalità proprie di diffusione dell’informazione; quella che si riferisce al diritto alla cancellazione, al blocco, al congelamento dei dati o all’opposizione al trattamento dei dati previsti dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 “relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”.

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

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

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

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

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

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

Ne consegue che, nell'annosa battaglia che vede contrapposti il diritto di cronaca e il diritto alla privacy⁸, la Corte, ha dimostrato di ritenere prevalente il secondo e ciò necessariamente a discapito dell'interesse economico connesso all'attività del motore di ricerca, gravato di un compito di controllo che, di fatto, almeno a priori, non sembrerebbe competergli.

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

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

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

Nondimeno, non può sottacersi che tale assimilazione susciti delle perplessità, visto e considerato che il motore di ricerca non tratta direttamente i dati inseriti. Il fulcro dell'attività in questione, infatti, è la ricerca di tutti i contenuti presenti sul web che si ricollegano a delle parole chiave scelte ed inserite direttamente dagli utenti, sulla base di un linguaggio specifico (SEO), all'interno dei quali confluiscono anche i dati di titolarità di soggetti privati. In questo caso, quindi, la Corte qualifica come "trattamento dei dati" un'attività che, in prima battuta, opera attraverso degli automatismi, in base a criteri di attinenza e popolarità (sarebbe impossibile, infatti, ipotizzare a priori uno *screening* sui miliardi di dati inseriti ogni giorno)¹⁰. In sostanza, dunque, la Corte addossa in capo al motore di ricerca, che non effettua alcuna operazione di filtraggio delle notizie, tantomeno basata su valutazioni di tipo meritorio, una responsabilità che agevolmente potrebbe essere definita oggettiva e che, addirittura, prescinde dalla liceità stessa della prima pubblicazione della notizia effettuata dall'editore¹¹.

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

⁹ CGUE, C-131/2012, cit., punto 83.

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

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

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

Ciò posto, appare assai complesso giustificare l'assimilazione di posizioni tanto diverse tra loro, ovvero quella di chi tratta quei dati personali come scopo principale della propria attività (come può essere l'attività della testata giornalistica che riporta la notizia) e quella di chi (motore di ricerca), al contrario, si limita a rendere disponibili gli stessi dati, già esistenti in quanto precedentemente trattati da altri soggetti¹². Peraltro, occorre altresì sottolineare che la normativa sul commercio elettronico esclude espressamente che possa rinvenirsi in capo al *provider* un obbligo generale di sorveglianza sulle informazioni che si ritrovi a trattare¹³.

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

¹³ Con il D.Lgs. n. 70 del 9 aprile 2003, l'ordinamento italiano ha recepito la direttiva europea n. 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico. Il legislatore italiano, nel delineare la responsabilità del *provider*, ha distinto tre figure di prestatore:

- prestatori di semplice trasporto, la cui attività consiste nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione (*mere conduit*);
- prestatori di servizi di memorizzazione automatica, intermedia e temporanea delle informazioni, effettuata al solo scopo di rendere più efficace il successivo inoltramento ad altri destinatari a loro richiesta (*caching*);
- prestatori di servizi di memorizzazione di informazioni fornite da un destinatario del servizio (*hosting*).

La responsabilità dell'intermediario viene definita negli artt. 14, 15 e 16 del D.Lgs. n. 70 del 2003 in negativo, in quanto, se sussistono le condizioni di cui al decreto, l'intermediario non è responsabile degli illeciti commessi dagli utenti utilizzando i suoi servizi. L'art. 17 del D.Lgs. n. 70 del 2003 sancisce per i destinatari nella prestazione dei servizi della società dell'informazione sopradescritti l'assenza di un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, e su questo presupposto si prevede un generale esonero da responsabilità per l'illiceità delle informazioni, con determinate deroghe, che attengono principalmente all'art. 14 allo svolgimento di un ruolo attivo nella trasmissione delle informazioni, all'art.

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

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

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

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

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

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

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

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

ne in un determinato elenco di risultati. La Corte evidenzia, infatti, che il diritto all'oblio e, dunque, alla riservatezza prevalgono «non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse [del] pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona». Ciò vale anche nei confronti di contenuti già disponibili da tempo e che emergono da ricerche successive. In questo caso, la Corte ha riconosciuto in capo al soggetto un diritto di opposizione a che quei dati vengano riconnessi al proprio nome, anche a prescindere dal pregiudizio che ciò possa arrecargli¹⁶. Le uniche eccezioni, secondo la Corte, sarebbero da rinvenire in condizioni particolari, come il ruolo ricoperto da un determinato soggetto nella vita pubblica. In tal caso l'ingerenza a scapito della propria sfera personale sarebbe giustificata dall'interesse preponderante del pubblico ad avere accesso a determinate informazioni¹⁷.

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

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

¹⁶ CGUE, C-131/12, cit., punto 97.

¹⁷ CGUE, C-131/12, cit., punto 98.

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

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

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

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

A livello normativo, il passo definitivo verso la positivizzazione del diritto all'oblio è stato compiuto dal legislatore europeo con il regolamento UE n. 679/2016¹⁹, entrato in vigore il 24 maggio 2016, la

¹⁸ CGUE, C-131/2012, cit., punto 93.

¹⁹ Regolamento UE n. 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), pubblicato in GUUE, L 119/1, 4 mag-

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In ottemperanza alla menzionata sentenza della Corte di giustizia²⁰,

²⁰ V. *supra* par. 2.

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

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

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

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

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

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

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

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

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

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

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

5. La Carta dei diritti Internet

Circa un anno dopo la sentenza della Corte di giustizia, in Italia è stata approvata una vera e propria Carta dei diritti e doveri della Rete²³

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

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

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

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

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

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

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

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

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

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

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

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

Interessante appare, al riguardo, il contenuto dei chiarimenti emanati nel 2004, in risposta ad alcuni quesiti posti dall'Ordine dei giornalisti²⁵.

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

Il Garante ha però tenuto a sottolineare che le finalità informative e/o giornalistiche *vanno comunque contemperate con il diritto all'oblio degli interessati*. Per di più, con specifico riguardo al trattamento dei dati personali su reti di comunicazione elettronica, stante l'accessibilità planetaria alle informazioni *online*, il Garante ha altresì specificato che il diritto all'oblio, in tale contesto, deve intendersi come il diritto degli interessati ad evitare che l'indefinita permanenza su *Internet* di dati e informazioni risalenti nel tempo – magari incompleti e non aggiornati in quanto privi dei successivi resoconti giornalistici circa l'evoluzione della notizia originariamente riportata – determini una lesione dei diritti che il Codice della Privacy tende complessivamente a proteggere²⁶.

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

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

²⁶ Cfr. Art. 2 che garantisce che «il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali».

reperibilità è facilitata attraverso motori di ricerca esterni. Inoltre, la lesione del diritto all'oblio (e l'impossibilità dell'interessato di tornare nell'anonimato) è resa ancor più grave quando le informazioni riprodotte o disponibili in maniera permanente, sebbene in origine legittimamente pubblicate, risultino poi nel tempo incomplete. Un esempio è il caso di un soggetto menzionato in un articolo giornalistico in quanto indagato ma successivamente assolto senza che di questa positiva evoluzione venga data notizia.

Ciò posto, il Garante ha evidenziato che il discrimine per pubblicare o meno una notizia è l'esistenza dell'interesse pubblico. Pertanto chiunque voglia successivamente riproporre e ripubblicare (o semplicemente far permanere) su *Internet* articoli giornalistici contenenti dati personali di terzi, è tenuto a verificare, a maggior ragione quando l'intendimento è quello di dare diffusione planetaria della notizia sul *web*, che tale interesse sussista al momento della ripubblicazione. Sarà dunque necessaria una nuova valutazione, altra rispetto a quella svolta dal giornalista autore della originaria pubblicazione, che tenga in debito conto – nell'ottica del diritto all'oblio – il fatto che la persona coinvolta sia o meno un personaggio pubblico.

A tale riguardo, particolarmente interessante appare il contenuto del provvedimento adottato dal Garante nel 2008 nell'accoglimento di un reclamo presentato da un privato cittadino²⁷. Nel caso di specie, il ricorrente richiedeva che non restassero associate perennemente al proprio nome in rete, per mezzo delle “scansioni” operate automaticamente dai motori di ricerca esterni al sito dell'editore, le notizie oggetto di un determinato articolo, considerato lesivo. Nella specie, il Garante ha ritenuto che i motivi prospettati apparissero meritevoli di specifica tutela tenuto conto del-

²⁷ Cfr. Autorità Garante per la protezione dei dati personali «Archivi storici online dei quotidiani e reperibilità dei dati dell'interessato mediante motori di ricerca esterni – 8 aprile 2009 – [1617673]» disponibile al seguente indirizzo <http://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/1617673>.

le peculiarità del funzionamento di *Internet*, che può comportare la diffusione di un gran numero di dati personali riferiti ad un medesimo soggetto. In particolare, il Garante, evidenziando quella che, in definitiva, deve considerarsi l'essenza stessa del diritto all'oblio, ha posto l'accento sul fatto che deve essere garantita ad un soggetto, che ha intrapreso nuovi percorsi di vita personale e sociale, la possibilità di allontanarsi da vicende pregiudizievoli risalenti nel tempo. Tale diritto viene ostacolato per mezzo della rappresentazione istantanea e cumulativa derivante dai risultati delle ricerche operate mediante i motori di ricerca che «rischiano di riverberare comunque per un tempo indeterminato i propri effetti sugli interessati come se fossero sempre attuali».

Sonora appare la conclusione a cui è giunto il Garante in tale occasione. All'editore, infatti, è stato imposto di adottare ogni misura necessaria affinché le generalità del ricorrente non risultassero più direttamente rinvenibili attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito *Internet*.

7. La posizione della giurisprudenza italiana sul diritto all'oblio

In tema di diritto all'oblio, l'orientamento sviluppato dai giudici italiani appare meritevole di approfondimento. In particolare, la Cassazione è intervenuta sul tema statuendo che «il soggetto titolare dei dati personali oggetto di trattamento deve ritenersi titolare del diritto all'oblio anche in caso di memorizzazione nella rete Internet, mero deposito di archivi dei singoli utenti che accedono alla rete e, cioè, titolari dei siti costituenti la fonte dell'informazione»²⁸. La Corte ha esplicitamente chiarito che sebbene l'interesse pubblico sotteso al diritto all'informazione, previsto dall'articolo 21 della Carta costituzionale, costituisca un limite al diritto fondamentale alla riservatezza, al sogget-

²⁸ Cass. Civ., Sez. III, 5 aprile 2012, n. 5525, in *Nuova giur. civ. comm.*, 2012, 10, p. 1.

to a cui appartengono i dati utilizzati deve essere correlativamente attribuito il diritto all'oblio.

Sebbene tale pronuncia, almeno parzialmente, si configuri come un *obiter dictum*²⁹, il riconoscimento espresso in capo al soggetto di uno specifico diritto all'oblio, anche al di fuori del classico paradigma diritto di cronaca/diritto di riservatezza, conferisce alla sentenza una portata innovativa.

La Suprema Corte, infatti, con tale pronuncia ha sancito e riconosciuto il diritto del soggetto a richiedere che non vengano ulteriormente divulgate notizie che, per il trascorrere del tempo, risultino ormai dimenticate o ignote alla generalità dei consociati.

In una pronuncia più risalente³⁰, la Corte di Cassazione aveva fornito alcune precisazioni al riguardo. Atteso che il trattamento dei dati personali può avere ad oggetto anche dati pubblici o già pubblicati, ha chiarito la Corte, il diritto all'oblio funge da limite per salvaguardare la *proiezione sociale dell'identità personale*, ovvero l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita – stante il lasso di tempo intercorso dall'accadimento del fatto che ne costituisce l'oggetto – di attualità delle stesse. La Suprema Corte, infatti, ha evidenziato che il trattamento di determinate informazioni può risultare non più giustificato o addirittura di ostacolo per il soggetto nell'esplicazione e nel godimento della propria personalità, in ragione del trascorrere del tempo.

Peraltro, già in una delle prime pronunce³¹, la Corte aveva precisato che, in materia di trattamento di informazioni, il soggetto cui l'informazione si riferisce ha diritto al rispetto della propria identità personale o morale. In altre parole, l'interessato ha diritto a non vedere «travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale e, pertanto, alla verità della propria immagine nel momento storico attuale».

²⁹ Cass. Civ., Sez. III, 9 aprile 1998, n. 3679, in *Giust. Civ., Mass.*, 1998, p. 778.

³⁰ Cass. Civ., Sez. I, 25 giugno 2004, n. 11864, in *Giust. Civ.*, 2005, f. 11, I, p. 2731.

³¹ Cass. Civ., Sez. I, 22 giugno 1985, n. 7769, *inedita*.

Più di tutto però, in materia, non può non essere ricordata la sentenza che la Suprema Corte ha emanato recentemente³². La questione, esaminata in primo grado dal Tribunale di Chieti, riguardava una condanna al risarcimento del danno per violazione del diritto all'oblio che aveva coinvolto sia il direttore sia l'editore di una testata giornalistica telematica, a motivo della permanenza di un articolo su una vicenda giudiziaria di natura penale che aveva coinvolto i ricorrenti per un fatto avvenuto tempo prima e che non si era ancora conclusa. Nella specie, i ricorrenti lamentavano che tale permanenza risultava pregiudizievole non solo per la propria reputazione personale ma anche per il danno di immagine arrecato all'attività commerciale dagli stessi gestita.

Giunta la questione dinanzi alla Suprema Corte, quest'ultima ha confermato la condanna al risarcimento del danno a carico del direttore e dell'editore della testata giornalistica. Nella specie, la Corte ha evidenziato che l'illecito trattamento di dati personali era stato correttamente ravvisato dal giudice di prime cure non già nel contenuto e nelle originarie modalità di pubblicazione e diffusione *on line* dell'articolo di cronaca e nemmeno nella conservazione e archiviazione informatica di esso, ma nel mantenimento del diretto ed agevole accesso a quel risalente servizio giornalistico pubblicato molto tempo prima e della sua diffusione sul web, anche in data successiva al ricevimento di specifica diffida da parte degli interessati. In particolare, secondo la Suprema Corte, il Tribunale aveva giustamente rilevato che risultava incontestato che digitando (tramite il motore esterno di ricerca *Google*) il nominativo dei ricorrenti si accedeva alla prima pagina del sito *web* che includeva, affiancato e associato alla reclamizzata attività del locale da loro gestito, anche il *link* sull'articolo di cronaca redatto tempo prima. Tale

³² Cass. Civ., Sez. I, 24 giugno 2016, n. 13161, in *Persona e Danno*, con nota di F. Sassano, *Diritto all'oblio. Fissato un tempo perché gli accadimenti siano cancellati dagli archivi online*, al seguente indirizzo: <https://www.personaedanno.it/riservatezza-privacy/diritto-all-oblio-fissato-un-tempo-perche-gli-accadimenti-siano-cancellati-dagli-archivi-on-line-cass-civ-13161-16-francesca-sassano>.

consultazione risultava di facile accessibilità e consultabilità, di molto superiore a quelle dei quotidiani cartacei, tenuto conto dell'ampia diffusione locale del giornale *on line*. Inoltre, secondo quanto rilevato dal giudice di prime cure, indubbiamente, il persistere del trattamento dei dati personali aveva determinato una lesione del diritto dei ricorrenti alla riservatezza ed alla reputazione, soprattutto in relazione alla peculiarità dell'operazione di trattamento, caratterizzata dalla capillarità della divulgazione dei dati trattati e dalla natura degli stessi, particolarmente sensibili attenendo ad una vicenda giudiziaria penale.

La Suprema Corte, nell'ambito di tale vicenda giudiziaria, ha evidenziato come il diritto all'oblio si spinga oltre la mera tutela della *privacy* e come sia un diritto di derivazione perlopiù giurisprudenziale e di elaborazione dottrinale, grazie anche alle posizioni assunte dalle Autorità Garanti europee. Esso, secondo la Corte, è da intendersi proprio quale diritto dell'individuo ad essere dimenticato; diritto che mira a salvaguardare il riserbo imposto dal tempo ad un notizia già resa di dominio pubblico.

Il fondamento normativo in Italia del diritto all'oblio, secondo la Suprema Corte, è da rinvenire nel Codice della Privacy laddove prevede che il trattamento di dati non risulti legittimo qualora gli stessi siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o trattati (articolo 11 del decreto legislativo 196/2003). Inoltre, in base a quanto specifica ulteriormente l'articolo 7 del medesimo decreto, l'interessato ha il diritto di conoscere in ogni momento chi possiede i suoi dati personali e come li adopera, nonché di opporsi al trattamento dei medesimi, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettifica, l'aggiornamento o l'integrazione.

La pronuncia risulta particolarmente rilevante in quanto la Corte evidenzia come il diritto all'oblio non sia altro che la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca. Così come non va reso pubblico il fatto la cui diffu-

sione (lesiva) non risponda ad un reale interesse della collettività, allo stesso modo non va riproposta la vecchia notizia (anch'essa lesiva) quando ciò non sia più rispondente ad una attuale esigenza informativa.

La portata innovativa di tale sentenza è, inoltre, da ravvisarsi in due ulteriori profili. In primo luogo, la Corte evidenzia come l'attualità o meno della notizia vada valutata non già con riferimento al procedimento giudiziario, il quale, se ancora in corso, rischierebbe di dilatare i tempi del diritto all'oblio, subordinandolo ai ritardi della giustizia italiana e, peraltro, differenziandolo da soggetto a soggetto, bensì al fatto storico. In secondo luogo, la Corte ha riconosciuto la possibilità di esercitare il diritto all'oblio, con la conseguente rimozione delle informazioni pregiudizievoli, anche in corso di processo.

Nella direzione tracciata dalla Suprema Corte si è mossa anche la giurisprudenza di merito.

In una recente pronuncia³³, ad esempio, il Tribunale di Roma ha concretamente applicato i principi elaborati dalla Corte di giustizia dell'Unione Europea nella decisione "*Google Spain*" riconoscendo, però, la prevalenza dell'interesse pubblico sul diritto all'oblio dell'interessato. Il caso riguardava un avvocato, che nel 2014 aveva richiesto a *Google* di deindicizzare alcuni URL risultanti da una ricerca concernente il proprio nominativo con riferimento a vicende giudiziarie in cui risultava implicato. Si trattava, nella specie, di notizie di cronaca relative a una vicenda giudiziaria risalente agli anni 2012/2013 che lo vedeva coinvolto, insieme ad altri personaggi romani, esponenti del clero e soggetti riconducibili alla c.d. "banda della Magliana" in presunte truffe e guadagni illeciti. Il professionista si doleva che tali informazioni riferite dai risultati del motore di ricerca, oltre ad essere false, facevano riferimento a una risalente vicenda giudiziaria nella quale era rimasto coinvolto senza che fosse mai stata pronunciata alcuna condanna. Nondimeno, il Tribunale ha respinto la domanda, chiarendo che

³³ Trib. Roma, Sez. I, 3 dicembre 2015, n. 23771, *inedita*.

seppure essa risultava riconducibile al trattamento dei dati personali e al diritto all'oblio, quale parte essenziale del diritto alla riservatezza, i dati trattati risultavano da un lato recenti e dall'altro di interesse pubblico.

Il Tribunale, infatti, ha evidenziato che il trascorrere del tempo dall'accadimento dei fatti, ai fini della lesione del diritto all'oblio, si configura come elemento costitutivo essenziale. Invero, i dati di cui il ricorrente richiedeva la cancellazione risultavano recenti e dotati di una loro innegabile attualità, soprattutto in considerazione del ruolo pubblico del ricorrente, professionista esercente l'attività di avvocato in Svizzera.

Il Tribunale ha aggiunto poi un tassello ulteriore, discostandosi però da quanto la Corte di giustizia aveva precedentemente statuito nel caso *Google Spain*. Relativamente alle doglianze sulla falsità delle notizie riportate dal motore di ricerca, infatti, a parere del Tribunale, l'interessato è tenuto ad agire a tutela della propria reputazione e riservatezza esclusivamente nei confronti dei siti terzi che abbiano pubblicato notizie infedeli o non aggiornate con i successivi sviluppi, eventualmente a lui favorevoli, ma non nei confronti del gestore del motore di ricerca, poiché questo opera meramente quale *caching provider* ai sensi dell'articolo 15 del decreto legislativo 70/2003.

Il giudice di merito ha dunque chiarito che, nel bilanciamento tra diritto alla riservatezza e l'interesse pubblico a rinvenire sul *web* notizie relative a persone che svolgono ruoli pubblici, il diritto di informazione prevale su quello all'oblio. Degna di nota appare, in questo senso, la conclusione del Tribunale che ha evidenziato come in ogni caso il diritto all'oblio non possa e non debba essere utilizzato per abbellire o smacchiare la reputazione di un soggetto che svolge ruoli di rilevanza pubblica.

Interessante sul tema appare anche una recente sentenza del Tribunale di Milano³⁴. Con tale pronuncia è stato imposto a *Google* di provvedere alla rimozione dei risultati connessi ad un articolo

³⁴ Trib. di Milano, Sez. I, 28 settembre 2016, n. 10374, *inedita*.

giornalistico riguardante una componente dell'Autorità Garante per l'Energia e il Gas (AEEG), la quale veniva apostrofata come la "raccomandata di Bersani".

Nella specie, il Tribunale di Milano, annullando il rigetto opposto dal Garante per la Privacy sul reclamo presentato dalla ricorrente, ha ordinato a *Google* di deindicizzare una pagina web in cui permaneva l'articolo del quotidiano "Il Giornale", dell'8 dicembre 2010, intitolato "*L'energia? Un affare di famiglia. Vince la raccomandata di Bersani*".

Il Tribunale, al riguardo, ha evidenziato che a prescindere dal carattere diffamatorio o meno, i medesimi dati personali, che magari nell'immediato potevano essere trattati lecitamente dai mezzi di informazione nel nome di un prevalente «interesse pubblico», possono poi perdere quell'interesse se, circolando sul *web* a distanza di tempo, «risultano non aggiornati, non pertinenti, non completi». Il Tribunale, in questo caso, specifica che l'interesse alla pubblicazione delle informazioni contenute nell'articolo non prevale, non tanto su un diritto all'oblio, quanto su un diritto al «ridimensionamento della propria visibilità telematica», perché l'interesse collettivo alla pubblicazione di una notizia deve essere verificato nel tempo.

8. Conclusioni

Come evidenziato, i contorni del diritto all'oblio sono stati ora definitivamente tracciati attraverso il nuovo regolamento "*Data Protection*" adottato dal legislatore europeo. A partire dal 2018, si renderà necessario valutare gli effetti e le problematiche che sorgeranno dall'applicazione della nuova regolamentazione.

Per ciò che attiene al momento presente in Italia, la tutela in forma specifica messa a disposizione in seguito alla sentenza della Corte di giustizia, che si risolve in un *format* che consente di richiedere direttamente al motore di ricerca la rimozione dei contenuti ritenuti pregiudici-

zievoli, come chiarito, riguarda per lo più la *privacy* e non strettamente il diritto all'oblio. Ciononostante, la percentuale delle domande che trova positivo accoglimento si aggira intorno al 33%. Questo dato pone l'Italia come fanalino di coda in Europa.

Occorre invece rilevare che tanto l'Autorità Garante per la Privacy quanto la giurisprudenza si sono mostrate piuttosto propense a riconoscere e, in taluni casi ad implementare, il diritto all'oblio e i suoi contenuti, già prima della sentenza della Corte di giustizia. A maggior ragione, dopo la pronuncia della Corte, questa tendenza favorevole è stata ampiamente riconfermata.

Da quanto emerge dai provvedimenti e dalle pronunce esaminate, sono eminentemente due i fattori che occorre tenere in considerazione perché il diritto all'oblio possa essere esercitato con successo: il fattore tempo e il venir meno dell'interesse generale della collettività ad essere informato in merito a determinati accadimenti. Se entrambe le condizioni sono verificate, ovvero è trascorso un ragionevole lasso di tempo tale da rendere la conoscenza di quella notizia non più rispondente ad un interesse pubblico, il diritto all'oblio potrà essere esercitato con successo consentendo così all'interessato di ristabilire quella che viene definita una “reputazione digitale integra”.