

Laura Valle – Laura Greco

**TRANSNAZIONALITÀ DEL
TRATTAMENTO DEI DATI
PERSONALI E TUTELA DEGLI
INTERESSATI, TRA STRUMENTI DI
DIRITTO INTERNAZIONALE
PRIVATO E LA PROSPETTIVA DI
PRINCIPI DI DIRITTO PRIVATO DI
FORMAZIONE INTERNAZIONALE**

Estratto



Milano • Giuffrè Editore

LAURA VALLE - LAURA GRECO

TRANSNAZIONALITÀ DEL TRATTAMENTO DEI DATI PERSONALI E TUTELA DEGLI INTERESSATI, TRA STRUMENTI DI DIRITTO INTERNAZIONALE PRIVATO E LA PROSPETTIVA DI PRINCIPI DI DIRITTO PRIVATO DI FORMAZIONE INTERNAZIONALE

SOMMARIO: 1. Il trattamento dei dati a livello transnazionale, il loro trasferimento transfrontaliero e la potenziale lesione dei diritti degli interessati. — 2. Le decisioni della Corte di Giustizia Ue sul trattamento transnazionale dei dati, la nozione di « stabilimento » del titolare del trattamento dei dati personali e la nozione di « trattamento » dei dati personali di cui all'art. 4 dir. 95/46. — 2.1. L'attuazione delle decisioni della Corte di Giustizia all'interno degli Stati membri, e oltre. — 3. Il trasferimento transfrontaliero dei dati personali nella disciplina della dir. 95/46. — 3.1. In particolare: l'intervento della Corte di Giustizia Ue con la sentenza *Schrems* e il *Privacy Shield* per il trasferimento dei dati negli Stati Uniti e i rapporti con gli operatori statunitensi. — 4. Il trattamento dei dati personali con profili di transnazionalità e il trasferimento dei dati personali all'estero nel nuovo Regolamento europeo 2016/679. Introduzione: il modello di tutela dei dati personali introdotto dal Regolamento europeo. — 4.1. (*segue*) Il nuovo criterio di applicazione territoriale della disciplina europea nel Regolamento europeo 2016/679. — 4.2. (*segue*) Il trasferimento di dati all'estero tra continuità ed innovazione nel nuovo Regolamento europeo. — 5. La tutela dei dati personali in prospettiva globale: le regole esistenti a livello internazionale. — 5.1. (*segue*) La Convenzione n. 108 del Consiglio d'Europa. — 5.2. (*segue*) Le Linee Guida dell'Ocse. — 5.3. (*segue*) Il *Privacy Framework* dell'A-PEC. — 5.4. (*segue*) I *Core Principle* individuati dall'UNCTAD. —

* Il presente lavoro è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le prassi correnti nella comunità dei giuristi.

** L'ideazione dell'articolo e della sua struttura sono di Laura Valle. A Laura Valle sono da attribuire i seguenti paragrafi: 1, 2, 3, 3.1, 4 (cpv. 4-6), 5, 5.1, 5.2,

5.3, 5.4, 6 e le seguenti note: 69, oltre a quelle dei parr. redatti dall'autrice. A Laura Greco sono da attribuire i seguenti paragrafi: 2.1, 4 (cpv. 1-3), 4.1, 4.2, e le seguenti note a piè di pagina: 4, 6, 7, 9, 13, 20, 49, 59, 64, 91, 120, 124, oltre a quelle dei parr. redatti dall'autrice. Nel corso del lavoro il dialogo e lo scambio di informazioni tra le autrici è stato costante.

6. Conclusioni. Da regole europee di diritto internazionale privato a principi di tutela dei dati personali di formazione internazionale.

1. IL TRATTAMENTO DEI DATI CON PROFILI DI TRANSNAZIONALITÀ, IL LORO TRASFERIMENTO TRANSFRONTALIERO E LA POTENZIALE LESIONE DEI DIRITTI DEGLI INTERESSATI.

La diffusività nella società contemporanea del ricorso ad un mezzo di comunicazione globale qual è Internet in contrasto con l'organizzazione del diritto su base nazionale o sovranazionale, ma non globale ¹, fa sì che il trattamento a livello transnazionale dei dati personali ed il trasferimento e la circolazione dei dati personali oltre le frontiere di un singolo Stato siano attualmente tra i profili più problematici nella disciplina della protezione dei dati personali, e, per questo, oggetto delle maggiori attenzioni. Nonostante l'armonizzazione della disciplina a livello europeo grazie alla dir. 95/46/CE, persistono divergenze tra le medesime normative di attuazione dei diversi Paesi membri dell'Unione europea, soprattutto rispetto alla regolazione e ai poteri sanzionatori delle Autorità di controllo ², destinate ad essere superate solo con l'entrata in vigore del Reg. (UE) 2016/679 prevista per il 25 maggio 2018.

Tanto tali profili della tutela dei dati personali caratterizzati dalla transnazionalità sono oggetto della massima attenzione, che sono in corso a livello sovranazionale dibattiti ed iniziative concrete per sviluppare regole dalla portata internazionale o, quanto meno, principi dalla base comune che siano compatibili tra loro. Come si vedrà nel corso di questo lavoro quello attuale si presenta quindi come un momento risolutivo per la presa di coscienza del problema e lo sviluppo di tali iniziative ³.

Sono responsabili del fenomeno del trattamento transnazionale dei dati personali e del trasferimento dei dati verso Paesi terzi, in

¹ Osserva a proposito di Internet la tensione tra globalità della fattispecie e territorialità della norma, DRAETTA, *Internet nel diritto internazionale*, in FINOCCHIARO-DELFINI, *Diritto dell'informatica*, Torino, Utet, 2014, p. 3.

² FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. inf.*, IV-V/2015, p. 793 e nota 42, che rimanda alle conclusioni dell'Avvocato generale del caso *Weltimmo*.

³ Afferma che l'ambito Internet pone particolari problemi di tutela della *privacy*, DRAETTA, *Internet nel diritto internazionale*, cit., p. 36, che esamina come i rapporti globali caratteristici di Internet si sono collocati nell'ambito di quello che si può

denominare diritto internazionale dei privati, esito del processo di erosione del diritto nazionale dal secondo dopoguerra in poi. « La globalizzazione ha portato ad una rivoluzione copernicana in materia, con il che un numero sempre crescente di norme applicabili ai privati viene determinato in un contesto extra-statale. Al complesso di queste norme abbiamo dato il nome convenzionale di diritto internazionale dei privati ». L'Autore osserva che nel diritto internazionale dei privati si possono collocare: norme internazionali di origine convenzionale, prodotte anche su iniziativa di organizzazioni internazionali; norme dell'Unione europea che si indirizzano direttamente ai rapporti tra privati (mentre in un primo tempo le norme europee comunitarie

particolare, le imprese che gestiscono motori di ricerca, *social network*, siti commerciali dalla portata transfrontaliera, gli operatori dei servizi di *cloud computing*. Il trattamento transnazionale ed il trasferimento dei dati accompagnano gli sviluppi tecnologici informatici del prossimo futuro tra i quali, oltre al *cloud computing* ⁴, i c.d. *big data* ⁵ e la *Internet of Things* (IoT) ⁶. Il trasferimento dei dati personali all'estero è anzi all'atto pratico coesistente allo svolgimento di servizi come

avevano ad oggetto la regolazione del mercato); regole che compongono la *lex mercatoria*; e regole di *soft law* contenute nelle linee guida e nei codici di condotta che, se pure non giuridicamente rilevanti, non sono irrilevanti per il diritto, potendo avere una funzione ausiliaria di indirizzo sia per colmare lacune normative che per interpretare norme vincolanti (pp. 8-16). Tali regole senz'altro non paiono poter far parte del diritto interno ma uguale disagio si prova ad inquadrarle nel diritto internazionale pubblico, eccetto che per il diritto uniforme unilateralmente imposto e, con qualche limite, per il diritto comunitario. « Tali norme, infatti, si rivolgono ad individui, non agli Stati. Inoltre esse prescindono dalle frontiere nazionali e le travalicano continuamente (il fenomeno è macroscopico per Internet e il commercio elettronico (...)), mentre il diritto internazionale presuppone gli Stati territoriali e i loro confini. Non rimane allora che pensare ad una vita internazionale del diritto in cui accanto alla tradizionale comunità degli Stati si formino in misura crescente comunità di individui che si danno proprie norme cui gli Stati devono dare attuazione come a quelle di diritto internazionale tradizionale » (p. 25).

⁴ Un rapporto dell'Istituto Nazionale di Statistica del 2014 ha evidenziato una forte crescita nell'impiego della tecnologia del *cloud computing*, utilizzata dal 40,1% delle imprese del campione, percentuale che sale al 47,4% nella fascia delle grandi imprese. L'Istat sottolinea l'alta diffusione anche tra le piccole imprese, attratte dalla scalabilità dei servizi e dalla possibilità di esternalizzare tutte le attività di manutenzione e sviluppo di ICT. I servizi di *cloud computing* acquistati più di frequente sono, nell'ordine, *e-mail* (di cui si avvale il 34,5% delle imprese), *software* per ufficio (16,5%), applicazioni per finanza e contabilità (13,4%), servizi di archiviazione di file (12,7%), *hosting* di database (11,1%), applicazioni CRM (5,8%) e utilizzo di potenza di calcolo per eseguire *software* (3,2%). Mentre gli ultimi quattro servizi sono utilizzati con più frequenza dalle imprese con almeno 250 addetti, la posta elettronica in

cloud è il servizio più diffuso al diminuire della dimensione aziendale. Tra i fattori che limitano l'uso di servizi *cloud* fra chi già li adotta sono il rischio di violazione della sicurezza (27,3% delle grandi imprese, 19,7% delle piccole) e la conoscenza non adeguata di questi servizi (13% delle grandi imprese e 22% delle piccole). Le grandi imprese inoltre sono più sensibili a problemi connessi alla difficoltà di trasferire dati in caso di recesso dal contratto con il fornitore (25,5%) e all'incertezza del quadro legislativo, specie nei casi di controversie (24,7%) e rispetto all'ubicazione dei dati (19,8%). Viene rilevato invece che i problemi legati all'accesso ai dati o al *software* in *cloud* (13%) e gli alti costi d'acquisto dei servizi (17%) sono comuni a tutte le imprese senza rilevanti differenze dimensionali. Tra i fattori che ostacolano l'uso di servizi *cloud* da parte di chi invece non li usa ancora il 31,6% di piccole imprese indica la conoscenza insufficiente dello strumento contro il 14,5% delle grandi, per le quali invece l'ostacolo maggiore è il rischio di violazione della sicurezza (30,8%). Il *report* è consultabile al sito *web* http://www.istat.it/it/files/2014/12/Report ICTimprese_2014.pdf

⁵ Rispetto al trattamento dei dati nelle operazioni di *big data* e di *cloud computing* il rapporto tra controllore (o titolare) ed elaboratore (o responsabile), o subelaboratori, è sempre più problematico in quanto la seconda figura tende progressivamente ad avere un potere reale di controllo maggiore senza incorrere in responsabilità, e le due figure possono trovarsi in Stati diversi con problemi di disciplina del trasferimento dei dati, FOCARELLI, *La privacy. Proteggere i dati personali nell'era digitale*, Bologna, Il Mulino, 2015, p. 123.

⁶ *Internet of Things* è l'espressione adottata per definire la rete delle apparecchiature e dei dispositivi, diversi dai computer, connessi a Internet. Si può trattare, ad esempio, di elettrodomestici, telecamere, container per il trasporto merci, automobili, radio, impianti di climatizzazione, sensori per il fitness. L'espressione *big data* viene utilizzata, invece, per indicare la capacità di usare le informazioni oggi dispo-

quelli di *cloud computing* oggi di ampio utilizzo e in via di sempre maggiore diffusione nel prossimo futuro ⁷. Il fenomeno del trattamento transnazionale dei dati si allarga, ancora, ad abbracciare la grande maggioranza dei siti Internet se si riflette sulla circostanza che i *cookie* impiegati dai siti raccolgono dati personali degli utenti, che si prestano spesso nel concreto ad essere trattati secondo leggi di Paesi terzi o ad essere trasferiti all'estero ⁸.

L'ampiezza di tale fenomeno si comprende altresì se si ha

nibili in grandi quantità per elaborare, analizzare e trovare riscontri oggettivi relativamente a diverse tematiche, e quindi gli algoritmi capaci di trattare così tante variabili in poco tempo e con poche risorse computazionali.

L'Osservatorio dei *Big data Analytics* e *Business Intelligence* e l'Osservatorio *IoT* della *School of Management* del Politecnico di Milano hanno condotto recentemente un'indagine relativa allo sviluppo di questi due recenti fenomeni. Relativamente ai *big data*, è emersa una crescita significativa (+44%), in gran parte trainata dalle grandi imprese, che si dividono l'87% della spesa complessiva, mentre le Pmi si fermano al 13%. Il settore più interessato nel mercato degli *Analytics* tra le grandi imprese è quello bancario (29%), seguito da quello manifatturiero (22%), delle telecomunicazioni e media (14%), Pubblica Amministrazione e sanità (8%), altri servizi (8%), GDO (7%), *utility* (6%) e assicurazioni (6%). Per maggiori approfondimenti, cfr. http://www.osservatori.net/it_it/osservatori/executive-briefing/nel-2016-boom-degli-analytics-in-italia-15-un-mercato-da-900-milioni-di-euro.

Anche il settore della *Internet of Things* è stato protagonista di uno sviluppo significativo, che ha coinvolto non solo i consumatori, ma anche città e imprese. In particolare, a guidare la crescita dell'*IoT* in Italia sono state le applicazioni consolidate che sfruttano la connettività cellulare (1,47 miliardi di euro, +28% rispetto al 2014) e quelle che utilizzano altre tecnologie come *Wireless M-Bus* o *Bluetooth Low Energy* (530 milioni di euro, +33%). Il principale segmento di mercato è costituito dalle soluzioni di *Smart Metering* (i contatori intelligenti per la misura dei consumi) e di *Smart Asset Management* nelle *utility* (la gestione in remoto per rilevare guasti, manomissioni, localizzazione, etc.). Segue la *Smart Car*, con 5,3 milioni di auto connesse in Italia, insieme alle soluzioni di *Smart Building* (18%), in particolare per la videosorveglianza e la gestione degli impianti foto-

voltaici, quelle di *Smart Logistics* (11%) per la gestione di flotte aziendali e antifurti satellitari e, infine, quelle di *Smart City & Smart Environment* (9%), tra cui si segnalano 200.000 mezzi di trasporto pubblico monitorati da remoto e 600.000 pali di illuminazione intelligente. Da segnalare è anche la *Smart Home* (7%), soprattutto con applicazioni di antintrusione e termostati controllati a distanza. Per maggiori approfondimenti, cfr. http://www.osservatori.net/it_it/osservatori/executive-briefing/Internet-of-things-il-futuro-e-giapresente.

⁷ A tal proposito si ricorda che molti dei processi di *cloud computing*, per ragioni sostanzialmente riconducibili al contenimento dei costi, si avvalgono dell'operato di società collocate in nazioni diverse da quella in cui ha sede il cliente, provocando così un flusso transfrontaliero di dati. Il medesimo risultato si ha anche quando il servizio offerto in modalità *cloud* costituisce un'aggregazione di diversi servizi acquisiti dalla società fornitrice del servizio e cumulativamente offerti, ma individualmente erogati da separati fornitori sempre in modalità *cloud*, dando così vita ad una pluralità di relazioni negoziali ed al trasferimento dei dati fra più soggetti. Ciò significa tra l'altro che l'utente non ha mai contezza della reale posizione dei suoi dati.

⁸ Si distinguono *cookie* tecnici che trovano la loro necessità nella sola navigazione su un determinato sito, da *cookie* di profilazione che invece non sono necessari tecnicamente per consentire la navigazione ma trovano ragione nell'attività di profilazione delle preferenze degli utenti del sito. I *cookie* sono regolarmente inviati, inoltre, non solo dal titolare del sito ma anche da terze parti, e tanto anche senza che il titolare del sito possa esercitare il suo controllo su tale attività di profilazione di terze parti. Il Garante per la protezione dei dati personali è intervenuto con un regolamento del 2014 (entrato in vigore nel giugno 2015) a disciplinare nel dettaglio la segnalazione dei *cookie* all'utenza dei siti, in aggiunta alla regolazione generale di cui all'art. 122 cod.

presente il significato molto largo secondo cui vanno intesi i concetti di “dato personale”⁹ (art. 4, lett. *b* cod. privacy) e di “trattamento” dei dati personali (art. 4, lett. *a* cod. privacy). Secondo la definizione normativa è dato personale « qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale » (art. 4, 1° co., lett. *b* cod. privacy). Ed è trattamento « qualunque operazione o complesso di operazioni, effettuati anche senza l’ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la

privacy (introdotta in attuazione della dir. 2009/136 dal d.lgs. n. 69 del 2012). Per quanto concerne la regolazione del fenomeno sotto il profilo della tutela del diritto personale alla *privacy*, il Garante ha specificato che i *cookie* tecnici devono essere preceduti da un’informativa ex art. 13 cod. privacy ma rispetto ad essi non è richiesto il consenso, che è invece necessario per i *cookie* di profilazione. Per la manifestazione di tale consenso, rispetto alla profilazione da parte del titolare del sito come da parte di terzi, il Garante ha previsto un’informativa sintetica che deve essere evidente sul sito non appena lo si raggiunga (secondo la previsione dell’art. 122, 1° co. che rinvia all’art. 13, 3° co. cod. privacy), ed un’informativa estesa di secondo livello che deve contenere tutti gli elementi previsti dall’art. 13 cod. privacy illustrando nel dettaglio le finalità della profilazione per quegli utenti che decidano di voler accedere ad informazioni di livello più approfondito sulla tutela dei dati. All’interno di tale informativa dev’essere inserito anche il *link* aggiornato alle informative e ai moduli di consenso delle terze parti con le quali il titolare ha stipulato accordi per l’installazione di *cookie* tramite il proprio sito. Qualora il titolare abbia contatti indiretti con le terze parti dovrà inserire i *link* ai siti dei soggetti che fanno da intermediari tra lui e le stesse terze parti. Tale tecnica di informativa dell’utenza e di acquisizione del consenso trova ragione nel contemperamento delle ragioni di tutela dei dati dell’utente con le attività di significato economico che sono sorte con la navigazione *online*.

⁹ « Muovendo (...) dall’ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l’insieme delle informazioni che al medesimo si

riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell’informazione ». FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, cit., p. 783, « il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare il controllo sul flusso delle proprie informazioni. Per questa ragione è frequente che il diritto alla protezione dei dati personali sia inteso come diritto all’autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi ».

L’ampiezza del concetto di “dato personale” è stata approfondita dal Gruppo di lavoro Art. 29 (la cui costituzione è prevista dall’art. 29 dir. 95/46, ed è composto da un rappresentante delle Autorità di controllo di ciascun Stato membro, da un rappresentante dell’*European Data Protection Supervisor* e da un rappresentante della Commissione europea) nel parere 4/2007 sul concetto di dati personali, adottato il 20 giugno 2007, in cui viene analizzata puntualmente la definizione offerta dalla dir. 95/46. Il Gruppo, pur riconoscendo l’estensione del concetto di dati personali, ha tenuto a ribadire che obiettivo del legislatore è « proteggere i diritti e le libertà fondamentali delle persone, in particolare il diritto alla vita privata, in relazione al trattamento dei dati personali », pertanto « il campo d’applicazione delle norme di protezione dei dati personali non va esteso oltre misura » per evitare che « le norme di protezione dei dati si applichino a situazioni che non erano destinate ad essere disciplinate da tali norme e per le quali il legislatore non le aveva previste ».

comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati » (art. 4, 1° co., lett. *a* cod. privacy). In via interpretativa di tali definizioni normative si è affermato da parte della giurisprudenza che sono ad esempio dati personali anche i dati relativi alla navigazione Internet ed ai siti visitati ¹⁰, e che è trattamento dei dati anche l'operazione consistente nel far comparire dati personali su una pagina Internet ¹¹, nonché la ricerca in modo automatizzato, costante e sistematico, di informazioni pubblicate su Internet da parte del gestore di un motore di ricerca allorché tali informazioni contengano dati personali ¹².

La disciplina seguita dagli operatori per il trattamento dei dati e per il loro trasferimento all'estero si trova definita nelle *privacy policy* che solitamente accedono alle condizioni di contratto relative ai servizi e/o prodotti da loro offerti. Le condizioni delle *privacy policy* possono essere contenute nei medesimi schemi contrattuali per lo scambio di beni o servizi oppure essere formulate come una serie di disposizioni autonome ¹³. Quest'ultimo caso si presta anche all'eventualità del trattamento dei dati che non si accompagna ad una fornitura di servizi o beni ma consegue

¹⁰ Secondo i giudici della High Court of Justice inglese, nel caso *Vidal-Hall, Hann, Bradshaw vs Google Inc.* (Case No: HQ13X03128), 16 gennaio 2014, i dati relativi alla navigazione Internet e i siti visitati sono qualificabili come dati personali. V. anche Court of Appeal UK, 27 marzo 2015, Case No: A2/2014/0403.

¹¹ Corte Giust. Ue, 1° ottobre 2015, C-230/14, *Weltimmo*, punto 37, e Corte Giust. Ue, 13 maggio 2014, C-131/12, *Google Spain*, punto 57, come aveva già affermato la Corte Giust. Ue, 6 novembre 2003, C-101/01, *Lindqvist*. Cfr. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. inf.*, IV-V/2015, p. 779-799.

¹² Corte Giust. Ue, 13 maggio 2014, C-131/12, *Google Spain*.

¹³ Si veda ad es. la *privacy policy* del sito amazon.it, cui si accede attraverso un link contenuto nelle condizioni di uso del sito (a loro volta in un documento intitolato "condizioni generali di uso e di vendita") presenti sul sito medesimo.

Nelle *privacy policy* — che nel trattamento transazionale dei dati personali sono soggette alla legge applicabile secondo le regole del diritto internazionale privato — è frequente individuare alcune disposizioni standard nelle quali il fornitore indica puntualmente quali dati verranno (o potranno

essere) raccolti, le operazioni che su di essi verranno (o potranno) essere effettuate, le finalità del trattamento, e così via, secondo quanto prevede, per il nostro ordinamento, l'art. 13 cod. privacy relativamente all'informativa sul trattamento dei dati che deve essere fornita all'interessato. Oltre a ciò che attiene alla stretta informativa, le *privacy policy* degli operatori includono di solito ulteriori diritti ed obbligazioni reciproche tra le parti come, ad esempio, disposizioni sulle modifiche della medesima *privacy policy*, usualmente introdotte dal fornitore, oppure garanzie di tutela relativamente all'eventuale trasferimento dei dati in Paesi terzi. Tra le altre disposizioni che è frequente rinvenire nelle *privacy policy* figura, ad esempio, quella che prevede il conferimento dei dati personali formulato in termini di facoltatività, accompagnata dall'avvertenza che qualora l'utente non aderisca all'informativa non potrà usufruire dei servizi e prodotti offerti, di modo che l'utente pare costretto a dare il proprio consenso al trattamento dei dati personali per poter accedere a quei servizi e/o prodotti (si tenga presente che l'art. 13, 1° co., lett. *b* cod. privacy prevede che l'interessato sia previamente informato circa « la natura obbligatoria o facoltativa del conferimento dei dati »). Una volta conferiti, i dati personali dell'utente potranno essere usati per svilup-

al semplice accesso ad un sito Internet ¹⁴. Le *privacy policy* possono presentare delle condizioni per il trattamento dei dati personali che seguono regole tipiche di un ordinamento di uno

pare nuovi servizi e prodotti oppure per personalizzare le esperienze dell'utente. In quest'ultimo caso vengono realizzate delle attività di profilazione, per le quali molti *service provider* stabiliscono di poter utilizzare i dati conferiti dagli utenti, ad esempio, a fini commerciali, di *marketing* e di *targeting* pubblicitario (si segnala nel contesto della conferenza annuale europea delle Autorità Garanti del maggio 2016 che il vero motore del sistema e il prossimo futuro delle attività di raccolta dei dati si sposta verso la profilazione degli utenti). In taluni casi è previsto che l'utente possa opporsi alla ricezione di annunci basati sui suoi interessi, mentre in altre *privacy policy* tale diritto non è esplicitato, né menzionato. Rispetto a tali attività l'art. 13, 1° co., lett. b cod. privacy prevede che l'interessato debba essere previamente informato circa « le finalità e le modalità del trattamento cui sono destinati i dati », e l'art. 3 cod. privacy prevede il principio di necessità nel trattamento dei dati, nel senso che « i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità ».

Quanto invece alle modalità di condivisione dei dati, l'art. 13, 1° co., lett. d cod. privacy prevede che l'interessato sia previamente informato circa « i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi ». Le più comuni *privacy policy* ne prevedono la comunicazione con il consenso dell'utente ovvero, in base alle esigenze, per completare transazioni o fornire un prodotto richiesto o autorizzato dall'utente. Ciò significa che tali dati potranno essere comunicati anche alle società affiliate e filiali controllate dal prestatore del servizio o a fornitori che lavorano per suo conto. Ancora, tali dati potranno essere condivisi se richiesto dalla legge o dall'autorità giudiziaria ovvero per mantenere la sicurezza dei prodotti e per proteggere i diritti o la proprietà del fornitore del servizio.

Conformemente a quanto prevede il nostro cod. privacy all'art. 7 le *privacy policy* prevedono alcuni diritti in capo all'utente,

come il diritto di accesso e controllo dei propri dati personali, i quali vengono solitamente conservati dal prestatore del servizio solo per il tempo necessario a perseguire le finalità indicate.

Una disposizione ricorrente nelle informative è poi quella concernente la sicurezza dei dati personali. In tal caso, le misure di sicurezza e i mezzi per la loro implementazione variano da fornitore a fornitore ma devono comunque rispettare un certo livello di idoneità e conformità. In relazione ai servizi o prodotti che presuppongono attività di geolocalizzazione, assumono rilevanza le disposizioni aventi ad oggetto il trattamento di dati personali come la posizione geografica. Data la peculiarità di tali dati, spesso ne viene privilegiato il trattamento in forma anonima.

Infine, un punto su cui le *privacy policy* sembrano differire tra loro è quello relativo alle modalità con cui vengono comunicate agli utenti le eventuali modifiche all'informativa. Taluni fornitori di servizi prevedono infatti la notifica diretta all'utente, mentre altri optano per la pubblicazione della modifica sul sito Internet. È evidente che la scelta dell'una o dell'altra modalità comporta un differente livello di protezione dell'utente, il quale, nel secondo caso, sarà tenuto a controllare regolarmente il sito del fornitore al fine di verificare eventuali cambiamenti dell'informativa. Ciò implica che, spesso, l'utente non sarà consapevole delle modifiche intervenute nelle *privacy policy* dei servizi o prodotti di cui fruisce e risulterà vincolato ad una informativa diversa rispetto quella originariamente sottoscritta o a lui portata a conoscenza. A tale riguardo si v. anche la nota seguente.

¹⁴ Si abbia presente che nel momento in cui le *privacy policy* prevedono il consenso all'utilizzo di dati personali, anche senza corrispettivo, e ad esempio le condizioni per la modifica della medesima *privacy policy*, introducono diritti ed obbligazioni e per questo possono essere guardate anche come clausole di un contratto, cfr. LOOS e LUZAK, *Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers*, in *Amsterdam Law School Legal Studies Research Paper*, No. 2015-01, p. 5. In quanto clausole contrattuali e clausole usualmente predisposte dall'operatore, esse — se utilizzate in contratti aventi come controparte un consumatore — sono suscettibili di sindacato di vessatorietà alla luce della disciplina delle clausole ves-

Stato terzo rispetto a quello del luogo ove raggiungono via Internet la persona interessata o, ancora, prevedono il trasferimento transfrontaliero dei dati, o comunque lo praticano ¹⁵. Non è sempre dato, così, che la *privacy policy* degli operatori rispetti le regole per il trattamento dei dati personali che l'interessato potrebbe attendersi di vedere applicate, come potrebbero essere quelle del luogo in cui egli ha la sua residenza, o in cui si trova nel momento in cui accede ad Internet, od ancora quelle della sua legge nazionale ¹⁶.

Secondo l'attuale disciplina di diritto internazionale privato relativa al trattamento dei dati personali, che si trova nell'art. 4, 1° co., lett. a della dir. 95/46, gli operatori sono chiamati a rispettare la legge del Paese di stabilimento del titolare del trat-

tamento nei contratti con il consumatore introdotta dalla dir. 93/13. Nel nostro cod. consumo (dove si trova ora la disciplina di attuazione della dir. 93/13) l'art. 33 lett. m) prevede tra l'altro che è clausola presuntivamente vessatoria la clausola che consente al professionista di modificare unilateralmente le clausole del contratto, ovvero le caratteristiche del prodotto o del servizio da fornire senza un giustificato motivo indicato nel contratto stesso (sulle modificazioni delle *privacy policy* v. *supra*, nota prec.). Si tenga presente inoltre che le clausole predisposte dalla parte professionale e inserite in un contratto con il consumatore devono essere redatte in modo chiaro e comprensibile, secondo le previsioni di cui all'art. 34, 2° co. e 35, 1° co. c. cons., pena la possibile nullità della clausola, oltre che l'interpretazione a sfavore dell'autore della clausola (art. 35, 2° co. c. cons.). A tale obbligo di trasparenza sono quindi soggette anche le clausole relative alla modifica delle condizioni di *privacy policy*. Si abbia inoltre presente che la pratica commerciale che induce o è idonea ad indurre in errore il consumatore medio sulla « portata degli impegni del professionista » è considerata ingannevole se lo induce o è idonea a indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso (art. 21, lett. c c. cons.). Si noti che il considerando n. 42 del nuovo Reg. 2016/679 recita ora in via espressa che « per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene. In conformità della dir. 93/13 (...)

è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e che non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio ». La natura contrattuale delle condizioni delle *privacy policy* è chiara nella prospettiva della sussunzione dell'intera area della regolazione della *privacy* nella disciplina dei contratti dei consumatori indicata da BEN-SHAHAR e STRAHILEVITZ, *Contracting over Privacy: Introduction*, in 45 *Journal of Legal Studies* S1, 2016, p. 51 ss.

¹⁵ Le *privacy policy* devono poi indicare espressamente se i dati oggetto di trattamento saranno trasferiti all'estero, ciò che avviene di regola nei contratti di *cloud computing*, specificando sulla base di quali situazioni di legittimità avviene il trasferimento. Si pensi che l'art. 13, lett. d cod. privacy prevede che debba essere indicato l'ambito di diffusione dei dati, oltre che i soggetti o categorie di soggetti a cui vengono comunicati i medesimi, ciò da cui si può desumere che è onere degli operatori indicare il trasferimento all'estero.

¹⁶ Quanto ai diritti della personalità la nostra legge di diritto internazionale privato, l. 218/1995 prevede all'art. 24 che « l'esistenza e il contenuto dei diritti della personalità sono regolati dalla legge nazionale del soggetto ». E che « le conseguenze della violazione dei diritti di cui al 1° co. sono regolate dalle legge applicabile alla responsabilità per fatti illeciti ».

tamento. Su tale criterio di collegamento sono intervenute importanti pronunce della Corte di Giustizia dell'Unione europea che fanno oggi da complemento interpretativo alla formulazione letterale della norma, come si vedrà al prossimo par. 2. Tale criterio è ad ogni modo destinato ad essere superato dalla previsione in materia del nuovo Regolamento europeo, come si vedrà più avanti nel par. 4.

Quanto in particolare al trasferimento dei dati verso Paesi terzi, la disciplina europea di cui alla dir. 95/46 prevede che il trasferimento dei dati personali « oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento » verso uno Stato terzo ¹⁷ « possa aver luogo soltanto se il Paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva » (art. 25, 1° co.). L'adeguatezza, che « è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati » ¹⁸, implica di per sé uno scostamento dallo standard europeo, ma richiede che il livello di protezione offra garanzie comparabili a quelle del modello europeo ¹⁹. Nel caso in cui la Commissione europea accerti che lo Stato terzo non garantisce un livello di protezione adeguato, gli Stati membri hanno l'obbligo di adottare le misure necessarie per impedire ogni trasferimento di dati della stessa natura (art. 25, 4° co.). L'art. 26 prevede tuttavia una serie di deroghe, tra le quali in primo luogo il consenso inequivocabile della persona interessata al trasferimento previsto (art. 26, 1° co., lett. a), ricorrendo le quali il trasferimento può avvenire anche

¹⁷ Relativamente alla nozione di trasferimento dei dati, la Corte di Giustizia ha precisato con la sentenza *Lindqvist* (Corte Giust. Ue, 3 novembre 2003, C-101/01) che non si configura un trasferimento di dati in un Paese terzo quando una persona che si trova in uno Stato membro inserisce in una pagina Internet dati personali, rendendoli così accessibili a chiunque si colleghi a Internet, compresi coloro che si trovano in Paesi terzi. Sentenza che sembra fondarsi sul timore di un'interpretazione estensiva della nozione di trasferimento, secondo cui si avrebbe un trasferimento verso un Paese terzo (vietato in principio dalla direttiva, se tale Paese non garantisce un livello di protezione adeguato) ogni qualvolta il dato sia caricato su Internet e sia quindi accessibile a chiunque in rete, anche se non trasferito direttamente da chi lo carica a chi vi accede. FOCARELLI, *op. cit.*, pp. 35 ss.

¹⁸ Diversamente, la circolazione dei dati nell'ambito dell'Unione europea è libera (come risulta dal medesimo titolo della dir. 95/46) e le disposizioni del cod. privacy

non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea (art. 42 cod. privacy). Viene tuttavia fatta salva l'adozione, in conformità allo stesso cod. privacy, di eventuali provvedimenti nel caso in cui i trasferimenti di dati siano effettuati al fine di eludere le disposizioni vigenti. « Si può immaginare il caso in cui il titolare trasferisca i dati in altro Stato dell'Unione europea al solo scopo di non applicare la normativa italiana più rigorosa, ad esempio, in materia di sicurezza dei dati ». Occorre comunque, perché il trasferimento sia effettivamente elusivo, che l'unica motivazione della scelta fatta sia appunto quella elusiva, in modo da realizzare la fattispecie dell'abuso del diritto. G. FINOCCHIARO, *Privacy e protezione dei dati personali*, Bologna, Zanichelli, 2012, p. 232.

¹⁹ MANTELERO, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per cittadini ed imprese?*, in *Contr. impr./Eur.*, II/2015, p. 721.

quando lo Stato terzo non garantisce una protezione adeguata ai sensi dell'art. 25, 2° co. Altre diverse alternative alla decisione di adeguatezza della Commissione europea consistono, come si vedrà più precisamente nel seguito del lavoro, al par. 3, nell'impiego di clausole contrattuali standard oppure nell'impiego di regole condivise nell'ambito del trasferimento di dati infragruppo di una medesima impresa. Tali previsioni saranno superate dalla disciplina del nuovo Regolamento che si esaminerà più avanti, che tuttavia non muta l'impostazione di fondo della materia fondata sul criterio dell'« adeguatezza ».

In questo momento le problematiche della definizione della legge applicabile al trattamento dei dati con portata transfrontaliera e delle condizioni cui sottoporre il trasferimento dei dati verso Paesi terzi è soggetta a particolari attenzioni rispetto ai rapporti tra i Paesi dell'Unione europea e gli USA, dato che lì hanno sede alcuni dei principali operatori di Internet del giorno d'oggi e, d'altro canto, il sistema giuridico statunitense si caratterizza per un diverso ed inferiore grado di tutela del diritto sui dati personali rispetto alla disciplina di matrice europea ²⁰. Si vedranno nel seguito del lavoro — al par. 3.1 — come si sono affrontate tali problematiche e si vedrà anche — al successivo par. 5 — come esse si prospettino non solo nei rapporti rotta Europa-USA, ma in un contesto più ampio di rapporti a livello internazionale, data la natura globale di Internet.

2. LE DECISIONI DELLA CORTE DI GIUSTIZIA UE, LA NOZIONE DI « STABILIMENTO » DEL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI E LA NOZIONE DI « TRATTAMENTO » DEI DATI PERSONALI DI CUI ALL'ART. 4 DIR. 95/46.

Più decisioni recenti della Corte di Giustizia dell'Unione europea si sono pronunciate sulle problematiche del trattamento transnazionale dei dati in via interpretativa dell'art. 4, 1° co., lett. *a* della dir. 95/46. In via di principio esse affermano di volersi attenere ad una forte tutela del diritto sui dati personali secondo la protezione ad esso data a livello fondamentale negli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, che vengono adottati quale base interpretativa della dir. 95/46 ²¹.

²⁰ Il trasferimento dei dati personali verso gli Stati Uniti è da sempre risultato problematico, appunto per via del differente grado di tutela lì assicurato ai dati personali rispetto all'elevato livello di protezione europeo. La protezione prevista dall'ordinamento statunitense appare infatti più labile rispetto alle dettagliate cautele previste dalla disciplina europea e ciò è il riflesso

di una diversa scala di valori tra i due ordinamenti. Sul confronto tre le normative dell'Unione europea e degli USA, ad es., P.M. SCHWARTZ, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, in *Harvard Law Rev.*, 2013, p. 1966 ss.

²¹ Affermano che le deroghe e le restrizioni alla tutela dei dati personali debbano operare nei limiti dello stretto necessa-

Mostrano inoltre di dare spazio nel proprio ragionamento ad un'interpretazione evolutiva della norma della dir. 95/46 seguendo la realtà attuale dei rapporti economici come si svolgono su Internet, che richiede l'allontanamento da rigorosi riferimenti territoriali per la determinazione della legge applicabile al trattamento dei dati personali.

La Corte di Giustizia perviene in definitiva al risultato di conferire una portata applicativa espansiva alla disciplina europea della tutela dei dati personali, affermando nella sentenza *Google Spain* che tanto risulta in particolare dai considerando da 18 a 20 e dall'art. 4 della dir. 95/46, attraverso i quali il legislatore dell'Unione ha inteso evitare che una persona venga esclusa dalla protezione garantita da tale direttiva e che tale protezione venga elusa (punto 54) ²². Non si può accettare — afferma la Corte nella medesima sentenza — che il trattamento dei dati personali effettuato per le esigenze del funzionamento del motore di ricerca in questione venga sottratto agli obblighi e alle garanzie previsti dalla dir. 95/46, ciò che pregiudicherebbe l'effetto utile di quest'ultima e la tutela efficace e completa delle libertà e dei diritti fondamentali delle persone che detta direttiva mira a garantire (punto 58) ²³.

Nel caso *Google Spain*, deciso nel 2014, era giunta all'attenzione della Corte l'attività della società *Google Spain*, avente sede in Spagna, ove essa realizzava la promozione e la vendita di spazi pubblicitari che la Corte individuava come parte essenziale dell'attività commerciale del gruppo *Google*. Tale attività era strettamente connessa a quella di *Google Search*, gestita e amministrata da *Google Inc.*, avente sede negli Stati Uniti. A tal proposito la Corte rilevava che non fosse contestato che *Google Spain* si dedicava all'esercizio effettivo e reale di un'attività mediante un'organizzazione stabile in Spagna e, essendo dotata di personalità giuridica propria, tale società costituiva una filiale di *Google Inc.* nel territorio spagnolo; e di conseguenza uno « stabilimento » ai sensi dell'art. 4, 1° co., lett. a della dir. 95/46 ²⁴. Affermava poi che il trattamento dei dati personali realizzato per

rio, Corte Giust. Ue, 8 aprile 2014, C-293/12, *Digital Rights Ireland*, punti 65 e 68; Corte Giust. Ue, 6 ottobre 2015, C-362/14, *Schrems*, punti 92, 93-94; Corte Giust. Ue, 11 dicembre 2014, C-212/13, *Rynes*, punto 28.

²² Corte Giust. Ue, 13 maggio 2014, C-131/12.

²³ Corte Giust. Ue, 13 maggio 2014, C-131/12, punti 54 e 58. Nella successiva sentenza *Weltimmo* la Corte afferma di nuovo a proposito dell'ambito applicativo della dir. 95/46 che « il legislatore dell'Unione ha

quindi previsto un ambito di applicazione territoriale della dir. 95/46 particolarmente esteso, che ha inserito nell'art. 4 della stessa » (punti 25 e 27).

²⁴ Il considerando n. 19 della dir. 95/46 recita che « lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile », ma che « la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo ».

esigenze di servizio di un motore come *Google Search*, gestito da un'impresa con sede in uno Stato terzo, ma avente uno stabilimento in uno Stato membro, si possa dire effettuato « nel contesto delle attività » di tale stabilimento, qualora quest'ultimo sia destinato a garantire in tale Stato membro la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo (punto 55). Infatti, in circostanze del genere, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio, essendo tale motore al tempo stesso lo strumento che consente lo svolgimento delle attività in questione (punto 56). Concludendo che l'art. 4, 1° co., lett. *a* non esige che il trattamento di dati personali in questione venga effettuato « dallo » stesso stabilimento interessato, bensì soltanto che venga effettuato, appunto, « nel contesto delle attività » di quest'ultimo, dirigendosi tra l'altro verso gli abitanti di detto Stato membro (punto 60).

Ha ritenuto inoltre la Corte che l'attività del motore di ricerca — consistente nella raccolta di dati attraverso l'esplorazione di Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni qui pubblicate che esso « estrae », « registra » e « organizza » successivamente nell'ambito dei suoi programmi di indicizzazione, « conserva » nei suoi *server* e eventualmente « comunica » e « mette a disposizione » dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche — realizza un « trattamento » dei dati secondo la disposizione dell'art. 2, lett. *b* della dir. 95/46 che contempla un tale genere di operazioni ²⁵. E che il motore di ricerca deve essere considerato il titolare di tale trattamento ai sensi dell'art. 2, lett. *d* della dir. (punto 33). È pacifico — osserva la Corte — che tale attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati in quanto li rende accessibili a qualsiasi utente di Internet che esegua una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina *web* su cui questi dati sono pubblicati (punto 36). Inoltre, l'organizzazione e l'aggregazione delle informazioni pubblicate su Internet da parte dei motori di ricerca al fine di

²⁵ Già nella sentenza *Lindqvist* la Corte Giust. Ue, 6 novembre 2003, C-101/01, aveva affermato che « l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, indicando

il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un trattamento di dati personali interamente o parzialmente automatizzato ai sensi dell'art. 3, n. 1 » della dir. 95/46.

facilitare ai loro utenti l'accesso a tali informazioni possono avere come effetto che tali utenti, quando la loro ricerca viene eseguita a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente di stabilire un profilo più o meno dettagliato di quest'ultima (punto 37). Pertanto l'attività di un motore di ricerca può incidere in modo significativo sui diritti fondamentali alla vita privata e alla protezione dei dati personali, in aggiunta all'attività degli editori dei siti *web*, e per questo il gestore del motore di ricerca deve assicurare che detta attività soddisfi le prescrizioni della dir. 95/46 affinché possa essere realizzata una tutela efficace e completa delle persone interessate, in particolare del diritto al rispetto della loro vita privata ²⁶. Infine, la Corte si esprime nel senso che la « visualizzazione stessa di dati personali su una pagina di risultati di una ricerca costituisce un trattamento di dati personali » (punto 57).

La Corte di Giustizia è ritornata sulla definizione del termine « stabilimento » nel caso *Weltimmo* deciso nel 2015 per affermare che l'art. 4, 1° co., lett. *a* consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il titolare del trattamento di tali dati è registrato purché quest'ultimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale realizza tale trattamento. Nel caso di specie la società *Weltimmo*, registrata in Slovenia, gestiva siti Internet aventi ad oggetto annunci immobiliari relativi ad immobili situati in Ungheria e redatti nella lingua di quest'ultimo Paese, e per la raccolta dei dati personali degli inserzionisti le era stata indirizzata una sanzione dalla Autorità Garante ungherese ²⁷.

In tale caso, in cui la controversia aveva ad oggetto la determinazione di quale tra due legislazioni degli Stati membri fosse

²⁶ Vista la gravità potenziale di tale ingerenza, essa non può essere giustificata dal semplice interesse economico del gestore.

²⁷ Gli annunci immobiliari erano gratuiti per un mese, dopo di che divenivano a pagamento. Allo scadere del periodo gratuito molti inserzionisti avevano inviato un messaggio di posta elettronica per chiedere la cancellazione dei propri annunci e dei propri dati personali. La *Weltimmo* però non aveva cancellato tali dati e aveva fatturato i servizi forniti e, a fronte del mancato pagamento della fatture, aveva trasmesso i dati personali degli inserzionisti ad alcune agenzie di recupero crediti. L'autorità na-

zionale ungherese incaricata della protezione dei dati e della libertà dell'informazione era intervenuta a seguito dei reclami presentati dagli inserzionisti.

Quanto agli elementi che occorre valutare per individuare la legge applicabile ricorrono — secondo quanto afferma la Corte — sia il grado di stabilità dell'organizzazione, sia l'esercizio effettivo delle attività in tale Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione, ciò che vale soprattutto per le imprese che offrono servizi esclusivamente tramite Internet. Si possono tenere nel conto, inoltre, sia il fatto che l'attività del respon-

applicabile — nelle specie slovena o ungherese — in base allo Stato in cui il trattamento era avvenuto, la Corte sottolinea di nuovo, come già in *Google Spain* ²⁸, che l'art. 4, 1° co., lett. a dir. 95/46 « non esige che il trattamento di dati personali in questione venga effettuato “dallo” stesso stabilimento interessato, bensì soltanto che venga effettuato “nel contesto delle attività” di quest'ultimo » ²⁹, ciò che conduce al « l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile (n.d.a. leggasi: titolare) del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge il trattamento ». Ne consegue, come aveva rilevato l'Avvocato generale nelle sue conclusioni (ai punti 28 e 32-34), una concezione flessibile della nozione di stabilimento che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata.

Da sottolineare è che il luogo verso cui l'attività è rivolta è anch'esso, in via interpretativa, elemento rilevante ai fini dell'individuazione della legge protettiva del diritto sui dati personali applicabile in maniera conforme all'impostazione della disciplina europea dei dati personali, volta ad assicurare quanto più possibile la tutela degli interessati (punto 41). Si è osservato che tutto ciò è tra l'altro coerente con l'impostazione di altre discipline normative dell'Unione europea a regolazione delle attività telematiche. Il considerando n. 19 della dir. 2000/31/CE sul commercio elettronico afferma infatti che il luogo di stabilimento per le società che forniscono servizi tramite siti Internet non è là dove si trova la tecnologia di supporto del sito, né dove esso è accessibile, bensì il luogo in cui dette società svolgono la loro attività economica ³⁰.

Nella successiva sentenza *Amazon* del 2016 tale principio del luogo verso cui è diretta l'attività dell'operatore per la definizione della legge applicabile, già pronunciato nelle sentenze *Google Spain* e *Weltimmo*, è ancor più messo in rilievo quale argomento

sabile di detto trattamento è principalmente — ovvero interamente — rivolta verso tale Stato membro, in quanto consiste nella gestione di siti Internet di annunci immobiliari riguardanti beni immobili situati nel territorio di tale Stato membro, redatti nella lingua di quest'ultimo, sia, d'altro canto, la circostanza che tale responsabile ha un rappresentante in detto Stato membro (punti 29-31).

²⁸ Punto 52 della decisione, rispetto alle attività realizzate da *Google Spain* in territorio spagnolo.

²⁹ Relativamente al significato dell'espressione « nel contesto delle attività di uno stabilimento » afferma che essa « non può ricevere un'interpretazione restrittiva ».

³⁰ Conclusioni dell'Avvocato generale di *Weltimmo*, FINOCCHIARO, *op. cit.*, p. 790.

principale della decisione ³¹. La Corte di Giustizia afferma che l'art. 4, 1° co., lett. *a* della dir. 95/46 dev'essere interpretato nel senso che il trattamento dei dati personali eseguito da un'impresa del commercio elettronico sia disciplinato dal diritto dello Stato membro verso il quale detta impresa dirige le proprie attività, qualora sia accertato che tale impresa operi il trattamento dei dati in esame nel contesto delle attività di uno stabilimento situato in detto Stato membro. Il caso si pronuncia sullo schema di contratto per il commercio elettronico della società Amazon EU (con sede in Lussemburgo ed appartenente ad un gruppo internazionale) rispetto alle attività svolte attraverso il sito Internet con dominio amazon.de, e rivolte anche a consumatori residenti in Austria, con riguardo ai profili inerenti alla *privacy*, alle clausole del trattamento dei dati al fine del recupero crediti e ad altri fini, ed alla determinazione della legge applicabile, definita come quella lussemburghese.

A proposito della nozione di « stabilimento » la Corte ripete, in linea con le conclusioni dell'Avvocato generale (par. 119) e come già affermato nel caso *Weltimmo*, che, sebbene l'impresa titolare del trattamento non possieda né filiali né succursali in uno Stato membro, ciò non esclude che essa possa ivi possedere uno stabilimento ai sensi dell'articolo sopra detto (punto 79), e che la nozione di stabilimento si estenda a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile (punto 75, richiamando la decisione *Weltimmo*, punto 31) ³². Mentre, d'altra parte, uno stabilimento non può esistere per il semplice fatto che ivi sia accessibile il sito Internet dell'impresa in questione (punto 76), e che occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività nello Stato membro interessato (punto 77, che richiama la decisione *Weltimmo*, punto 29). Allo stesso tempo, come già affermato in precedenza, la Corte ripete che non occorre che il trattamento dei dati personali in questione venga effettuato « dallo » stabilimento interessato stesso, bensì soltanto « nel contesto delle attività » di quest'ultimo ³³.

Allo stesso modo che nella decisione *Weltimmo*, e prima ancora nella decisione *Google Spain*, la Corte — come detto sopra — mette l'accento sul luogo verso il quale è diretta l'attività dell'operatore per farne derivare la determinazione del diritto applicabile. Con ciò si apre la possibilità di associare alla tutela dei dati

³¹ Corte Giust. Ue, 28 luglio 2016, C-191/15, *Verein für Konsumenteninformation c. Amazon EU*.

³² Per il caso di specie la Corte ha rimandato al giudice del rinvio la determinazione di quale legge sia applicabile al

trattamento dei dati personali, se eventualmente quella tedesca.

³³ Corte Giust. Ue, 28 luglio 2016, C-191/15, punto 78, che richiama Corte Giust. Ue, 1° ottobre 2015, C-230/14, punto 35.

personali del consumatore parte di un contratto di fornitura di beni e servizi secondo la disciplina di tutela dei dati personali del suo Paese di residenza (se ed in quanto in tale Paese l'operatore esegua il trattamento dei dati nel contesto delle sue attività) ³⁴ la disciplina del contratto secondo le norme imperative di regolazione del contratto del consumatore del suo Paese di residenza, così come prevede il Regolamento Roma I al suo art. 6, 2° co., se il consumatore venga qui "raggiunto" dall'operatore commerciale attraverso lo svolgimento delle sue attività ³⁵.

In conclusione, dalle decisioni della Corte di Giustizia emergono diverse linee interpretative dell'art. 4, 1° co., lett. a della dir. 95/46 che si concentrano sia sulla nozione di stabilimento che sulla nozione di trattamento dei dati, con i seguenti profili di rilevanza applicativa. Quanto alla nozione di « stabilimento », una sua

³⁴ M. MÜLLER, *Amazon and Data Protection Law - The end of the private-Public Divide in EU conflict of laws?*, in *EuCML*, 2016, p. 218, rileva che sfortunatamente la Corte di Giustizia rimane in silenzio sulla relazione tra la direttiva sulla protezione dei dati personali e il Reg. Roma I, non citando nemmeno l'art. 23 di quest'ultimo, che è dedicato alle relazioni con altre disposizioni del diritto comunitario, prevedendo che « il presente regolamento non pregiudica l'applicazione delle disposizioni dell'ordinamento comunitario che, con riferimento a settori specifici, disciplinino i conflitti di legge in materia di obbligazioni contrattuali ».

³⁵ Si tratta dell'art. 6, 2° co. del Reg. Roma I che prevede che al consumatore sia in ogni caso assicurata — anche di fronte alla determinazione nel contratto di una diversa legge applicabile — l'applicazione delle norme imperative della legge del suo Paese di residenza qualora l'operatore professionale persegua la sua attività professionale nel Paese in cui il consumatore ha la sua residenza abituale, o in qualsiasi modo diriga le sue attività verso quel Paese, o più Paesi incluso quello; ed è da precisare che il modo di intendere tali circostanze pare si vada ampliando. Ai quesiti interpretativi a proposito di quando un'attività si possa definire "diretta" verso un determinato Paese, si è per esempio risposto che svolgere attività di *marketing* integra il requisito dell'attività "diretta", ma che la semplice accessibilità del sito dal Paese di residenza abituale del consumatore non integra tale requisito. L'art. 15 del Reg. Bruxelles I lascia privo di definizione il concetto di attività "dirette" (il Reg. Roma I richiede il coordinamento tra Roma I e Bruxelles I), che si trova invece nel considerando n. 24 del Reg.

Roma I che pure, tuttavia, non assicura chiarezza. Di ausilio è la sentenza della Corte Giust. Ue, 7 dicembre 2010, cause C-585/08 e C-144/09, che individua una serie di parametri in base ai quali il giudice può accertare che l'attività sia definibile come "diretta" ed afferma che l'operatore commerciale deve aver manifestato la sua intenzione di stabilire una relazione commerciale con i consumatori di uno o più Stati membri, incluso quello del domicilio del consumatore, avendo l'obiettivo di concludere un contratto con tali consumatori (parr. 75-76 della sentenza). A riguardo REICH, *EU Strategies in Finding the Optimal Consumer Law Instrument*, in *Eur. Rev. Contr. Law.*, 2012, p. 18 ss. Degna di nota la decisione della Corte Giust. Ue, 6 settembre 2012, causa C-190/11, relativa ad una questione interpretativa dell'art. 15, 1° co., lett. c Reg. Bruxelles I, che riferisce del procedimento svoltosi in Austria precedentemente al rinvio pregiudiziale e così l'affermazione del giudice austriaco — alla luce della decisione della Corte Giust. Ue nelle cause C-585/08 e C-144/09 — secondo la quale si può ritenere che l'operatore commerciale abbia diretto la sua attività verso il Paese del consumatore se il suo sito Internet sia consultabile dal Paese membro del consumatore e vi siano stati contatti a distanza tra le parti per telefono e per posta elettronica (punto 21).

Nella sentenza *Amazon* la Corte Giust. Ue si sofferma anche sulla clausola di individuazione della legge applicabile, per specificare che essa è soggetta al sindacato di vessatorietà innanzitutto sotto il profilo della sua trasparenza (richiamando il suo precedente del 23 aprile 2015, C-96/14, *Van Hove*, in cui ha chiarito che la trasparenza è da intendere a questo proposito in modo esten-

nozione svincolata dal contesto territoriale della registrazione dell'operatore in un determinato Stato membro, e legata al luogo dello svolgimento effettivo delle attività dell'operatore o alla presenza di un rappresentante; e una sua nozione che ricomprende non soltanto le operazioni svolte direttamente dall'operatore, ma anche le operazioni che si svolgono « nel contesto » delle attività dell'operatore; che tiene conto anche della loro natura di attività che vengono realizzate tramite Internet; che tiene conto anche del luogo verso il quale si indirizzano le attività, se sia quello di uno Stato membro e di quale Stato membro, e in quest'ottica della lingua nella quale si svolgono. Quanto alla nozione di « trattamento » dei dati, una sua nozione che considera trattamento dei dati l'attività del motore di ricerca consistente nella raccolta di dati attraverso l'esplorazione di Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni qui pubblicate, e la « visualizzazione stessa di dati personali su una pagina di risultati di una ricerca ». Ne consegue in definitiva un rafforzamento della portata protettiva del diritto sui propri dati personali della disciplina europea di cui alla dir. 95/46 ed un ampliamento della sua portata applicativa.

2.1. *L'attuazione delle decisioni della Corte di Giustizia all'interno degli Stati membri, e oltre.*

La giurisprudenza della Corte di Giustizia pare esser stata recepita da parte delle autorità nazionali degli Stati membri, tanto da parte delle autorità giurisdizionali, quanto delle Autorità Garanti del trattamento dei dati personali.

Una decisione della *Court of Appeal* inglese ³⁶ ha affermato la responsabilità della società informatica *Google Inc.*, con sede negli Stati Uniti, per l'illecito utilizzo dei dati personali degli utenti (*misuse of private information*), che risultava fossero stati raccolti senza il loro consenso né la loro consapevolezza attraverso il *browser* Safari grazie ad un sistema di *cookie*. Le c.d. *Browser Generated Information* venivano quindi aggregate e trasmesse da *Google* ai suoi *advertiser* che potevano in questo modo selezionare e far visualizzare sui dispositivi le pubblicità e

sivo). La Corte ha anche affermato che qualora gli effetti di una clausola siano determinati da disposizioni imperative di legge è essenziale che il professionista informi il consumatore relativamente alla ricorrenza di tali disposizioni (decisione del 26 aprile 2012, C-472/10, *Invitel*), ciò che corrisponde a conferire efficacia e — per altro verso — a contrastare l'elusione della previsione dell'art. 6, 2° co. Reg. Roma I, ai sensi del quale la scelta della legge applica-

bile non può valere a privare il consumatore della protezione assicuratagli dalle disposizioni alle quali non è permesso derogare convenzionalmente ai sensi della legge che sarebbe applicabile in mancanza di scelta (punto 69).

³⁶ Court of Appeal inglese, *Google Inc. vs Vidal-Hall, Hann, Bradshaw* (Case No: A2/2014/0403), 27 marzo 2015, che ha confermato la decisione di primo grado.

gli annunci più aderenti al profilo degli utenti. Ritenuto configurabile il reato di *misuse of private information* come autonoma categoria di *tort* ³⁷, il giudice di primo grado ha affermato la risarcibilità del danno da esso derivante, anche se non connesso ad alcuna effettiva perdita in termini economici. La pronuncia è di rilievo in quanto la *Court of Appeal* ha seguito da vicino le previsioni della dir. 95/46, mentre la legge di attuazione inglese non recepiva fedelmente le disposizioni della normativa europea.

Un'interessante pronuncia della Corte d'Appello di New York del 14 luglio 2016 corrisponde nella sostanza ad un recepimento della posizione della Corte di Giustizia europea. Con la decisione sul caso 14-2985, *Microsoft v. United States*, la Corte d'Appello di New York accoglie la posizione della società *Microsoft Corporation*, con sede a Washington, contro il Governo degli Stati Uniti, affermando che tale società non è tenuta a rivelare i dati degli *account* e-mail, conservati su un *server* europeo, relativi al servizio di posta elettronica che offre gratuitamente ai propri utenti ³⁸. A seguito della citazione in giudizio di *Microsoft* da parte del Governo per non aver ottemperato ad un ordine di *disclosure* emanato nell'ambito della finalità di repressione dei reati (si sospettava che l'*account* e-mail fosse impiegato per il traffico di narcotici), i giudici d'appello hanno riconosciuto l'inapplicabilità della normativa americana al di fuori dei confini degli Stati Uniti, ritenendo appunto legittimo il rifiuto di *Microsoft* opposto a tutela degli interessi di riservatezza dei propri utenti. La Corte americana ha fondato la propria decisione sullo *Stored Communications Act* introdotto nel 1986 nell'ambito dell'*Electronic Communications Privacy Act* (ECPA) per estendere la tutela della riservatezza, prevista dal quarto emendamento della Costituzione americana, anche alle comunicazioni elettroniche. La decisione è stata inoltre basata sui precedenti orientamenti giurisprudenziali consolidati in relazione all'extraterritorialità dello *Stored Com-*

³⁷ La Corte d'Appello inglese confermava la decisione del giudice della *High Court of Justice* che aveva ritenuto competente l'autorità giudiziaria inglese (uno degli argomenti dell'appello da parte di *Google* era appunto l'incompetenza giurisdizionale delle corti inglesi a decidere la controversia, oltre all'errata configurazione del reato di cui veniva accusato e della conseguente risarcibilità del danno morale da esso derivante). La *Court of Appeal* rilevava che una delle condizioni perché venisse decisa in Inghilterra una controversia relativa ad un soggetto domiciliato, residente o con sede all'estero consisteva nella circostanza che il danno derivante da un dato comportamento illecito fosse patito all'interno della giurisdizione inglese.

Qualificando il *misuse of private information* alla stregua di un illecito civile, la Corte autorizzava a che la causa potesse essere trattata dinanzi all'autorità inglese, incrementando con ciò le possibilità di ricorso per i privati cittadini che, diversamente, sarebbero stati scoraggiati dal dover ricorrere all'autorità giudiziaria in un Paese straniero.

³⁸ *Microsoft* conserva il contenuto della corrispondenza e i dati tecnici relativi agli *account* e-mail (c.d. *non-content information*) in diversi *datacenter*, collocati di solito nel luogo di stabilimento dell'utente. Uno di tali *datacenter* si trova in Irlanda, dove opera un impianto secondario di *Microsoft* che memorizza i dati relativi agli *account* di quel luogo.

munications Act e ha affermato che l'applicazione extraterritoriale della disciplina avrebbe dovuto essere espressamente prevista, tenuto conto anche dell'ulteriore circostanza che l'obiettivo principale di tale normativa è la tutela della riservatezza degli utenti, ed eccezioni che limitino la protezione della loro sfera personale si collocano in antitesi con tale obiettivo.

Nella diffusione delle decisioni della Corte di Giustizia stanno svolgendo un ruolo fondamentale anche le Autorità Garanti dei Paesi membri che hanno adottato i primi provvedimenti in materia nei confronti di importanti società di gestione di servizi *web* ³⁹. L'Autorità Garante della *privacy* italiana ha adottato un provvedimento nei confronti di *Facebook Ireland* ordinando alla società di mantenere una condotta idonea a consentire il corretto esercizio dei diritti dell'interessato di cui gli artt. 7 e 8 cod. *privacy* ⁴⁰. Quanto al quesito sulla competenza e sulla legge applicabile rispetto ad una società avente sede negli Stati Uniti ed una sede europea in Irlanda ⁴¹, di rilievo prioritario per la soluzione del caso, il Garante ha osservato che *Facebook* è presente anche in Italia con un'organizzazione stabile, *Facebook Italy*, e che le attività di quest'ultima sono « inestricabilmente connesse » con la sede irlandese. Sulla scorta delle decisioni della Corte di Giustizia europea su casi analoghi, e in particolare la sentenza *Weltimmo*, il Garante ha deciso di esaminare il ricorso e di accoglierlo. Peraltro, già prima della sentenza *Schrems* dell'ottobre 2015 ⁴², il Garante italiano rivestiva un ruolo particolarmente attivo nel controllo del trattamento dei dati personali effettuato dai *service provider*. Con il provvedimento del 10 luglio 2014 nei confronti di *Google Inc.* il Garante aveva prescritto alla società di rendere l'informativa conforme ai principi del codice della *privacy* e di implementare misure idonee, da un lato, ad acquisire il preventivo consenso degli utenti anche non autenticati e, dall'altro, a consentire il corretto esercizio dei diritti degli utenti (in particolare, quello di richiedere la disattivazione e la sospensione della raccolta dei dati per la cronologia delle ricerche, della localizzazione, nonché per l'attività vocale e audio e quello di cancellare i dati personali dell'utente autenticato entro tempistiche determinate). Con un comunicato stampa del 29 luglio 2016 il Garante ha reso noto l'adempimento di *Google* rispetto agli impegni presi con tale Autorità, affermando di proseguire le verifiche ove necessario.

³⁹ I poteri di controllo delle Autorità Garanti sono stati tra l'altro riconosciuti e ribaditi dalla sentenza *Schrems*, punti 40-43.

⁴⁰ Autorità Garante Prot. dati personali, provvedimento 11 febbraio 2016, n. 56.

⁴¹ La sede operativa europea di *Facebook* presso la quale sono trattati i dati dei profili è quella irlandese.

⁴² Da cui è risultato invalidato l'accordo di *Safe Harbour*, come si vedrà *infra*, par. 3.1.

Anche l'Autorità Garante francese CNIL (*Commission Nationale de l'Informatique et des Libertés*) è intervenuta nei confronti di *Microsoft Corporation*, accusata di effettuare un'eccessiva attività di raccolta di dati non necessari attraverso il servizio di telemetria ⁴³. Nella stessa occasione l'Autorità ha rilevato ulteriori condotte non conformi alla normativa in materia di protezione dei dati personali tra cui un insufficiente sistema di sicurezza circa l'autenticazione al sistema operativo Windows 10, la mancata acquisizione del consenso preventivo al trattamento di dati personali con finalità di *advertising* e la mancata informativa circa l'utilizzo di *cookie*. Il Garante francese ha dunque concesso alla società di informatica un termine di tre mesi per conformarsi alla normativa in materia di protezione dei dati personali, sollecitando in particolare l'aggiornamento dell'informativa sulla *privacy* che relativamente al trasferimento dei dati personali fa ancora riferimento all'ormai invalidato regime dell'accordo di *Safe Harbour* ⁴⁴.

3. IL TRASFERIMENTO TRANSFRONTALIERO DEI DATI PERSONALI NELLA DISCIPLINA DELLA DIR. 95/46.

Come si è detto sopra nel par. 1, il trasferimento transnazionale dei dati dai Paesi membri dell'Unione europea verso Paesi terzi può avvenire seguendo la disciplina di cui agli artt. 25 e 26 della dir. 95/46 così come attuata negli ordinamenti degli Stati membri, la quale sarà superata dagli artt. 44-50 del nuovo Reg. 2016/679, che non ne mutano tuttavia i principi fondamentali.

L'attuale disciplina europea per il trasferimento dei dati personali dai Paesi membri dell'Unione europea verso Paesi terzi di cui alla dir. 95/46 si basa principalmente sulla ricorrenza di decisioni della Commissione europea, di cui all'art. 25, 6° co. della dir., che affermino che il livello di protezione dei dati personali da parte della disciplina dello Stato terzo è adeguato rispetto a quello garantito dalla disciplina europea ⁴⁵. « La Commissione può constatare (...) che un Paese terzo garantisce un livello di protezione adeguato ai sensi del par. 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (...) ai fini della tutela della vita

⁴³ Il provvedimento dell'Autorità francese relativo al procedimento di verifica nei confronti di *Microsoft Corporation*, Décision n. 2016-058 del 30 giugno 2016, è consultabile al seguente link: <https://www.cnil.fr/fr/windows-10-la-cnil-met-publiquement-en-demeure-microsoft-corporation-de-se-conformer-dans-un-delai>.

⁴⁴ Su cui si v. *infra*, par. 3.1.

⁴⁵ Le decisioni di adeguatezza sinora emesse sono relative ai seguenti Paesi: Andorra, Argentina, Australia (solo in relazione ai dati del codice di prenotazione, c.d. *Passenger Name Record*), Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA.

privata o delle libertà e dei diritti fondamentali della persona ». L'adeguatezza del livello di protezione garantito da un Paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati, ed in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il Paese d'origine e il Paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel Paese di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate (art. 25, 2° co. dir. 95/46). Come conseguenza della valutazione di adeguatezza risulterà possibile trasferire i dati personali in tale Paese terzo. Più nel dettaglio, l'art. 44 lett. *b* del nostro cod. privacy prevede che il trasferimento dei dati all'estero è autorizzato dal Garante del Paese da cui i dati provengono, sulla base delle decisioni di adeguatezza del livello di protezione garantito dal Paese destinatario assunte dalla Commissione europea secondo la previsione di cui all'art. 25, 6° co. della direttiva.

In deroga alla richiesta ricorrenza del requisito dell'“adeguatezza” del livello di protezione dei dati personali nel Paese terzo, l'art. 26 dir. 95/46 prevede che il trasferimento di dati personali verso un Paese terzo possa diversamente avvenire a condizione che: la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto; il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto tra la persona interessata e il titolare del trattamento, o nell'interesse della persona interessata tra il titolare del trattamento ed un terzo; il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante; sia necessario per la salvaguardia dell'interesse vitale della persona interessata; oppure il trasferimento avvenga a partire da un registro pubblico (art. 26, 1° co. dir. 95/46 e art. 43 cod. privacy, che attua la previsione della dir., in maniera non identica). È da notare, quindi, che l'operatore del Paese terzo potrebbe comunque conseguire il trasferimento dei dati personali degli utenti qualora si tratti dei dati necessari, ad esempio, per la conclusione o l'esecuzione del contratto, come il nome e l'indirizzo dell'acquirente. Non si potrebbe invece, allo stesso modo, realizzare il trasferimento dei dati personali in deroga alla ricorrenza del requisito dell'adeguatezza se l'obiettivo sia raccogliere altri dati del cliente ulteriori a quelli indispensabili per l'esecuzione del contratto, ad esempio gusti e preferenze del cliente ai fini della sua profilazione. In base alla medesima previsione dell'art. 26, 1° co. dir. 95/46, tali dati potrebbero comunque sempre essere raccolti e trasferiti all'operatore del Paese terzo, a prescindere da una decisione che attesti l'adeguatezza della disciplina del Paese terzo,

in base ad un inequivoco specifico consenso della persona interessata ⁴⁶.

Secondo la previsione dell'art. 26, 2° co. della dir. 95/46, uno Stato membro può inoltre autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un Paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'art. 25, 2° co. qualora il titolare del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, garanzie che possono segnatamente risultare da clausole contrattuali appropriate. Secondo l'art. 26, 4° co. qualora la Commissione decida che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui al 2° co. gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione (così l'art. 44, lett. b cod. privacy). Le *Standard Contractual Clauses* costituiscono quindi uno strumento negoziale attraverso cui le parti, tra le quali avviene il flusso di dati, si accordano affinché il *data importer* si impegni a garantire un livello adeguato di protezione dei dati personali. Tali clausole sono soggette al riconoscimento della Commissione che con una sua decisione attesti la loro idoneità ad offrire le garanzie sufficienti di cui al 2° co. dell'art. 26 dir. 95/46 (art. 26, 4° co.) ⁴⁷. Per il caso in cui le clausole adottate non abbiano avuto l'approvazione della Commissione, possono diversamente essere approvate dalle Autorità Garanti nazionali clausole che prevedano l'impegno del *data importer* nel senso suddetto (art. 26, 2° co.).

Altro strumento fondato sull'autonomia negoziale sono le *Binding Corporate Rules* che non sono clausole approvate dalla Commissione europea, bensì clausole vincolanti per tutte le società appartenenti ad uno stesso gruppo, elaborate dall'impresa capogruppo secondo lo schema delineato dal Gruppo Art. 29 ⁴⁸ per regolare il flusso dei dati nei trasferimenti infragruppo tra le diverse società ⁴⁹. Lo strumento delle *Binding Corporate Rules* si

⁴⁶ Cfr. G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., p. 286.

⁴⁷ La Commissione europea ha adottato una nuova decisione il 5 febbraio 2010, n. 2010/87 (la precedente era del 2001) relativa alle clausole contrattuali tipo il cui inserimento in un contratto viene considerato garanzia sufficiente per poter effettuare il trasferimento verso Paesi terzi, sebbene questi ultimi non garantiscano un adeguato livello di protezione dei dati personali trasferiti. Successivamente il Garante ha pubblicato l'autorizzazione ai trasferimenti dei dati personali verso Paesi non appartenenti all'Unione europea che siano posti in essere in conformità alle clausole contrat-

tuali tipo di cui a tale decisione. G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., p. 284 e nota 335.

⁴⁸ Si vedano i documenti di lavoro del Gruppo di Garanti europei WP 74 del 2003 <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1609361> e WP 153 del 2008 <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1619530>.

⁴⁹ Viene indicato come tipico il caso della banca dati sulle risorse umane collocata in un Paese extraeuropeo che elabori i dati dei dipendenti e collaboratori dislocati nelle molteplici sedi dell'impresa nel mondo,

basa su un sistema di mutuo riconoscimento delle decisioni convenuto fra un numero rilevante di Garanti, cui ha aderito anche il Garante italiano ⁵⁰.

3.1. *In particolare: l'intervento della Corte di Giustizia Ue con la sentenza il Privacy Shield per il trasferimento dei dati negli Stati Uniti e i rapporti con gli operatori statunitensi.*

Come si è detto sopra, un particolare rilievo riveste il trasferimento transnazionale dei dati nei rapporti Europa-USA per ragioni legate all'importanza degli operatori *online* aventi sede negli Stati Uniti. Con una decisione di adeguatezza del 2000 la Commissione europea aveva "ratificato" il c.d. accordo di *Safe Harbour* ⁵¹ che regolava i rapporti tra Europa e Stati Uniti nell'ambito del trattamento dei dati personali, riconoscendo come legittimi e consentendo liberamente i trasferimenti di dati tra Paesi membri dell'Unione europea e gli USA. Tale accordo rappresentava una posizione di compromesso con l'impostazione della tutela della *privacy* nella disciplina normativa degli USA — meno protettiva di quella europea — che trovava nei fatti le sue ragioni negli interessi commerciali, grazie ai quali si erano fatte speciali concessioni alle imprese statunitensi ⁵².

La decisione della Commissione che aveva riconosciuto l'accordo di *Safe Harbour* sul flusso transfrontaliero dei dati tra

G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., p. 287.

Per approfondimenti sui meccanismi di garanzia alternativi alle decisioni di adeguatezza, si vedano G. RICCIO, *Model contract clauses e corporate binding rules: valide alternative al Safe Harbor Agreement?*, e MANTELERO, *Il trattamento dati nelle imprese nel post "Safe Harbour"*, *Strategie di breve, medio e lungo periodo*, in *Dir. inf.*, IV-V/2015, rispettivamente pp. 865-885 e 887-908; PALLARO, *Rapporti commerciali tra UE e Stati terzi e la questione della tutela dei dati personali. Il difficile confronto UE-USA*, in *Dir. comm. internaz.*, III/2000, pp. 753-788.

⁵⁰ V. il documento "Trasferimento di dati personali relativi ai dipendenti e alla clientela verso Paesi non appartenenti all'UE mediante BCR: provvedimento di autorizzazione nazionale", 8 aprile 2010. G. FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., pp. 288-289.

⁵¹ Decisione della Commissione Ue n. 2000/520, 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "Domande più frequenti"

(FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

⁵² « Il *Safe Harbour* è nato come un accordo politico ed economico, in cui l'Unione europea ha accettato un compromesso in materia di *data protection* che non ha eguali nelle relazioni con i Paesi terzi », MANTELERO, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per cittadini ed imprese?*, cit., p. 720. Esso è frutto di un negoziato tra la Commissione europea e il *Department of Commerce* statunitense condotto tra la fine del 1998 e il 2000, ed è di fatto l'accettazione ad opera dell'Unione europea di un indebolimento della propria posizione sul principio di adeguatezza, attraverso un approccio del tutto eccezionale in favore delle imprese statunitensi che non ha pari nei rapporti con gli altri Paesi terzi. L'adesione delle imprese ai principi di *Safe Harbour* avveniva su base volontaria e attraverso una forma di autocertificazione, prevedendosi appropriati meccanismi di controllo e di *enforcement* a garanzia del rispetto di una protezione « adeguata » (p. 722). Rispetto al concreto operare di questi ultimi si v. tuttavia *infra*, ult. par.

Unione europea e Stati Uniti, ritenendo « adeguato » alla luce dell'art. 25 della dir. 96/45 il livello di protezione garantito dalla disciplina degli USA, è stata invalidata dalla Corte di Giustizia dell'Unione europea con la decisione *Schrems* dell'ottobre del 2015⁵³. Dall'epoca degli accordi di *Safe Harbour* era nel frattempo accaduto che il modello europeo fosse andato progressivamente affermandosi mentre, per altro verso, si fossero sperimentate prassi statunitensi di sorveglianza di massa sui dati personali⁵⁴.

La decisione *Schrems* ha stabilito che il trattamento posto in essere dalle autorità statunitensi per i fini di sicurezza nazionale violava i principi di necessità e proporzionalità cui è soggetto il trattamento dei dati nella disciplina europea, e che gli interessati dal trattamento dei dati non godevano di tutela amministrativa o giudiziaria quanto ai diritti inerenti al trattamento dei loro dati⁵⁵. Essa ha prodotto come conseguenza che venisse meno la base legale adatta a legittimare il trasferimento dei dati verso gli USA lasciando operare quale regime interinale, nelle more del raggiungimento di un nuovo accordo tra l'Unione europea e gli USA⁵⁶ — secondo le indicazioni alle imprese da parte dell'Art. 29 *Data Protection Working Party*⁵⁷ — il ricorso ad altri strumenti come le *Standard Contractual Clauses* e le *Binding Corporate*

⁵³ Corte Giust. Ue, 6 ottobre 2015, causa C-362/15, *Schrems c. Data Protection Commissioner, Digital Rights Ireland Ltd.* Il caso aveva avuto origine dal ricorso di un cittadino austriaco, Max Schrems, contro Facebook in Irlanda — dove la società ha la sua sede europea — che lamentava la mancanza di un adeguato livello di protezione dei dati personali inviati da Facebook negli USA in ragione dell'accesso indiscriminato che la *National Security Agency* (NSA) statunitense aveva sui dati inviati da Facebook verso i server situati in territorio statunitense. La *High Court of Ireland*, presso la quale era stato portato il ricorso contro la decisione dell'Autorità per la protezione dei dati personali irlandese che si era basata sull'accordo di *Safe Harbour*, aveva rilevato i dubbi sull'adeguatezza del sistema di protezione offerto dagli USA e sollevato la questione pregiudiziale di fronte alla Corte di Giustizia Ue.

⁵⁴ Si v. *infra*, la nota seguente.

⁵⁵ Corte Giust. Ue, 6 ottobre 2015, causa C-362/15. In base alle norme statunitensi, le autorità statunitensi potevano avere un accesso generalizzato ai dati privati detenuti dalle imprese statunitensi e tale situazione importava un'illegittima interferenza con i diritti fondamentali riconosciuti dagli artt. 7 e 8 Carta dir. fondamentali Ue, la cui

tutela può subire limitazioni e deroghe soltanto ove strettamente necessario. La mancanza di tutela giurisdizionale o amministrativa confliggeva poi con l'art. 47 Carta dir. fondamentali Ue. Per queste ragioni la Corte Giust. Ue ha ritenuto che la decisione della Commissione sull'accordo *Safe Harbour* non soddisfacesse l'adeguatezza del regime giuridico di protezione dei dati personali offerto dall'ordinamento statunitense e che tale accordo dovesse essere dichiarato invalido.

⁵⁶ Sulle conseguenze della decisione *Schrems* si v. anche KUNER, *Reality and illusion in EU data transfer regulation post Schrems*, in *Legal Studies Research Paper Series*, University of Cambridge, Faculty of Law, Paper no. 14/2016, Marzo 2016, disponibile anche on-line al sito https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346 ora in *German Law Journal*, 2017, p. 181 ss.; VON KAI VON LEWISKI, *Privacy Shield — Notdeich nach dem Pearl Harbour für die transatlantischen Datentransfers*, in *EuR- EuropaRecht*, 2016, p. 405 ss.

⁵⁷ L'Article 29 *Data Protection Working Party* in un suo comunicato successivo alle conseguenze applicative della sentenza *Schrems* ha ribadito l'illegittimità di un eventuale trattamento transfrontaliero basato unicamente sull'accordo *Safe Harbour*.

Rules, di cui si è detto sopra, nel par. precedente. E, in alternativa a tali strumenti, il ricorso alla valutazione caso per caso da parte delle Autorità Garanti europee rispetto alle specifiche ipotesi di trasferimento e trattamento dei dati quanto al livello di protezione dei dati personali offerto dagli USA e alla sua “adeguatezza” ai sensi dell’art. 25 dir. 95/46.

È stato infine elaborato il *Privacy Shield*, un accordo frutto del negoziato tra la Commissione europea e il Governo USA, formalmente adottato dalla Commissione Ue il 12 luglio 2016⁵⁸ successivamente all’accordo politico sul nuovo regime per gli scambi transatlantici di dati personali a fini commerciali raggiunto il 2 febbraio 2016. Esso è stato concepito come lo strumento designato a succedere all’accordo di *Safe Harbour* per disciplinare la tutela della *privacy* nei rapporti Europa — USA⁵⁹, e a partire dal 1° agosto 2016 le imprese possono certificarsi come aderenti al *Privacy Shield* presso il Dipartimento del commercio degli Stati Uniti⁶⁰.

Il *Privacy Shield* si fonda su obblighi rigorosi per le imprese statunitensi che importano dati personali dall’Europa quanto al trattamento dei dati e alla protezione dei dati personali. Le imprese sono inoltre sottoposte ad un severo controllo finalizzato a rendere effettivi gli obblighi. È previsto che il Dipartimento del Commercio statunitense sottoponga le imprese aderenti allo “scudo” a verifiche ed aggiornamenti periodici per accertare che essi rispettino nella pratica le regole che hanno volontariamente accettato⁶¹. Diversamente, l’impresa si espone a sanzioni e alla cancellazione dall’elenco degli aderenti.

Altro profilo degli accordi raggiunti si concentra sul rispetto in termini chiari della sicurezza dei dati e degli obblighi di trasparenza per l’accesso ai dati personali da parte del governo statunitense, che ha dato assicurazione all’Unione europea che l’ac-

⁵⁸ Decisione della Commissione 2016/1250 del 12 luglio 2016 sull’adeguatezza della protezione fornita dal *Privacy Shield* EU-US.

Sul sito *ec.europa.eu* si trova una Guida al *Privacy Shield* EU-US. Dal sito *privacyshield.gov* si accede al *Privacy Shield Framework* gestito dal *Department of Commerce* degli USA e dalla Commissione europea.

⁵⁹ KUNER, *op. cit.*, p. 37, definisce il *Privacy Shield* il “tentativo di costruire un ponte tra due differenti discipline *privacy* che potrebbe rivelarsi una soluzione innovativa per il trasferimento dei dati”. Allo stesso tempo, tuttavia, l’A. critica il *modus operandi* dell’Unione europea nel giungere alla definizione di tale accordo, sostenendo che « the EU needs to modernize and open up its working methods to allow such sche-

mes to be commented on in public while they are being devised, rather than being negotiated in secret with third countries and then adopted hurriedly without proper debate ».

⁶⁰ Nel dicembre 2016 l’Art. 29 *Data Protection Working Party* ha pubblicato dei documenti di risposta a FAQ per il trasferimento dei dati sotto il regime del *Privacy Shield* per le imprese e per i soggetti privati (anche rispetto ai mezzi di tutela dei loro diritti) pubblicati sul sito *ec.europa.eu*, sezione *justice, data protection*.

⁶¹ Si era accertato che nell’esperienza applicativa del *Safe Harbour* i controlli sull’osservanza dell’accordo da parte degli operatori aderenti si erano manifestati non effettivi, cfr. *infra*, ult. par., e note 134 e 135, secondo quanto riferisce Mantelero.

cesso ai dati personali da parte delle pubbliche autorità statunitensi per scopi di applicazione della legge e di sicurezza nazionale è soggetto a limitazioni, garanzie e meccanismi di vigilanza precisi.

Ulteriore profilo del *Privacy Shield* concerne la protezione effettiva dei diritti dei cittadini europei attraverso maggiori possibilità di ricorso a rimedi. Sono previsti più meccanismi di composizione delle controversie per assicurare una tutela effettiva dei diritti individuali, al fine di assicurare a chiunque ritenga di aver subito un abuso sui dati che lo riguardano che ricada nel contesto del *Privacy Shield* di avere a disposizione diversi meccanismi di composizione delle controversie, di agevole accesso e dal costo contenuto. Il funzionamento del *Privacy Shield* sarà monitorato attraverso un riesame annuale comune.

Il trasferimento dei dati in base al *Privacy Shield* non ha ricevuto immediato accoglimento da parte delle imprese, come risulta da una recente ricerca condotta dalla *International Association of Privacy Professionals* ⁶² secondo la quale una percentuale altissima di imprese (corrispondente all'80%) sta attualmente facendo affidamento su altri strumenti, diversi dal *Privacy Shield*, per il trasferimento dei dati all'estero, come quelli delle *Standard Contractual Clauses* e delle *Binding Corporate Rules*, e solo il 34% prospetta di avvalersi del *Privacy Shield* (mentre era il 50% delle imprese ad affidarsi a *Safe Harbour*). Si abbia presente, tuttavia, che lo strumento delle *Standard Contractual Clauses* è attualmente sotto discussione: a seguito della sentenza *Schrems* l'autorità di protezione dei dati tedesca ha affermato che valuterà la liceità dei trasferimenti dei dati basati su strumenti alternativi (*Standard Contractual Clauses* e *Binding Corporate Rules*) e che non rilascerà più nuove autorizzazioni per l'uso di tali strumenti ⁶³. Per altro verso lo strumento delle *Binding Corporate Rules* presenta anche la criticità di non risultare appropriato per le piccole imprese, in quanto troppo costoso ed

⁶² *Privacy Governance Report* annuale per il 2016 della *International Association of Privacy Professionals* (IAPP) basato sulle risposte di 600 professionisti in materia di *privacy* da una parte e dall'altra dell'oceano in merito alla loro organizzazione del trasferimento dei dati.

⁶³ Tanto risulta dal documento programmatico pubblicato dalla Conferenza sulla protezione dei dati delle autorità tedesche di protezione dei dati a livello federale e statale del 26 ottobre 2015. Nel contempo, il Garante dello Schleswig-Holstein con una decisione del 14 ottobre 2015 aveva dichiarato l'inadeguatezza delle *Standard Contractual Clauses*. Si veda, Unabhaengiges Landeszentrum für Datenschutz Schleswig-

Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, 14 October 2015, § 4, <https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html>.

Le *Standard Contractual Clauses* potrebbero in effetti essere reputate uno strumento che non offre le necessarie garanzie. Si mette infatti in avviso che in ordinamenti in cui norme di natura imperativa legittimino un esteso accesso ai dati in favore delle autorità pare difficile ammettere che il ricorso ad accordi contrattuali sia efficace, dato che questi ultimi necessariamente ce-

impegnativo in termini di tempo per un tale genere di imprese, adattandosi invece piuttosto ai grandi gruppi di imprese transnazionali ⁶⁴.

4. IL TRATTAMENTO DEI DATI PERSONALI CON PROFILI DI TRANSAZIONALITÀ E IL TRASFERIMENTO DEI DATI PERSONALI ALL'ESTERO NEL NUOVO REGOLAMENTO EUROPEO 2016/679. INTRODUZIONE: IL MODELLO DI TUTELA DEI DATI PERSONALI INTRODOTTO DAL REGOLAMENTO EUROPEO.

Dal 25 maggio 2018 la disciplina europea in materia di trattamento dei dati con profili di transnazionalità e di trasferimento di dati all'estero sarà quella del nuovo Reg. (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati ⁶⁵, che a tutti gli effetti sostituirà, abrogandola, la disciplina contenuta nella dir. 95/46 che per tanto tempo ha costituito il punto di riferimento della disciplina europea.

Il Regolamento è nato dalla necessità di assicurare un'armonizzazione completa a livello europeo in materia di protezione dei dati personali, cosicché si avrà una disciplina effettivamente comune a tutti i Paesi membri dell'Unione europea, salvo che per quei profili che il Regolamento lascia all'iniziativa dei singoli Stati membri disciplinare diversamente ⁶⁶.

Il Regolamento mira in particolare a consolidare e ad adeguare

drebbro di fronte a tali disposizioni, così che il *data importer* potrebbe trovarsi a non poter rispettare il contenuto di alcune delle clausole standard. Cfr. MANTELEO, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per cittadini ed imprese?*, cit., p. 719 ss.

⁶⁴ A proposito della normativa relativa ai trasferimenti di dati all'estero è interessante la riflessione critica di KUNER, *op. cit.*, p. 37-38, il quale ritiene che l'Unione europea debba in un certo modo innovarsi affinché possa essere in grado di assicurare un sistema di trasferimenti di dati efficiente e concreto. Secondo l'A.: « Three points are crucial to a workable system of data transfer regulation in EU law. First, the EU must move beyond formalistic and political measures and legal fictions to implement actual protection in practice. Second, it must discard illusions, such as the idea that DPAs and national courts can perform meaningful assessments of the adequacy of non-EU data protection systems. Third, data protection law cannot by itself resolve issues relating to surveillance for national security or

intelligence-gathering purposes (...). In particular, it is necessary for the Court or the EU legislator to clarify the application of data protection rights under the Charter to situations involving national security, in order to remove any gaps in protection ».

⁶⁵ Pubblicato nella G.U.U.E. 4 maggio 2016, n. L 119.

⁶⁶ La discrezionalità concessa agli Stati membri ha un rilievo tale da impedire di « procedere ad un commento strutturato ed esaustivo della nuova regolazione, che illustri adeguatamente agli utenti il quadro normativo complessivo, anche tenendo conto, caso per caso, delle diverse regolazioni nazionali » fino a quando non saranno adottate le norme statali attuative e i provvedimenti di organizzazione delle Autorità nazionali, ciò che è obbligatorio fare entro il 25 maggio 2018, PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, II, Torino, Giappichelli, 2016, p. X. Volendo assicurare « un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possano ostacolare la libera circolazione dei dati personali nel mercato interno » e garantire certezza

agli sviluppi tecnologici i principi di protezione dei dati personali già precedentemente contenuti nella direttiva e manifesta la presa d'atto da parte delle istituzioni europee che nel mondo contemporaneo la tutela dei dati personali non può che avere una portata globale, pena la sua ineffettività. Si fonda inoltre sulla prospettiva secondo la quale la tutela dei dati personali degli utenti è necessaria per il medesimo sviluppo del commercio elettronico affinché gli utenti possano farvi ricorso con la fiducia che i propri dati personali saranno trattati nel rispetto dei loro diritti ⁶⁷. I punti nodali della nuova disciplina consistono dunque in « un rafforzamento dei diritti della persona, una più rigorosa applicazione delle norme, una razionalizzazione dei trasferimenti internazionali di dati personali e l'istituzione di norme di protezione dei dati a livello globale. Le norme sono concepite per garantire che i dati personali dei cittadini europei siano protetti — indipendentemente dal luogo in cui sono inviati, trattati o conservati — anche al di fuori dall'UE, come può spesso accadere in un mondo digitale » ⁶⁸.

Quanto ai profili di rafforzamento dei diritti della persona, il Regolamento conferisce alla persona interessata una maggiore consapevolezza rispetto al trattamento dei dati che la riguardano, offrendo uno standard di trasparenza più elevato rispetto alla dir. 95/46 dato che agli interessati devono essere forniti nuovi elementi di conoscenza, concernenti in particolare la “logica” del trattamento, al fine di garantire che questi siano posti nelle condizioni di essere realmente consapevoli di quale sia la logica utilizzata nel

del diritto e una tutela dei dati personali uniforme in tutti gli Stati dell'Unione (considerando 13) il Regolamento è costretto a fare i conti anche con le differenze economiche e culturali che caratterizzano i diversi Paesi e i loro ordinamenti (p. 18). In alcuni casi esso rimette agli Stati di regolare soltanto profili “interstiziali” di norme specifiche relative alla tutela di aspetti circoscritti degli istituti disciplinati. A volte la normativa statale è essenziale per l'attuazione del Regolamento, altre volte il potere regolatorio statale è essenzialmente facoltativo ma, se esercitato, integra le disposizioni del Regolamento con norme stabilite dalla legislazione nazionale (p. 17). È infatti lasciata agli Stati membri la libertà, ad esempio, di stabilire le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito (considerando n. 10); o ancora, gli Stati membri possono altresì prevedere ulteriori condizioni, comprese limitazioni, con riguardo al trattamento dei dati genetici, biometrici o quelli relativi alla salute (art. 9,

4° co.). Ancora, in via esemplificativa, è concesso agli Stati membri di prescrivere che i titolari del trattamento consultino l'autorità di controllo e ne ottengano l'autorizzazione preliminare in relazione al trattamento per l'esecuzione di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (art. 36, 5° co.).

In quest'ottica, vi sono molte disposizioni del Regolamento che richiedono agli Stati membri e alle Autorità di protezione dei dati chiarimenti ed integrazioni prima di poter essere attuate, ciò che consente il costante aggiornamento in linea con lo sviluppo della tecnologia e della realtà. V. Intervento di Giuseppe Busia, Segretario generale del Garante per la protezione dei dati personali, pp. 1-2, cit., *infra*, nota 95.

⁶⁷ OCSE, *Recommendation of the Council on Consumer Protection in E-commerce*, 24 marzo 2016.

⁶⁸ Comunicazione della Commissione al Parlamento europeo e al Consiglio, “Trasferimenti transatlantici di dati — Ripristinare la fiducia attraverso solide garanzie”, COM(2016) 117, 29 febbraio 2016, par. 2.2.

trattamento dei propri dati ⁶⁹. La medesima definizione di dato personale si allarga ad includere i dati sulla ubicazione e gli identificativi *online* (art. 4 n. 1); inoltre tra le “categorie particolari di dati personali” sono ricompresi i dati genetici e biometrici (art. 9). La tutela dell’interessato si evince anche dalle condizioni per il consenso previste dal Regolamento: il consenso al trattamento dei dati deve essere dato attraverso un atto positivo inequivocabile che può consistere ad esempio in una dichiarazione scritta, anche attraverso mezzi elettronici, o orale (mentre il silenzio o le caselle preselezionate non sono più sufficienti a rappresentare il consenso) (art. 7).

Il Regolamento ha rafforzato il diritto dell’interessato all’accesso e alla rettifica dei propri dati (artt. 15 e 16). Prevede anche un nuovo “diritto alla portabilità dei dati” (art. 20) che mira a favorire la possibilità di scelta dell’utente nell’ambito dei servizi *online*, fornendo agli interessati il diritto di riappropriarsi dei propri dati personali, a suo tempo ceduti ad un gestore di servizi per l’ottenimento di una determinata prestazione, in modo da poterli trasferire ad un gestore diverso per avvalersi dei suoi servizi ⁷⁰. Prevede, ancora, il diritto a non essere soggetti a decisioni basate su un trattamento automatizzato dei dati, inclusa la profilazione, a meno che non ricorrano circostanze specifiche, tra le quali il chiaro consenso informato dell’interessato (art. 22). Una novità è anche l’introduzione dell’obbligo di valutazione preventiva d’impatto sulla protezione dei dati a carico del titolare del trattamento quando un tipo di trattamento può presentare un rischio elevato per i diritti e la libertà delle persone fisiche (c.d. principio del *privacy impact assessment*) (art. 35), così come si prevede che il titolare del trattamento metterà in atto misure tecniche ed organizzative adeguate ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, quali la pseudonimizzazione o la minimizzazione (art. 25).

Nella recente comunicazione della Commissione europea del gennaio 2017 “*Building a European Data Economy*” il nuovo Regolamento fa da base alla disciplina del trattamento dei dati

⁶⁹ La logica del trattamento è conoscibile attraverso l’informativa, ove vengono descritte le modalità e le finalità del trattamento. Qualora la logica sottostante al trattamento non sia indicata nell’informativa o appaia poco chiara, l’interessato può esercitare i propri diritti e richiedere al titolare di comunicare in forma intelligibile la logica e le finalità su cui si basa il trattamento, secondo quanto previsto dallo stesso art. 7, 2° co., lett. c cod. privacy.

È tuttavia oggetto di dibattito la circostanza che determinati procedimenti per il trattamento dei dati personali, come quelli fondati sui *big data*, contraddicono tecnicamente tale principio di fondo della disciplina europea e si debba quindi trovare una soluzione a tali istanze poste dal progresso tecnologico.

⁷⁰ Intervento di Giuseppe Busia, Segretario generale del Garante per la protezione dei dati personali, p. 3, cit. *infra*, nota 95.

personali, che è concepita dalle istituzioni europee come in piena evoluzione. Al fine della costruzione di una *data economy* ⁷¹ la Commissione pone l'attenzione sulla necessità di un quadro di *policy* che consenta l'uso dei dati su tutta la catena del valore per scopi scientifici, sociali e industriali ed in particolare sulla necessità che il flusso dei dati all'interno dell'Unione europea sia consentito e protetto, dato che un flusso dei dati libero, sicuro e affidabile è strumentale alla protezione delle quattro libertà fondamentali del mercato unico europeo previste dai Trattati ⁷². Contestualmente viene proposta la revisione della dir. 2002/58 sul trattamento dei dati personali e sulla tutela della vita privata nelle comunicazioni elettroniche attraverso un nuovo Regolamento al fine di assicurare un elevato livello di protezione in coerenza con il Reg. 2016/679 ⁷³.

4.1. (segue) *Il nuovo criterio di applicazione territoriale della disciplina europea nel Regolamento europeo 2016/679.*

In ragione del perseguimento degli obiettivi di rafforzamento dei diritti degli interessati, enunciati nel precedente par., il legislatore europeo ha provveduto a modificare l'ambito di applicazione territoriale della normativa ⁷⁴. Dalla nuova estensione della sua applicazione emerge la volontà di recepire gli orientamenti delineatisi nella giurisprudenza della Corte di Giustizia Ue (soprattutto a partire dalla sentenza *Google Spain*), diretti a rendere la disciplina europea di tutela dei dati personali operativa anche nei confronti di titolari non europei e, per i cittadini europei, a renderla operativa anche nei casi in cui i loro dati siano trattati principalmente al di fuori dei confini europei.

Come si è visto sopra al par. 2, attualmente la dir. 95/46 prevede l'applicabilità della normativa quando il trattamento di dati personali è « effettuato nel contesto delle attività di uno stabilimento del responsabile situato nel territorio di uno Stato membro » (art. 4, 1° co., lett. a). In virtù di tale regola, letteralmente intesa, il criterio per la determinazione dell'ambito di applicazione della direttiva è il luogo fisico in cui i dati vengono trattati, mentre né la cittadinanza o il luogo di residenza abituale dell'in-

⁷¹ Che inerisce all'impatto complessivo del mercato dei dati sull'economia nel suo insieme; essa concerne la generazione, la raccolta, la conservazione, la distribuzione, l'analisi, l'elaborazione, la consegna e l'utilizzazione dei dati consentita dalle tecnologie digitali.

⁷² COM(2017) 9 final, 10 gennaio 2017, aprendo ad una pubblica consultazione sulla materia.

⁷³ COM(2017) 10 final, 10 gennaio

2017, che contiene appunto una proposta di Regolamento.

⁷⁴ Per approfondimenti sulle problematiche che hanno dato origine alla proposta di Regolamento e sulle soluzioni che il legislatore ha cercato di fornire con la nuova disciplina, si v. ad es. KOTSCHY, *The proposal for a new General Data Protection Regulation — problems solved?*, in *International Data Privacy Law*, IV/2014, pp. 274-281.

teressato, né l'ubicazione fisica dei dati personali sono decisivi a tali fini. Tale disposizione si è rivelata nel tempo inadeguata e limitativa, tanto da essere usata come schermo dai grandi fornitori di servizi sul *web* e, in generale, dalle multinazionali, per sfuggire all'applicazione della normativa europea. Si è osservato, infatti, che « il vero limite di questa disposizione, che è stato all'origine di infiniti problemi applicativi anche per quanto riguarda le legislazioni nazionali, è che essa esclude l'applicabilità della normativa europea ai trattamenti effettuati da chi abbia stabilimento al di fuori dell'Unione e possa sostenere di non compiere alcun trattamento di dati nel territorio di questa » ⁷⁵.

Come si è detto, la necessità di definire in maniera più puntuale i contorni dell'ambito operativo della disciplina europea è emersa a seguito della globalizzazione e degli sviluppi tecnologici. Essi hanno introdotto nella quotidianità contemporanea relazioni sempre più frequenti tra consumatori e imprese appartenenti a giurisdizioni diverse generate anche dal ricorso alla Rete per la circolazione dei beni e dei servizi, con la correlata condivisione di dati personali in un ambiente digitale, nel quale la loro reale ubicazione e il loro impiego sono difficili da accertare ⁷⁶.

Si è quindi fatta strada nel tempo una volontà riformatoria del criterio di applicazione territoriale della normativa europea i cui primi segnali si possono rintracciare nel Parere espresso dal Gruppo Art. 29 nel dicembre del 2010 ⁷⁷, ove per la prima volta viene esaminata la nozione di “contesto delle attività” ⁷⁸ e vengono suggerite alcune possibili soluzioni al trattamento effettuato da titolari situati al di fuori dei confini europei ⁷⁹. In realtà già tempo prima, nel gennaio 2010, con lo “Studio comparativo dei diversi approcci alle nuove sfide della *privacy*, in particolare alla luce degli sviluppi tecnologici” la stessa Commissione europea aveva palesato delle remore circa l'ambiguità e la contrastante attuazione delle disposizioni della direttiva sul diritto applicabile, raccomandando « regole migliori, più chiare e univoche sul diritto

⁷⁵ Così PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, p. 79.

⁷⁶ Ciò è messo in rilievo anche dall'Ocse nel suo *Explanatory Memorandum alle Guidelines del 2013 sulla protezione della privacy* e i flussi transfrontalieri di dati personali di cui si dirà *infra*, par. 5.2.

⁷⁷ Gruppo di lavoro Art. 29, *Opinion 8/2010 on applicable law*, WP n. 179, 16 dicembre 2010.

⁷⁸ Per l'interpretazione dottrinale di tale concetto, si veda CAGGIANO, *L'interpretazione del “contesto delle attività di stabi-*

limento” dei responsabili del trattamento dei dati personali, in *Dir. inf.*, IV-V/2014, pp. 605-622.

⁷⁹ I criteri proposti dal gruppo delle Autorità Garanti europee erano, rispettivamente, quello del c.d. “approccio orientato al servizio” (poi implementato nel recente Regolamento 679/2016), consistente nell'applicazione del diritto dell'UE sulla protezione dei dati quando l'attività che implica il trattamento di dati personali è mirata a cittadini europei; e quello relativo agli “strumenti/mezzi” consistente nell'individuazione di eventuali infrastrutture di trattamento dei dati in territorio europeo e applicabile solo in via residuale in caso di inapplicabilità degli altri criteri.

applicabile »⁸⁰. A tale studio aveva fatto poi seguito una comunicazione del novembre 2010, ove la Commissione evidenziava la necessità di « rivedere e chiarire le disposizioni vigenti in materia di diritto applicabile, compresi gli attuali criteri determinanti, al fine di migliorare la certezza giuridica, di chiarire le competenze degli Stati membri nell'applicare le norme di protezione dei dati e di garantire lo stesso livello di protezione alle persone residenti nell'UE, a prescindere dalla localizzazione geografica dal responsabile del trattamento »⁸¹.

Tali studi e documenti hanno fatto strada alla posizione della Corte di Giustizia europea che con una serie di pronunce di rilievo fondamentale ha poi sostenuto l'interpretazione estensiva del criterio di applicazione territoriale della disciplina europea, recepita infine dal nuovo Regolamento. Il riferimento è ai casi *Weltimmo*, *Google Spain* e *Amazon*, di cui si è detto nel par. 2, con i quali la Corte ha effettuato un'operazione ermeneutica volta ad ampliare l'ambito operativo della disciplina europea attraverso la valutazione della flessibilità ed estensibilità del concetto di « stabilimento » e, allo stesso tempo, l'ampliamento del concetto di « trattamento » dei dati personali⁸².

Il Regolamento ribalta infine il tradizionale principio di stabilimento, sancendo al suo art. 3 l'applicabilità della disciplina da questo dettata « indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione » e prevedendo l'applicazione della normativa anche a titolari e responsabili non stabiliti nell'Unione europea, quando l'attività di trattamento riguardi: *a*) l'offerta di beni o la prestazione di servizi a soggetti interessati che si trovano nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure *b*) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione (art. 3, 1° e 2° co. del Regolamento)⁸³. Inoltre è da notare che, secondo quanto prevede il nuovo Rego-

⁸⁰ *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, 20 gennaio 2010, disponibile all'indirizzo: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

⁸¹ «Un approccio globale alla protezione dei dati personali nell'Unione europea», COM(2010) 609, 4 novembre 2010.

⁸² Si v. *supra*, par. 2.

⁸³ Si v. anche i considerando nn. 22 e 23 del Reg. Il considerando n. 23 recita che « onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati

personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito *web* del titolare del trattamento, del responsabile del trattamento o

lamento, la normativa europea a tutela dei dati personali potrà essere applicata non solo ai trattamenti effettuati nell'ambito delle attività di uno stabilimento del titolare situato nell'Unione ⁸⁴, ma anche nel caso in cui si tratti di uno stabilimento del responsabile ⁸⁵.

4.2. (segue) *Il trasferimento di dati all'estero tra continuità e innovazione nel nuovo Regolamento europeo.*

In materia di trasferimento dei dati personali all'estero il Regolamento pare assumere un carattere di continuità rispetto alla precedente direttiva in materia, pur fornendo un impianto normativo molto più ampio e dettagliato rispetto ad essa ⁸⁶. Ciò si colloca in linea con la prospettiva indicata nella comunicazione della Commissione del febbraio 2016 in cui si poneva l'accento sulla razionalizzazione dei trasferimenti internazionali dei dati personali e sulla problematica del livello globale della protezione dei dati personali ⁸⁷. In particolare, in un'ottica di incentivazione del commercio e della cooperazione internazionale il Regolamento ha il merito di facilitare sotto il profilo burocratico i flussi di dati personali verso e dai Paesi al di fuori dell'Unione, e verso le organizzazioni internazionali, garantendone pur sempre la sicurezza e il rispetto dei principi di tutela.

Scendendo nel dettaglio della normativa, va preliminarmente segnalato che la disciplina ricopre un ambito di applicazione più ampio consentendo il trasferimento non solo verso Paesi terzi, ma anche verso « organizzazioni internazionali » (art. 44, 1° co.). Inoltre, l'operatività della disciplina risulta ancor più allargata se si considera che la Commissione può adottare una decisione di

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

⁸⁴ Ai sensi del 3° co. dell'art. 3 del Regolamento, la disciplina europea si applica tra l'altro anche ai titolari non stabiliti nell'Unione ma sottoposti alla legge nazionale di uno Stato membro in virtù del diritto pubblico internazionale. Tale disposizione non ha carattere innovativo in quanto ri-

produce la clausola già presente nella dir. 95/46 all'art. 4, lett. *b*.

⁸⁵ Là dove, secondo le definizioni di cui all'art. 4 del Reg. 2016/679, il « titolare del trattamento » è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o assieme ad altri, determina le finalità e i mezzi di trattamento dei dati personali e il « responsabile del trattamento » è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. È facoltà del titolare nominare uno o più responsabili e uno o più incaricati del trattamento dei dati.

⁸⁶ Basti notare che il Regolamento dedica ai trasferimenti di dati personali all'estero l'intero Capo V (artt. 44-50), mentre la dir. 95/46 riserva all'argomento solo due norme (artt. 25-26).

⁸⁷ COM(2016) 117, 29 febbraio 2016, di cui *supra*, par. 4.

“adeguatezza” — il criterio già previsto dalla dir. 95/46, di cui si è sopra detto al par. 2 — non solo nei confronti dei menzionati soggetti statali e soggetti istituzionali, ma anche solo di « un territorio o uno o più settori specifici all’interno del paese terzo ».

Salva questa specificazione, nulla muta in relazione al menzionato principio di “adeguatezza” come vagliato dalla Commissione europea (art. 45), ossia il meccanismo basato sul riconoscimento da parte dell’istituzione europea dell’adeguatezza del livello di protezione assicurato ai dati personali europei dal Paese terzo ⁸⁸. Tale presupposto di legittimità del trasferimento dei dati all’estero era infatti già presente nella dir. 95/46 — come si è visto sopra, al par. 3 — ma ora la procedura sottostante per l’accertamento della ricorrenza del requisito viene delineata in modo più preciso. In particolare, la Commissione è tenuta a verificare la sussistenza di una serie di elementi non solo tecnico-giuridici, bensì afferenti anche alla sfera politica e ideologica dello Stato terzo o dell’organizzazione internazionale, la cui presenza dovrebbe essere sintomatica di un adeguato livello di protezione dei dati personali ⁸⁹. Inoltre, è previsto un meccanismo di riesame periodico (almeno ogni quattro anni) delle decisioni di adeguatezza adottate, che si basa sulla valutazione di tutti gli sviluppi rilevanti nel Paese terzo o nell’organizzazione internazionale che potrebbero avere conseguenze dirette, anche negative, sul livello di protezione offerto.

La novità più rilevante in materia concerne però la specificazione delle c.d. « garanzie adeguate » (di cui già all’art. 26, 2° co. dir. 95/46 come « garanzie sufficienti »), sulla base delle quali un titolare o un responsabile può trasferire dati personali verso un Paese terzo od un’organizzazione internazionale in assenza di una decisione di adeguatezza (art. 46).

Oltre ad arricchire il novero di tali presupposti di legittimità, il Regolamento ne fa oggetto di specifica previsione normativa. Mentre infatti l’art. 26, 2° co. della dir. 95/46 menzionava nello specifico le sole « clausole contrattuali appropriate », ora il Regolamento inserisce tra gli strumenti di garanzia adeguata anche le *Binding Corporate Rules*, o norme vincolanti d’impresa (di cui si è detto sopra, al par. 3), i codici di condotta, i meccanismi di certificazione, le clausole contrattuali tra il titolare del tratta-

⁸⁸ Anche nell’adozione del principio di *adequacy*, piuttosto che quello di *interoperability* sostenuto dagli USA, si ravvisa una scelta di carattere politico: il legislatore europeo ha in questo modo imposto di sposare la propria concezione della protezione dei dati personali come un diritto fondamentale. Come detto, gli Stati Uniti sostengono invece una visione opposta incentrata sull’autoregolamentazione, settorialità e com-

mercialità della disciplina della *privacy*. In proposito, cfr. PAGALLO, *La tutela della privacy negli Stati Uniti d’America e in Europa. Modelli giuridici a confronto*, Milano, Giuffrè, 2008; SARTOR-VIOLA DE AZEVEDO CUNHA, *Il caso “Google” e i rapporti regolatori USA/EU*, in *Dir. inf.*, IV-V/2014, pp. 657-680.

⁸⁹ Si veda il dettato dell’art. 45, 2° co., lett. a, b e c del Regolamento.

mento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale, e le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati ⁹⁰. Vengono inoltre fissati dei requisiti minimi per le *Binding Corporate Rules* come l'indicazione della struttura organizzativa del gruppo imprenditoriale, i trasferimenti di dati previsti, le regole che l'organizzazione ritiene giuridicamente vincolanti, la dichiarazione di come l'organizzazione intende applicare i principi base di protezione dei dati personali, i diritti dei soggetti interessati, il riconoscimento di potenziali responsabilità per qualunque violazione delle norme vincolanti d'impresa, il monitoraggio interno rispetto alla *compliance*, la comunicazione con i soggetti interessati e la cooperazione con i regolatori (art. 47).

Molto interessante è la disposizione di cui all'art. 48, ove è previsto che un trasferimento di dati possa legittimamente avvenire sulla base delle sentenze di un'autorità giurisdizionale e delle decisioni di un'autorità amministrativa di un Paese terzo, purché basate su un accordo internazionale in vigore tra il Paese terzo richiedente e l'Unione o un suo Stato membro, e fatti salvi gli altri presupposti di trasferimento.

L'art. 49 del Regolamento è invece dedicato alle deroghe in virtù delle quali è legittimo il trasferimento dei dati anche in mancanza dei presupposti sinora menzionati, disposizione che riproduce pressoché fedelmente le deroghe già previste dalla dir. 95/46 all'art. 26 — secondo quanto si è visto sopra al par. 3 —, sebbene la previsione denoti un grado di dettaglio molto più elevato. A tale riguardo, un'aggiunta di non poca importanza è quella secondo la quale, in assenza dei presupposti di legittimità e delle deroghe per il trasferimento dei dati, questo possa ugualmente avvenire « se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali » (1° co., ult. par.).

⁹⁰ Si tenga conto che, ai sensi dell'art. 46, 2° e 3° co. del Regolamento, solo le norme vincolanti d'impresa, le clausole tipo (sia quelle adottate dalla Commissione sia quelle dell'Autorità di supervisione), i codici di condotta e i meccanismi di certifica-

zione costituiscono garanzie adeguate, senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo. Le restanti "garanzie" devono invece passare al vaglio dell'autorità di controllo competente.

Il Capo V del Regolamento dedicato ai trasferimenti di dati personali all'estero si conclude con una disposizione particolarmente rilevante, contenente una serie di misure volte ad incentivare la cooperazione internazionale per la protezione dei dati personali, e cioè dirette a sviluppare meccanismi di cooperazione internazionale, prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, coinvolgere le parti interessate in discussioni ed attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali, promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali (art. 50).

5. LE PROBLEMATICHE DI TUTELA DEI DATI PERSONALI IN PROSPETTIVA GLOBALE: I PRINCIPI E LE REGOLE ESISTENTI A LIVELLO INTERNAZIONALE.

In tempi a noi vicini le problematiche relative ai profili transnazionali del trattamento dei dati quanto alla legge applicabile e al trasferimento dei dati personali all'estero si sono manifestate in special modo rispetto ai rapporti Europa — USA in ragione dell'importanza del flusso di dati in tale direzione. Esse sorgono tuttavia non soltanto nel contesto di questi rapporti ma, in via più generale, nei rapporti con gli operatori collocati in qualsiasi altra parte del globo, come consegue al notevole sviluppo dei rapporti commerciali — e non solo — che si svolgono *online*⁹¹. Ad esempio, importanti operatori dell'*e-commerce* di portata internazionale hanno sede in Lussemburgo, e sempre più hanno la potenzialità di svilupparsi a livello commerciale anche rapporti con operatori di Paesi dalle economie in via di sviluppo⁹². Come si è detto in apertura di questo lavoro, la natura globale dell'attuale flusso di dati e delle connesse problematiche di tutela è

⁹¹ Sta diffondendosi sempre più un'economia del c.d. *shopping online cross-border*, ossia del commercio elettronico transfrontaliero. A dimostrarlo sono alcuni dati derivanti dallo studio condotto da Deloitte e commissionato da eBay nel 2013 ("The Omnichannel Opportunity: A Report for eBay") da cui è emerso che il 15% dei consumatori europei ha acquistato *online* dei prodotti provenienti da Paesi o *retailer* stranieri. Per quanto riguarda il ruolo dell'Italia nel *cross-border trade*, rispetto al 2013, quando solo il 4% del commercio transfrontaliero proveniva dal nostro Paese, ad oggi l'*export* — secondo l'Osservatorio *eCommerce* del Politecnico di Milano — inteso come il valore delle vendite da siti italiani a consumatori stranieri, nel 2016 è cresciuto del 17% e supera i 3,4 miliardi di euro.

⁹² Senza sottacere che in realtà in un mondo dai rapporti globalizzati la sede fisica dell'impresa potrebbe essere collocata (quasi) ovunque a seconda delle convenienze del caso, v. DRAETTA, *op. cit.*, p. 5, che osserva che a partire dal secondo dopoguerra la matrice nazionale degli operatori impegnati in traffici internazionali viene ad assumere un rilievo sempre meno significativo. « Infatti, le imprese si organizzavano con sedi operative situate dovunque apparisse conveniente, così che la sede legale dell'impresa stessa finiva con l'avere un rilievo solo formale. In altre parole, da imprese internazionali, esse divenivano multinazionali o *tout court* globali. I singoli operatori economici, d'altra parte, operavano spostandosi di volta in volta, seguendo

legata alla medesima diffusione di tecnologie quali il *cloud computing*, i *big data* e la *Internet of Things*, che rappresentano il futuro prossimo dell'informatica e della telematica ⁹³.

È emersa quindi in maniera evidente la portata essenzialmente internazionale che oggi giorno presentano le esigenze di tutela del diritto sui dati personali, e con ciò l'idea che l'unica forma efficace di tutela giuridica dei dati personali debba essere affidata a strumenti giuridici elaborati al medesimo livello internazionale ⁹⁴. Nelle sedi internazionali emerge, ancor più, che la questione della tutela dei dati personali necessita di essere affrontata a questo livello con urgenza, sia per quanto riguarda la formazione delle regole, sia per quanto riguarda l'assicurazione della loro effettività, ossia l'*enforcement* di tali regole.

Così nella sede della riunione dei Garanti della *privacy* dei diversi Paesi europei del maggio 2016, si è affermata l'importanza del livello globale di tutela dei dati evidenziando che talune esigenze di protezione dei dati personali possono essere soddisfatte solo se operano a livello internazionale ⁹⁵. Nel contesto delle conferenze internazionali delle Autorità Garanti della *privacy* e sulla protezione dei dati ⁹⁶ già nel 2009, nella Conferenza di Madrid, si era adottata la Risoluzione di Madrid "Norme globali sulla *privacy* per un mondo globale", con il fine di « definire una

criteri di convenienza, nello Stato che meglio favoriva i loro traffici ».

⁹³ Al riguardo si v. *supra*, note 4 e 6.

⁹⁴ In tal senso FOCARELLI, *op. cit.*, p. 105, afferma che tra le ragioni per le quali le norme attualmente regolanti la protezione dei dati personali sono inadeguate vi è appunto la circostanza che tali norme sono nazionali, o tutt'al più regionali, come quelle dell'Unione europea, e non globali come richiederebbe il contesto attuale.

⁹⁵ Nell'Intervento del Segretario generale del Garante per la protezione dei dati personali Busia alla Conferenza di primavera delle Autorità nazionali di protezione dei dati personali del 2016, consultabile sul sito del *garanteprivacy.it*, p. 2, si legge: « occorre (...) chiedersi se una regolamentazione europea sia oggi sufficiente o se abbiamo bisogno di qualcosa di più. In molti casi — basti pensare alle criticità legate alla tutela del diritto all'oblio sul *web* — sappiamo che, per essere davvero efficace e garantire concretamente i diritti fondamentali dei cittadini, avremmo bisogno di regole globali o, almeno, di principi globali ». Il Segretario generale del Garante per la protezione dei dati personali nel suo intervento afferma che il nuovo Reg. 2016/679, la nuova dir. 2016/680 e la Convenzione del Consiglio d'Europa n. 108, nella nuova revisione, costituiscono il vero "pacchetto sulla prote-

zione dei dati personali" che dovrebbe garantire un nuovo quadro giuridico in vista del futuro e delle sfide tecnologiche che questo pone. Nel contesto del nuovo quadro si sta iniziando a sperimentare il nuovo Comitato europeo della protezione dei dati, organo istituito dal Reg. 2016/679, al cui interno opereranno e coordineranno la propria azione tutte le autorità nazionali di protezione dei dati, su cui *infra*, ult. par.

⁹⁶ Nell'ottica della collaborazione e della cooperazione a livello internazionale è fondamentale il ruolo delle conferenze annuali delle autorità garanti per la protezione dei dati personali a livello internazionale (*International Conference of Data Protection & Privacy Commissioners*) ed a livello europeo (Conferenze di primavera), nel contesto delle quali si valutano le azioni da intraprendere per il presente ed il futuro della tutela dei dati personali. Nelle conferenze internazionali vengono adottate risoluzioni sui diversi problemi sul tappeto, e tra queste un *Action Plan* triennale, risoluzioni sull'*enforcement* e sulla relativa cooperazione internazionale, sulla tutela della *privacy* nelle azioni umanitarie e sull'educazione alla tutela della *privacy*, e sulle necessità degli sviluppi tecnologici del prossimo futuro (così "Resolution on the future of privacy" del 2012, "Privacy in the Digital Age" del 2014, le risoluzioni sui *Big Data*

serie di principi e diritti garantendo una tutela della *privacy* efficace ed uniforme a livello internazionale con riguardo al trattamento dei dati personali, e facilitare i flussi internazionali di dati personali necessari in un mondo globalizzato »⁹⁷. Nella successiva Conferenza di Varsavia del 2013 era stata adottata una Risoluzione “Sul diritto internazionale quale fondamento della protezione dei dati e della *privacy*” con la quale si osservava che « vi è un’esigenza pressante di elaborare un accordo internazionale vincolante in materia di protezione dei dati che garantisca i diritti umani attraverso la tutela della *privacy*, dei dati personali e dell’integrità delle reti »⁹⁸ e si era « delibera[to] di sollecitare i governi a chiedere l’adozione di un protocollo addizionale all’art. 17 del Patto internazionale sui diritti civili e politici ».

Le problematiche internazionali del trattamento e del trasferimento dei dati hanno attratto anche l’intervento dell’ONU, se pure sotto il profilo della sorveglianza e del controllo di massa piuttosto che sul piano dei rapporti di tipo privatistico⁹⁹, e nel 2015 si è proceduto a nominare un Relatore speciale sul diritto

del 2014 e sul *Cloud Computing* del 2012). L’*Action Plan* più recente (2016-2018), adottato nella conferenza del 2015, comprende tra le priorità strategiche il punto “*Advancing Global Privacy in the Digital Age*” nell’ambito del quale si prevede di prestare assistenza e consulenza al Rappresentante speciale per la *privacy* dell’ONU, di sviluppare approcci e mezzi comuni per la protezione della *privacy* e dei dati personali, nonché di rafforzare la connessione tra autorità e con le organizzazioni internazionali, con i *networks* coinvolti nella protezione transnazionale dei dati e nell’*enforcement* della *privacy*, e con le conferenze regionali delle autorità garanti. Relativamente al profilo dell’*enforcement*, nella conferenza del 2014 era stata adottata una risoluzione sull’*Enforcement Cooperation* e così anche nel 2016 sull’*International Enforcement Cooperation* che prevede tra l’altro l’interazione con il gruppo *Global Privacy Enforcement Network* (GPEN, su cui v. *infra*, nota 103) e con altri importanti *networks* per la creazione di progetti che coordinino meglio gli sforzi verso la cooperazione globale sull’*enforcement*.

A livello europeo un ruolo di primario rilievo per le problematiche transnazionali di tutela della *privacy* ha sinora rivestito il Gruppo di lavoro Art. 29, su cui v. *supra*, nota 9, destinato ad essere sostituito dal Comitato europeo per la protezione dei dati di cui *infra*, nota 140.

⁹⁷ Secondo quanto prevede l’art. 1 della Risoluzione. Nella Risoluzione vengono enunciati i principi del trattamento dei

dati secondo correttezza, in modo lecito e proporzionato con riguardo a scopi specifici, espliciti e legittimi, sulla base di politiche trasparenti, garantendo l’accuratezza, la riservatezza e la sicurezza dei dati nonché la legittimità del trattamento e i diritti degli interessati di accedere, rettificare, cancellare i dati ed opporsi al loro trattamento, mettendo in atto i principi di *accountability* e responsabilità, ed offrendo garanzie più idonee quando si tratta di dati sensibili. Si danno inoltre espresse indicazioni di principio sul trasferimento dei dati all’estero, sulla sicurezza, sulla promozione di misure che favoriscano una migliore osservanza delle norme applicabili in materia, sulla cooperazione e il coordinamento tra autorità garanti.

⁹⁸ « E al contempo rafforzi la trasparenza dei trattamenti realizzando il giusto bilanciamento rispetto alla sicurezza, agli interessi economici ed alla libertà di espressione ».

⁹⁹ Successivamente ai “Principi guida per la regolazione dei file di dati personali computerizzati” adottati con una Risoluzione non giuridicamente vincolante del 1990, e diretti tra l’altro ad influire sulla legislazione degli Stati e sulla condotta delle altre organizzazioni internazionali (FOCARELLI, *op. cit.*, p. 114) nel dicembre 2013, e poi anche nel 2014 e nel 2015, l’ONU ha adottato delle Risoluzioni sul “diritto alla *privacy* nell’era digitale” nelle quali si esprime la preoccupazione per l’impatto negativo che la sorveglianza e l’intercettazione delle comunicazioni può avere sull’esercizio ed il godi-

alla *privacy* ¹⁰⁰. Anche lo studio dell'UNCTAD (*United Nations Conference on Trade and Development*) dell'aprile 2016 "*Data protection regulations and international data flows: Implications for trade and development*" ¹⁰¹ mette in luce come la regolazione adeguata della tutela dei dati personali sia un elemento determinante per lo sviluppo delle relazioni commerciali ¹⁰². Nel contempo è emerso che, oltre alla formazione di regole dalla portata globale, sono fondamentali anche la collaborazione e la cooperazione a livello internazionale per assicurare l'*enforcement* delle discipline di tutela dei dati personali ¹⁰³.

Da tempo a livello internazionale esistono più enunciazioni di tutela giuridica della *privacy* e dei dati personali, a cominciare dalle dichiarazioni e convenzioni per la tutela dei diritti umani di rango fondamentale nelle quali si trovano dichiarazioni generali del diritto al rispetto della vita privata come diritto dell'uomo, in cui viene tradizionalmente ricompreso il diritto alla tutela sui propri dati personali ¹⁰⁴.

La tutela di un diritto sui propri dati personali si fonda sulla Dichiarazione universale dei diritti dell'uomo, che al suo art. 12 prevede che « nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata (...) ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o

mento dei diritti umani, chiedendo a tutti gli Stati di adottare misure e leggi interne idonee a prevenire sue eventuali violazioni, sulla circostanza che certi tipi di metadati una volta aggregati possono rivelare informazioni personali.

¹⁰⁰ Tra i cui compiti rientra riferire su presunte violazioni del diritto alla *privacy* ovunque commesse e sottoporre questioni particolarmente gravi all'attenzione del Consiglio e dell'Alto commissario per i diritti umani, FOCARELLI, *op. cit.*, p. 135 ss.

¹⁰¹ Consultabile *online* sul sito Internet dell'UNCTAD.

¹⁰² Si riconosce espressamente che i dati personali sono il carburante che conduce molte attività commerciali *online* (p. 12 dello Studio). E questo sia per i governi che, specie nei Paesi in via di sviluppo, trovano problematico adottare una normativa di tutela e per lo più si rifanno al modello europeo, sia per i consumatori, relativamente ai quali è fondamentale costruire fiducia nell'ambiente *online* (lo studio riferisce che vi sono evidenze che i consumatori siano preoccupati del trattamento dei loro dati personali *online*, di come essi vengono raccolti ed utilizzati, e che queste preoccupazioni sono crescenti, e sono aggravate dalla mancanza di chiarezza rispetto ai profili di protezione e ai rimedi), sia per le

imprese, che da parte loro temono che un regime di protezione troppo stringente possa significare una riduzione delle attività, un aumento dei costi amministrativi ed un ostacolo all'innovazione, e che la mancanza di chiarezza e compatibilità tra regimi diversi crei incertezza con effetti negativi sugli investimenti, nonché che regimi divergenti di tutela inibiscano l'adozione delle tecnologie emergenti riducendo i connessi benefici a livello sociale (p. 13).

¹⁰³ A proposito v. *supra*, nota 96, in fine. A seguito di una Raccomandazione dell'Ocse sulla cooperazione transnazionale e sull'*enforcement* delle leggi di protezione della *privacy* è stato costituito nel 2010 il *Global Privacy Enforcement Network* (GPEN) che è un gruppo informale di autorità per l'*enforcement* delle norme sulla *privacy* la cui missione consiste nel migliorare la cooperazione nell'*enforcement* delle regolazioni della *privacy*. Tra i membri vi sono le autorità garanti della *privacy* di: Australia, Belgio, Bulgaria, Canada, Macau, Repubblica Ceca, Estonia, Francia, Germania, Guernsey, Irlanda, Israele, Italia, Corea, Messico, Olanda, Nuova Zelanda, Norvegia, Polonia, Slovenia, Spagna, Svizzera, Ucraina, Gran Bretagna, Stati Uniti, e Unione europea. V. anche *supra*, nota 96.

¹⁰⁴ FOCARELLI, *op. cit.*, p. 147.

lesioni », e sul Patto internazionale sui diritti civili e politici, che all'art. 17 riprende la formulazione dell'art. 12 della Dichiarazione universale, con la differenza che il Patto è dotato di forza giuridica vincolante ¹⁰⁵. Altra enunciazione di carattere fondamentale, se pure in ambito europeo e non internazionale, è quella che si trova nella Convenzione europea dei diritti dell'uomo, che all'art. 8 prevede un generale diritto al rispetto della vita privata e familiare ¹⁰⁶.

Come si vedrà qui di seguito altre fonti di tutela sono previste a livello di convenzione internazionale oppure di linee guida a livello internazionale, mentre attualmente più iniziative da parte di organizzazioni internazionali sono dirette a promuovere la creazione di regole internazionali o, almeno, regole internazionali di principio che diano vita a discipline di tutela dei dati personali compatibili tra loro.

5.1. (segue) *La Convenzione n. 108 del Consiglio d'Europa.*

Un ruolo di grande rilievo nella protezione dei dati personali a livello internazionale ha svolto e svolge il Consiglio d'Europa ¹⁰⁷ nel cui ambito è stata elaborata la Convenzione n. 108 del 1981, di cui è in corso la revisione che si attende a breve ¹⁰⁸. La Convenzione n. 108 trae diretta ispirazione dall'art. 8 della

¹⁰⁵ « 1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze ed offese ».

¹⁰⁶ Prevedendo l'art. 8, 2° co. che non può esservi ingerenza di un'autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza non sia prevista dalla legge e costituisca una misura che in una società democratica è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del Paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Si v. M.E. BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti umani e diritto internaz.*, III/2011, p. 437 ss.

¹⁰⁷ Il Consiglio d'Europa, fondato nel 1949, è un'organizzazione internazionale composta da 47 membri che ha per scopo di promuovere la democrazia, i diritti umani,

l'identità culturale europea e la ricerca di soluzioni ai problemi sociali in Europa. Dal 1989 ha lo status di osservatore dell'Assemblea generale delle Nazioni Unite. Dei 47 Stati membri, 28 fanno parte dell'Unione europea. Gli Stati geograficamente europei che non fanno parte del Consiglio d'Europa sono soltanto il Vaticano e la Bielorussia, mentre cinque Stati del Consiglio non fanno parte dell'Europa geografica: Georgia, Armenia, Azerbaigian, Cipro, Turchia.

¹⁰⁸ Le evoluzioni della revisione della Convenzione si possono seguire sul sito c.e.int. La decisione di procedere ad una revisione della Convenzione era stata adottata il 10 marzo 2010, e il 3 dicembre 2014 il Comitato *ad hoc* sulla protezione dei dati del Consiglio d'Europa ha approvato le proposte di modernizzazione della Convenzione e ha incaricato il Segretario di preparare un identico progetto di Protocollo di emendamento. Sulla Convenzione n. 108 si v., ad esempio, FUMAGALLI MERAVIGLIA, *Le nuove normative europee sulla protezione dei dati personali*, in *Dir. com. e scambi internaz.*, I/2016, p. 2 ss., 12 ss. La revisione della Convenzione n. 108 è stata oggetto di una specifica risoluzione di supporto nella sede della Conferenza di primavera delle auto-

Convenzione europea dei diritti dell'uomo del 1950 che, attraverso la giurisprudenza della Corte europea dei diritti dell'uomo, ha svolto un ruolo essenziale nell'interpretazione del diritto fondamentale al rispetto della vita privata ¹⁰⁹.

Il testo rivisto della Convenzione — che manterrà le sue previsioni al livello di principi per accordare agli Stati membri una certa misura di discrezionalità nella fase della loro implementazione negli ordinamenti nazionali — sarà accompagnato da testi settoriali sotto forma di raccomandazioni o linee guida ed aspira ad assicurare coerenza e compatibilità con il quadro di protezione legale europeo, a mantenere previsioni tecnologicamente neutre, e a riaffermare il potenziale della Convenzione come uno standard universale. L'art. 23 della Convenzione prevede che possano essere invitati ad aderire anche Stati non membri del Consiglio d'Europa, ed ora il progetto di modifica estende la categoria dei soggetti che hanno facoltà di aderirvi, ricomprendendovi anche le organizzazioni internazionali ¹¹⁰. Profilo importante della revisione è appunto la direzione verso la globalizzazione della Convenzione ¹¹¹, registrandosi ad oggi come Stati aderenti non europei l'Uruguay, il Marocco, le Isole Mauritius, il Senegal e la Tunisia.

Nel suo testo oggetto di revisione ¹¹² la Convenzione — che come detto intende collocarsi su una traccia di compatibilità con il quadro giuridico dell'Unione europea ¹¹³ — introduce nel suo preambolo un'attestazione del diritto all'autodeterminazione informatica e prevede il consenso dell'interessato, che era assente nel testo della Convenzione del 1981, come presupposto del trattamento dei dati. L'art. 5, 2° co. prevede appunto che il trattamento dei dati possa essere effettuato soltanto sulla base del

rità garanti europee del 2017 tenutasi a Cipro.

¹⁰⁹ Riferisce che la portata e il contenuto della disposizione è stato ampliato attraverso un'interpretazione evolutiva da parte della Corte europea dei diritti dell'uomo, FUMAGALLI MERAVIGLIA, *op. cit.*, p. 3.

¹¹⁰ Questo potrà avvenire successivamente all'entrata in vigore della Convenzione, dopo che cinque Stati membri del Consiglio d'Europa abbiano espresso il loro consenso ad essere vincolati dalla Convenzione (art. 22).

¹¹¹ GREENLEAF, "Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?, in *Computer Law & Security Review*, 2013, p. 2 dell'estratto. Si è osservato che i profili di modernizzazione e di globalizzazione della Convenzione sono simbiotici, dato che il primo è finalizzato all'attrazione dell'adesione di Stati non europei attraverso la messa

a punto di un livello di protezione dei dati che sia "just right", ovvero non troppo elevata, ciò che scoraggerebbe l'ampia adesione di Paesi non europei (p. 12 dell'estratto).

¹¹² Che qui si segue, anziché il testo del 1981 che pare troppo lontano nel tempo per essere guardato come testo di confronto con altri sistemi di regole a livello europeo ed internazionale a noi contemporanei. Il testo della revisione qui preso a riferimento è la versione consolidata del settembre 2016.

¹¹³ Si è osservato che il processo di revisione della Convenzione va verso un irrigidimento della maggior parte dei principi impiegati nella tutela dei dati e ne aggiunge di nuovi in linea con la disciplina europea. Prevede poteri più forti per le autorità di supervisione, sanzioni giudiziali e non giudiziali, e rimedi per le violazioni che accrescono i requisiti di *enforcement* domestico. GREENLEAF, *op. cit.*, p. 10.

consenso libero, specifico, informato ed inequivocabile della persona interessata o in virtù di altre basi legittime previste dalla legge. Viene inoltre introdotta una nozione più ampia di trattamento dei dati rispetto al passato (art. 2, lett. *b*) se pure, per altro verso, il campo di applicazione della Convenzione esclude il trattamento dei dati da parte di persone fisiche per uso esclusivamente personale e domestico (art. 1 *bis*)¹¹⁴. Il trattamento dei dati dev'essere proporzionato al legittimo scopo perseguito e riflettere ad ogni stadio del trattamento un equo bilanciamento degli interessi implicati, e dei diritti e delle libertà in gioco (art. 5, 1° co.). I dati devono essere trattati in modo corretto e trasparente (e l'art. 7 *bis* è espressamente dedicato alla trasparenza del trattamento), raccolti per finalità esplicite, determinate e legittime, trattati in modo compatibile con queste finalità, e in maniera adeguata, pertinente e non eccessiva rispetto alle finalità per le quali sono trattati (art. 5, 4° co.). Sono previste norme sul trattamento dei dati sensibili che comprendono esplicitamente i dati genetici e biometrici (art. 6), e sulla sicurezza dei dati (art. 7)¹¹⁵. Vengono quindi previsti diversi diritti dell'interessato come quello di non essere oggetto di una decisione che abbia ripercussioni notevoli e che sia stata presa unicamente sulla base di un trattamento automatizzato dei suoi dati, di ottenere conferma di un trattamento dei dati che lo concernono, di essere informato del ragionamento sottostante il trattamento dei dati¹¹⁶, di opporsi al trattamento dei dati che lo concernono, di ottenere la rettifica e la cancellazione dei dati, di disporre un ricorso conformemente all'art. 10 in caso di violazione dei diritti previsti dalla Convenzione, di beneficiare dell'assistenza di un'autorità di controllo secondo l'art. 12 *bis* della Convenzione (art. 8). Il testo della Convenzione prosegue prevedendo l'impegno di ogni parte a mettere in atto appropriate sanzioni e ricorsi giurisdizionali e non

¹¹⁴ Una tale esclusione risulta discussa data la diffusività oggi dell'utilizzo di Internet ed il conseguente trattamento dei dati personali, anche per scopi non immediatamente professionali e commerciali.

¹¹⁵ Nell'ambito della sicurezza dei dati, in particolare, vengono introdotte due rilevanti previsioni, non contemplate nel testo del 1981: il 2° co. dell'art. 7 prevede che gli Stati debbano controllare che il titolare del trattamento comunichi ogni violazione dei dati personali (*data breach*) alle autorità di vigilanza; e l'art. 8 *bis*, che elenca misure addizionali a tutela dei dati. Tra queste figura, al 2° co., un nuovo ed importante onere in capo al titolare del trattamento, il quale è tenuto a condurre una valutazione del potenziale impatto del trattamento sui

diritti e le libertà fondamentali dei soggetti interessati, predisponendo un piano operativo che consenta di ridurre al minimo il rischio di interferenza tra il trattamento e i diritti di questi ultimi. Tali disposizioni sono tuttavia derogabili ai sensi dell'art. 9, che prevede che vi si possa derogare per previsione normativa o per motivi di sicurezza nazionale, per gli interessi economici e finanziari dello Stato, per la repressione dei reati o, infine, per la protezione del soggetto interessato e dei diritti e libertà di terzi, in particolare della libertà d'espressione.

¹¹⁶ Tanto corrisponde all'impostazione data nel nuovo Regolamento 2016/679 là dove prevede che agli interessati debbano essere forniti elementi di conoscenza relativi alla "logica" del trattamento, come visto *supra*, par. 4.

giurisdizionali per le violazioni delle disposizioni nazionali che danno effetto alle previsioni della Convenzione (art. 10).

Relativamente al trasferimento transfrontaliero dei dati una parte non può, per il solo scopo di protezione dei dati personali, proibire o sottoporre a speciale autorizzazione il trasferimento dei dati verso un ricevente che è soggetto alla giurisdizione di altra parte della Convenzione. Mentre se il ricevente è soggetto alla giurisdizione di uno Stato o di un'organizzazione internazionale non parte della Convenzione, il trasferimento dei dati può avere luogo soltanto quando sia garantito un livello adeguato di protezione dei dati personali in base alle disposizioni della Convenzione (art. 12) ¹¹⁷. In maniera simile alle previsioni del nuovo Regolamento europeo, un livello di protezione dei dati adeguato può essere garantito dalla legislazione dello Stato terzo o dell'organizzazione internazionale, o da garanzie contrattuali specifiche o standardizzate; inoltre, sempre similmente alla disciplina europea, sono previste una serie di deroghe a tale generale riferimento all'adeguatezza.

Le parti della Convenzione devono provvedere ad avere una o più autorità responsabili di assicurare l'osservanza delle misure della legge nazionale che danno effetto ai principi della Convenzione (art. 12 *bis*) e si accordano per rendersi reciproca assistenza nell'implementazione della Convenzione (art. 13). La Convenzione prevede inoltre agli artt. 18 ss. un Comitato che ha tra le altre funzioni quella di fare raccomandazioni per facilitare o migliorare l'applicazione della Convenzione, di valutare, su richiesta di uno Stato o di un'organizzazione internazionale, se il loro livello di protezione dei dati personali è conforme alle disposizioni della Convenzione, e di raccomandare se del caso le misure da adottare per raggiungere tale conformità.

5.2. (segue) *Le Linee Guida dell'Ocse.*

Linee Guida per la protezione della *privacy* e per il flusso transfrontaliero dei dati dal carattere non vincolante ha formulato l'Ocse, l'Organizzazione per la cooperazione e lo sviluppo economico, che conta 35 Paesi membri ¹¹⁸. La prima versione delle Linee Guida del 1980 (che rappresenta il primo accordo

¹¹⁷ Nelle prime versioni del testo della revisione lo standard generale dell'adeguatezza della protezione dei dati era stato sostituito con quello dell'"appropriata" protezione. Quest'ultimo standard era stato criticato per il rischio dell'abbandono di una certa e significativa restrizione nel trasferimento dei dati a favore della strategia degli Stati Uniti di spingere verso l'interoperabilità di standard molto differenti di prote-

zione, cfr. GREENLEAF, *op. cit.*, p. 8 dell'estratto.

¹¹⁸ Oltre a Paesi dell'area europea ne fanno parte anche Paesi di altre aree del mondo come, tra gli altri, Messico, Corea del Sud, Canada, Usa, Giappone, Australia. L'Ocse fu fondata nel 1948, l'ultimo Paese ad aderirvi è stata la Lettonia nel 2016.

internazionale sui principi condivisi in materia di *privacy*) è stata rivista nel 2013 (*Oecd Guidelines governing the protection of Privacy and Transborder Flows of Personal Data*) alla luce del progresso tecnologico, informatico e telematico della società ¹¹⁹. Tali Linee Guida che — come detto — non hanno portata vincolante ¹²⁰ indicano ai Paesi membri principi per la tutela dei dati personali, concentrandosi anche sulle problematiche di gestione del rischio e della sicurezza, sui profili inerenti al trasferimento dei dati e più in generale sulla dimensione globale della loro protezione attraverso una migliore interoperabilità. Con la Raccomandazione sulle *Guidelines* il Consiglio dell'Ocse si rivolge agli Stati membri con l'indicazione di dimostrare impegno e guida nella protezione della *privacy*, implementare le *Guidelines*, e diffondere la medesima Raccomandazione (che porta in allegato le *Guidelines*) nei settori pubblico e privato.

Le *Guidelines* si indirizzano ai dati personali rispetto ai quali o per le modalità del trattamento, o per la loro natura, o per il contesto in cui sono utilizzati, si pone un rischio per la *privacy* e per le libertà personali (par. 2). Esse si propongono come un minimo standard che può essere accompagnato da misure addizionali per la protezione della *privacy* e delle libertà individuali relative al flusso transfrontaliero dei dati (par. 6). È previsto che siano posti dei limiti alla raccolta dei dati e che i dati siano ottenuti, qualora risulti appropriato, con il consenso o la conoscenza dell'interessato (par. 7). I dati personali devono essere rilevanti per gli scopi per i quali sono utilizzati e nei limiti necessari agli scopi, i dati debbono essere accurati, completi e tenuti aggiornati (par. 8). Gli scopi per i quali i dati vengono raccolti debbono essere specificati nel momento della raccolta e l'utilizzo dei dati limitato al raggiungimento di tali scopi (par. 9). I dati personali non possono essere resi noti, resi disponibili o altrimenti utilizzati per scopi diversi da quelli specificati in linea

¹¹⁹ L'Ocse ha elaborato altri strumenti in materia di *privacy*: la *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy* del 2007, la *Recommendation on Principles for Internet Policy Making* del 2011. Nel processo di revisione delle *Guidelines* del 1980 nella nuova versione del 2013 l'Ocse ha inoltre elaborato due report, "*The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines*" del 2011 e "*Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation*" pure del 2011.

¹²⁰ Le linee guida fanno parte di quel complesso di norme, regole e principi non dotati di efficacia cogente, ma aventi una

particolare rilevanza a livello politico: ciò significa che essi non danno vita ad obblighi giuridici in capo a chi li applica o vi aderisce, ma svolgono una funzione ausiliaria di indirizzo, con l'obiettivo di colmare lacune normative e di fornire un modello flessibile che possa essere adottato dalla maggior parte degli ordinamenti nazionali. Tali strumenti si classificano come *soft law*. Si v. SNYDER, *Soft law and Institutional practice in the European Community Law*, in MARTIN (a cura di), *The construction of Europe: Essays in Honour of Emile Noel*, Dordrecht, Kluwer Academic Publishers, 1994, p. 198, ove si riferisce alle regole di *soft law* come a "rules of conduct which, in principle, have no legally binding force but which nevertheless may have practical effects".

con il par. 9, salvo che su consenso dell'interessato o per previsione di legge (par. 10). I dati personali devono essere protetti da adeguati mezzi di sicurezza (par. 11). In particolare, il par. 15 prevede che tra gli oneri del titolare del trattamento vi sia quello di predisporre il c.d. *privacy management programme*, ossia un vero e proprio complesso di misure tecniche ed organizzative a salvaguardia della *privacy* elaborato sulla base della tipologia e del volume delle operazioni di trattamento e della natura dei dati. In capo al titolare del trattamento sussiste l'ulteriore onere di dimostrare l'adeguatezza del "piano" da lui predisposto, nonché quello di notificare alle autorità competenti ogni eventuale violazione della sicurezza che possa avere un qualche impatto sui dati personali.

Sono poi previsti taluni diritti a protezione dell'interessato e dei suoi dati personali, tra cui quelli di ottenere conferma dal titolare del trattamento della presenza dei suoi dati, nonché di chiedere la cancellazione, la rettifica, la completezza o la correzione dei dati (par. 13). Nell'implementare i detti principi gli Stati membri devono sviluppare strategie che riflettono un approccio coordinato tra i diversi organi di governo, devono adottare leggi di tutela della *privacy*, devono stabilire e mantenere delle *authority* che assicurino efficacia alla tutela dei dati personali, incoraggiare e supportare l'autoregolazione, adottare mezzi efficaci di protezione individuale, e adeguate sanzioni e rimedi (par. 19).

Rilevante è il principio in base al quale il titolare del trattamento rimane responsabile dei dati che tratta, a prescindere dalla loro localizzazione e, dunque, anche in caso di trasferimento degli stessi (art. 16). In questo ambito, le *Guidelines* paiono abbastanza flessibili nel prevedere che il trasferimento dei dati non possa essere impedito se lo Stato terzo ricevente aderisca ai principi ivi stabiliti o assicuri sufficienti garanzie attraverso un livello di protezione conforme a quello delle Linee guida (art. 17). Eventuali restrizioni ai flussi transfrontalieri di dati sono infatti ammesse solo se proporzionate al rischio, alla natura dei dati e agli scopi del trattamento (art. 18).

Anche gli Stati membri svolgono un ruolo attivo nella protezione dei dati oggetto di trasferimento, dovendo adottare misure appropriate per facilitare la cooperazione nella tutela transfrontaliera dei dati personali e incoraggiare e supportare lo sviluppo di accordi internazionali che promuovano l'interoperabilità tra le strutture quadro di tutela della *privacy* che diano pratico effetto alle Linee Guida (parr. 20 e 21). Questo nella prospettiva attuale, nella quale il flusso transfrontaliero dei dati — come indica l'*Explanatory Memorandum* alle *Guidelines* Ocse — è cambiato rispetto al 1980, quando era legato a trasmissioni puntuali tra imprese e enti governativi. I dati oggi giorno possono essere trattati simultaneamente in più luoghi, sparsi per essere immagazzinati in tutto il globo, ricombinati istantaneamente, trasferiti

attraverso le frontiere dai singoli individui a mezzo dei loro supporti mobili; e servizi come il *cloud computing* consentono alle organizzazioni e ai singoli individui di accedere ai dati che possono essere depositati ovunque nel mondo.

Nel 2016 l'Ocse ha inoltre adottato una nuova versione della Raccomandazione sulla tutela del consumatore nel commercio elettronico ¹²¹ (*Consumer Protection in E-Commerce*) introducendo — tra i profili chiave della revisione — due nuove previsioni in materia di tutela della *privacy* e dei dati personali che mettono in rilievo specifiche esigenze di protezione di particolare importanza per l'*e-commerce* tra professionista e consumatore, considerato che i dati personali dei consumatori sono al cuore di molti servizi del commercio elettronico e che ciò incrementa i rischi relativi alla tutela dei dati personali e alla loro sicurezza. Sono dedicati alla *privacy* e alla sicurezza i parr. 48 e 49 della Raccomandazione. Il par. 48 prevede che i professionisti devono tutelare la *privacy* dei consumatori assicurando che le loro pratiche relative alla raccolta ed uso dei dati siano conformi alla legge, trasparenti e conformi a correttezza, e consentano la partecipazione e la scelta del consumatore, introducendo sufficienti cautele quanto alla sicurezza. Il par. 49 prevede che i professionisti devono far fronte ai rischi di sicurezza digitale ed introdurre misure di sicurezza per ridurre o mitigare gli effetti negativi della partecipazione del consumatore al commercio elettronico.

5.3. (segue) *Il Privacy Framework dell'APEC.*

Un *Privacy Framework* composto da regole non vincolanti è stato approvato nel 2004 anche nel contesto dell'APEC, *Asia-Pacific Economic Cooperation*, che raccoglie 21 economie dell'area dell'Asia e del Pacifico ¹²². Come dice l'introduzione al documento tali regole, che sono simili alle Linee Guida Ocse quanto alla loro forza giuridica, sono state adottate in quanto i

¹²¹ L'Ocse aveva adottato il primo strumento internazionale per la protezione del consumatore nel commercio elettronico ("*Consumer Protection in the Context of Electronic Commerce*") con una Risoluzione del 1999, della quale la Raccomandazione del 2016 rappresenta una revisione. La Raccomandazione si rivolge agli Stati membri dell'Ocse e agli Stati non membri aderenti alla Raccomandazione affinché lavorino nei rapporti con i soggetti professionali, i rappresentanti dei consumatori ed altre organizzazioni della società civile in maniera trasparente ed inclusiva per l'implementazione dei principi della Raccomandazione nelle loro *policy* dirette alla prote-

zione del consumatore nel commercio elettronico.

¹²² L'*Asia-Pacific Economic Cooperation* (APEC) è un organismo nato nel 1989 per favorire la cooperazione e la crescita economica, il libero scambio e gli investimenti nell'area asiatico-pacifica. Tale area coincide non solo con l'Asia Pacifica ma con l'intero *Pacific Rim* (anello del Pacifico). Si definisce come organismo e non come organizzazione internazionale in quanto è composto da economie e non da Stati, ed è privo di una piena personalità giuridica. Ne fanno parte Australia, Brunei, Canada, Cile, Cina, Indonesia, Giappone, Repubblica di Corea, Hong Kong, Malesia, Messico, Nuova Ze-

membri APEC riconoscono il grosso potenziale del commercio elettronico quale mezzo di espansione delle opportunità economiche, di riduzione dei costi, aumento dell'efficienza, miglioramento della qualità della vita, e facilitazione di una maggiore partecipazione delle piccole imprese al commercio globale, ritenendo che un quadro di riferimento che consenta trasferimenti di dati a livello regionale sia foriero di benefici per consumatori, imprese e governi. L'approvazione del *Privacy Framework* ha appunto il significato dell'acquisizione di consapevolezza da parte delle economie membri dell'APEC di quanto sia importante lo sviluppo di un'effettiva protezione della *privacy* per assicurare la continuità del commercio e la crescita economica nella loro regione, evitando barriere ai flussi informativi (Preambolo, punto 1). Un ruolo chiave viene riconosciuto anche alla cooperazione sia nella promozione dell'effettiva protezione della *privacy* delle informazioni che del libero flusso delle informazioni nella regione asiatico-pacifica nello sforzo di migliorare la fiducia dei consumatori e la crescita del commercio elettronico ¹²³ (Preambolo, punto 1). I principi contenuti nel *Framework* sono stati elaborati in un contesto — quello della cooperazione economica asiatico-pacifica — in cui alcuni Paesi ed economie hanno leggi o pratiche sulla *privacy* ben consolidate mentre altri sono nella fase della presa di coscienza della questione ¹²⁴. In questo contesto di diversità il *Framework* è stato elaborato appunto per promuovere un approccio coerente tra i regimi di tutela della *privacy* delle informazioni nelle economie dell'area (Commento al principio 9) considerato che anche nelle economie dei Paesi che hanno una

landa, Papua Nuova Guinea, Perù, Filippine, Russia, Singapore, Taiwan, Thailandia, Stati Uniti, Vietnam.

¹²³ Il riconoscimento della portata economica della disciplina di tutela della *privacy* e dei dati personali figura anche tra le ragioni alla base del processo di riforma della disciplina europea adottata con il Reg. 2016/679.

¹²⁴ A titolo di esempio tra i Paesi delle economie APEC il Cile è stato il primo Paese dell'America latina a dotarsi di una normativa generale in materia di protezione dei dati personali, la *Ley n. 19.628 sobre protección de la vida privada* del 1999, riformata più volte ma ritenuta obsoleta e inadeguata, mancando tra l'altro nel Paese un'autorità garante per la protezione dei dati personali. Si è recentemente annunciato una riforma della regolazione in materia per evitare gli effetti negativi di una normativa inadeguata sulla sfera dei rapporti commerciali con gli altri Paesi, seppure risulta che le imprese cilene si siano basate sugli standard internazionali per il

trattamento ed il trasferimento dei dati. Il Perù ha adottato solo nel 2011 una normativa generale in materia di protezione dei dati personali ispirata al modello europeo, la *Ley de Protección de Datos Personales*, entrata in vigore nel 2015. LEIVA, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, in *International Law News*, IV/2012, Vol. 41, disponibile all'indirizzo web http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latina_america_survey_legal_approaches.html.

Quanto alla Cina, si tratta di un Paese che non è in grado al momento di offrire un adeguato livello di sicurezza in materia di protezione dei dati personali. Un divieto assoluto dei flussi di dati personali con la Cina sarebbe comunque impraticabile date le sempre più intense relazioni commerciali e il crescente uso di servizi *online*, i cui *datacenter* sono sovente localizzati in territorio cinese. Tuttavia, la Cina non ha ancora adottato una legislazione in materia di

disciplina consolidata non ricorre, comunque, un modo esattamente identico di regolare il trattamento delle informazioni personali. Il *Framework* si applica ai dati personali delle persone fisiche — e non delle persone giuridiche — quali informazioni personali che possono essere utilizzate per identificare una persona, includendo anche le informazioni che non presentano tale requisito ma che, quando associate ad altre informazioni, possono identificare una persona. Esso, che è compatibile con i principi generali delle *Guidelines* Ocse del 1980 (Preambolo, punto 5), ha per carattere distintivo di focalizzare l'attenzione sulla protezione pratica e coerente della *privacy* delle informazioni, e per fare ciò bilancia le necessità di tutela della *privacy* con i bisogni delle attività d'impresa e gli interessi commerciali, e allo stesso tempo tiene conto delle diversità culturali e delle altre differenze tra le economie membre (Preambolo, punto 6).

5.4. (segue) *I Core Principles individuati dall'UNCTAD nel 2016.*

Nello studio dell'UNCTAD dell'aprile 2016, già sopra citato, si afferma che di fronte alla mancanza, oggi, di un modello condiviso di protezione di dati personali, è la compatibilità l'obiettivo prefissato di molte iniziative a livello globale e regionale. Lo studio riassume lo stato dell'arte sulla regolazione del trattamento dei dati personali nella specifica ottica della delicatezza della questione per lo sviluppo delle relazioni economiche globali in rapporto all'incremento dell'importanza del commercio elettronico e in considerazione della disomogeneità della disciplina della materia nelle diverse aree del mondo, che crea incertezza. Altro

protezione dei dati personali e le uniche disposizioni esistenti sono di tipo settoriale, tra le quali la c.d. *Decision on Internet Information Protection* ("2012 SC-NPC Decision"). Tale Decisione viene considerata di fatto lo standard di protezione dei dati personali in Cina e ad essa devono conformarsi tutti i regolamenti del Ministero dell'Industria e dell'*Information Technology*, sebbene la disciplina dettata paia lacunosa sotto molteplici profili. L'ambito di applicazione è soltanto quello digitale, non sono previsti meccanismi di attuazione, né sono riconosciuti diritti ai soggetti interessati dal trattamento dei dati personali, e la lista dei principi della normativa pare tralasciare alcuni principi cardine dettati invece dalla normativa europea. La protezione dei dati personali è contemplata solo in relazione alla figura della persona fisica-consumatore e non in capo a qualsiasi individuo-soggetto interessato, come avviene nella normativa europea. Tale ambito ristretto è giustificato dal fatto che in Cina la protezione dei dati

personali viene concepita come strumentale per lo sviluppo dell'*e-commerce* e non come diritto fondamentale a sé stante. Ciò è ulteriormente confermato dal fatto che il settore pubblico rimane pressoché sempre escluso dal campo di applicazione delle norme settoriali a protezione dei dati personali. Il quadro di tutela che si ottiene non è quindi reputato soddisfacente. GREENLEAF-TIAN, *Data Protection Widened by China's Consumer Law Changes*, in *Privacy Laws and Business International Report*, 2013, pp. 127-128. In Giappone vige il c.d. *Personal Information Protection Act* (entrato in vigore nel 2005 ed emendato nel 2014) che, da un lato, ha ampliato la definizione di dato personale includendo le informazioni biometriche come le impronte digitali ed il riconoscimento facciale e, dall'altro lato, ha introdotto un trattamento speciale per alcuni dati sensibili come il credo religioso, la provenienza, lo *status* e il casellario giudiziale, istituendo al contempo un'autorità indipendente prima non prevista.

problema sentito è quello della sicurezza nazionale e del bilanciamento tra sorveglianza e tutela dei dati personali ¹²⁵.

Nonostante le significative divergenze sugli aspetti specifici delle normative a tutela dei dati personali nei diversi sistemi giuridici nel mondo, lo studio mette in rilievo che alcuni principi cardine di protezione dei dati sono condivisi da leggi nazionali e regolazioni internazionali, ritenendo che tale *set* di principi condivisi possa servire da punto di partenza per l'acquisizione di una maggiore compatibilità ed armonizzazione tra i diversi sistemi ¹²⁶.

Lo studio riconosce che vi sono all'attenzione più profili critici in merito alla protezione dei dati personali e della *privacy* provenienti da più parti, da parte dei consumatori e della società civile, così come dei soggetti professionali e dei governi ¹²⁷. La sfida per le discipline a protezione dei dati personali e della *privacy* è quella di bilanciare tali tre differenti serie di preoccupazioni ed interessi, ciò che è idealmente da fare in modo da non ostacolare in maniera non necessaria i rapporti commerciali. Lo studio esprime la posizione secondo la quale al fine di facilitare il commercio transfrontaliero *online* è essenziale cercare soluzioni che risultino compatibili a livello internazionale. Come lo studio mostra, il sistema esistente non è soddisfacente e la situazione ha bisogno di essere affrontata urgentemente in vista dell'incremento delle attività economiche e sociali sulla rete Internet e dell'introduzione di nuove tecnologie, e in tale prospettiva si cerca di identificare possibili modi di intervento nella direzione di un sistema che riconosca un appropriato bilanciamento tra la protezione dei dati e il trasferimento del flusso di dati personali ¹²⁸. Al fine di acquisire un'adeguata protezione che faciliti il commercio e l'innovazione è essenziale continuare il dialogo tra i diversi interessati a livello nazionale, regionale e globale, e le organizzazioni internazionali come l'UNCTAD possono offrire una piattaforma per tale dialogo ¹²⁹.

I *Core Principles* che si individuano come riconosciuti in maniera diffusamente condivisa sono: l'apertura, nel senso dell'apertura delle aziende rispetto alle loro pratiche sui dati personali; la limitazione nella raccolta dei dati, che deve seguire i principi della limitazione, liceità e correttezza, di solito previa conoscenza e/o consenso; la specificazione dello scopo; la limita-

¹²⁵ "Data protection regulations and international data flows: Implication for trade and development", UNCTAD, 2016, p. XI ss., 10 ss., 15 s.

¹²⁶ "Data protection regulations and international data flows: Implication for trade and development", cit., p. 56.

¹²⁷ Si sono già segnalati *supra*, nota 102.

¹²⁸ "Data protection regulations and international data flows: Implication for trade and development", cit., p. 56.

¹²⁹ "Data protection regulations and international data flows: Implication for trade and development", cit., p. 14.

zione dell'uso allo scopo; la sicurezza; la qualità dei dati, che devono essere rilevanti, accurati e aggiornati; l'accesso e la correzione; la responsabilità (*accountability*). Questi otto principi figurano in qualche forma in tutti i più importanti accordi internazionali e regionali e nelle linee guida sulla protezione dei dati. Un principio aggiuntivo, quello della minimizzazione dei dati, appare solo nella disciplina europea, riconosciuto prima sotto la forma di principio di necessità nel trattamento dei dati nell'art. 3 della dir. 95/46, e ora nel Regolamento europeo nell'art. 5¹³⁰.

Le principali sfide nello sviluppo di leggi di protezione dei dati invece risiedono, secondo lo studio: nell'affrontare i vuoti di protezione, nel far fronte alle nuove tecnologie, nel regolare le restrizioni al trasferimento transfrontaliero dei dati, nel bilanciare sorveglianza e protezione, nel rafforzare l'*enforcement*, nella determinazione della giurisdizione, nel gestire il peso dell'ottemperanza alla disciplina della *privacy*¹³¹.

6. CONCLUSIONI. DA REGOLE EUROPEE DI DIRITTO INTERNAZIONALE PRIVATO A PRINCIPI DI TUTELA DEI DATI PERSONALI DI FORMAZIONE INTERNAZIONALE.

Nella definizione della legge applicabile al trattamento transfrontaliero dei dati personali la norma di cui all'art. 4, 1° co. lett. *a* dir. 95/46 sulla nozione di « stabilimento » è stata interpretata dalla Corte di Giustizia tenendo conto delle caratteristiche dei rapporti che si realizzano oggi attraverso i mezzi telematici, allontanandosi con ciò dalla concezione più classica di « stabilimento » come criterio di collegamento fondato su canoni tradizionali, come quello della territorialità, come si è visto sopra al par. 2. Attraverso la previsione secondo la quale la disciplina europea si applica « indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione » il nuovo Regolamento si è distaccato definitivamente da profili di collocazione territoriale del trattamento dei dati.

Per altro verso, per quanto concerne l'altro profilo della regolazione transfrontaliera dei dati personali relativo al trasferimento verso Paesi terzi esso è legato a dei canoni, come quello del controllo dell'adeguatezza della disciplina del Paese terzo e della decisione sull'adeguatezza di clausole standard da parte della Commissione europea, che poco si adattano ad un flusso di dati quale quello che si reputa conveniente allo sviluppo delle attività

¹³⁰ Che tra i principi applicabili al trattamento dei dati personali prevede alla lett. *c* che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati).

¹³¹ “*Data protection regulations and international data flows: Implication for trade and development*”, cit., p. 56 ss.

economiche nel mondo contemporaneo. Se pure il sistema del trasferimento dei dati nella disciplina europea fondato sull'adeguatezza riceve una più dettagliata regolazione nel nuovo Regolamento rispetto alla dir. 95/46, risultando anche significativamente ampliato il novero degli strumenti ammessi ad attestare una protezione "adeguata", mentre d'altro canto tale tramandato canone dell'adeguatezza riceve molte eccezioni, non viene introdotta nel Reg. n. 2016/679 una nuova e diversa impostazione del regime di trasferimento dei dati. Una simile impostazione giustifica l'affermazione secondo la quale "come una cittadella medievale l'Unione europea ha creato, con il suo quadro regolativo comune della tutela dei dati personali, un muro legale sulle informazioni relative ai cittadini europei e soltanto pochi varchi di accesso al prezioso patrimonio rappresentato dai dati personali"¹³².

Si è anche messo in rilievo che non sono stati sempre eseguiti controlli sull'effettiva adeguatezza del concreto trattamento dei dati oggetto di trasferimento, come ha attestato l'esperienza applicativa dell'accordo *Safe Harbour*, relativamente al quale si è accertato che i controlli della sua osservanza da parte degli operatori aderenti si sono manifestati non effettivi¹³³. Rispetto alle decisioni di adeguatezza sulle legislazioni dei Paesi terzi e sulle *Standard Contractual Clauses* si è osservato inoltre come non vi sia nessuna evidenza di come le istituzioni europee monitorino l'effettivo rispetto delle legislazioni sui dati personali negli Stati terzi e se esse monitorino le modifiche di tali normative coperte dalla decisione di adeguatezza e delle relative pratiche applicative, così come l'adeguamento del livello di protezione da parte del Paese terzo, non escluso nel caso in cui si adottino delle *Standard Clauses*¹³⁴. Ciò ha portato a concludere che le previsioni europee sul trasferimento dei dati e sulla sovranità sui dati europei paiono avere principalmente natura declaratoria, come dimostrano l'esperienza di una tutela più formale che reale dei dati personali in più Paesi europei e la mancanza di controllo

¹³² MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignty on personal data*, in *Contr. impr./Eur.*, 2016, p. 339.

¹³³ MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignty on personal data*, cit., p. 340, nel senso che un gran numero di organizzazioni e società avevano fatto falsa dichiarazione di attenersi al contenuto dell'accordo *Safe Harbour*.

¹³⁴ MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignty*

on personal data, cit., p. 341. Inoltre, in linea con l'adozione delle clausole, gli "esportatori" di dati dovrebbero fermare ogni trasferimento di dati o fornire ulteriori garanzie qualora venissero a conoscenza che le normative straniere possano avere effetti avversi sulle garanzie date con le clausole. Tuttavia, le *Standards Clauses* sono spesso adottate dalle imprese europee in base ad un approccio "copia e incolla" senza alcun controllo delle norme imperative che potrebbero incidere sulla *compliance* delle terze parti aventi sede fuori dall'Unione europea.

sull'*enforcement* delle soluzioni contrattuali per il trasferimento transfrontaliero dei dati ¹³⁵.

La regolazione europea si pone come un modello di tutela dei dati personali, in via di principio, tra i maggiormente protettivi dei diritti sui dati personali degli interessati, e come un modello dalla portata espansiva. Sia perché questo corrisponde alle indicazioni provenienti dalla giurisprudenza della Corte di Giustizia dell'Unione europea ¹³⁶ e dalla disciplina del nuovo Reg. 2016/679, volti ad assicurare in ogni caso agli interessati che si trovano nell'Unione la protezione secondo la disciplina europea, sia perché rappresenta un modello cui gli Stati terzi guardano quale esempio, come avviene da parte dei Paesi in via di sviluppo nel momento in cui elaborano una loro normativa di tutela dei dati personali ¹³⁷.

Il modello europeo di protezione dei dati personali si pone come forte e compiuto anche nelle intenzioni a livello politico ¹³⁸, e con l'effettiva applicazione del nuovo Regolamento conseguirà l'importante obiettivo di rappresentare una disciplina comune a tutti i Paesi europei ¹³⁹, con un'unica autorità garante di riferimento (*European Data Protection Supervisor*, EDPS) — già in precedenza operante oltre alle autorità garanti nazionali — e un comitato centralizzato di collaborazione tra le autorità garanti

¹³⁵ MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignty on personal data*, cit., p. 344, « the EU provisions on data flows, and on EU data sovereignty, seem to have mainly a declaratory nature, as demonstrated by the more formal than real safeguard of personal data existing in many EU countries and by the lack of control on the enforcement of the contractual solutions for trans-border data transfer ». Sul sistema di protezione europeo rispetto al trasferimento dei dati si v. *supra*, nota 64, anche le considerazioni di Kuner.

¹³⁶ Questo era comunque già in applicazione della dir. 95/46, come interpretata dalla Corte di Giustizia. Ricordano infatti D'ANTONIO-SICA, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in RESTA-ZENO ZENGOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai Safe Harbour Principles al Privacy Shield*, Roma Tre-Press, Roma, 2016, p. 138, che « la scelta di *policy* dell'Unione, sotto questo profilo, è stata quella di porsi quale modello forte di tutela della riservatezza, imponendo a qualunque esportatore di dati personali di origine comunitaria di confrontarsi con lo schema normativo europeo, garantendo alle informazioni in transito un livello di tutela particolarmente ele-

vato, modellato appunto sul paradigma della direttiva 95/46/CE ».

¹³⁷ Cfr. a questo ultimo riguardo lo Studio dell'UNCTAD del 2016, cit., p. 12.

Anche se, per altro verso, un elevato livello di protezione dei dati personali viene talvolta riguardato come problematico rispetto all'obiettivo della condivisione in maniera diffusa del suo modello. Come si è visto *supra*, a nota 113, si teme ad esempio relativamente alla nuova versione della Convenzione n. 108 del Consiglio d'Europa che un'impostazione troppo stringente in termini di tutela sia di ostacolo alla condivisione in maniera più diffusa della Convenzione a livello internazionale. È da notare comunque che il considerando n. 4 del Reg. 2016/679 contiene un interessante principio di "bilanciamento" affermando che « il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerata alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ottemperanza del principio di proporzionalità », su cui A. RICCI, *Sulla « funzione sociale » del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2017, p. 586.

¹³⁸ MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignty on personal data*, cit., p. 344.

¹³⁹ Seppure con i limiti di cui si è detto *supra*, nota 66.

nazionali (*European Data Protection Board*, EDPB) ¹⁴⁰. Tale modello, con i suoi effetti sui flussi di dati a livello internazionale, si propone anche come uno strumento per rafforzare la *leadership* europea rispetto alla formulazione di una regolazione globale sulla protezione dei dati — si è osservato —, piuttosto che come una semplice garanzia di un effettivo standard di protezione elevato. La natura politica del modello di regolazione europea che è stato realizzato è quindi da comprendersi collocandolo nel più ampio contesto della dimensione globale della protezione dei dati composta da più *stakeholders*, diverse aree economiche (USA, Europa, Cina, ecc.) e differenti organizzazioni (COE, APEC, OECD, UN) ¹⁴¹, di cui si è avuto un saggio nei precedenti parr.

Si è visto sopra che è in corso un processo verso l'elaborazione di principi comuni a livello internazionale in materia di protezione dei dati personali, dettato dall'evidenziata necessità di sviluppare delle regole dalla portata globale per un problema dal carattere globale quale quello della tutela dei dati personali su Internet. Ed è su questo processo che si concentrano le prospettive di maggiore novità nella regolazione della tutela dei dati personali per il prossimo futuro, al di là dei profili di immediata attualità dell'entrata in vigore del nuovo Regolamento europeo e degli strumenti di regolazione dei trasferimenti di dati personali dall'Europa agli Stati Uniti.

Su questo processo di elaborazione di principi a livello internazionale — si è visto — si concentra l'attività di più organizzazioni internazionali (come il Consiglio d'Europa, l'Ocse, l'UNCTAD) ed il dibattito nelle sedi delle conferenze a livello internazionale ed europeo delle Autorità Garanti, di modo che il trattamento transnazionale dei dati personali ed il trasferimento dei dati personali verso Paesi terzi risultino realizzabili in base a regole comuni o quantomeno in base a principi comuni ¹⁴², dando spazio allo sviluppo delle attività economiche che implicano il trattamento dei

¹⁴⁰ Mette in evidenza l'importanza di questo nuovo elemento del Regolamento europeo di recente adozione LINSKEY, *The "Europeanisation" of Data Protection Law*, in *Cambridge Yearbook of European Legal Studies*, 2016, p. 1 ss. dell'estratto. La EDPB sarà un comitato centralizzato che fornirà coordinamento e coerenza alle azioni delle autorità di sorveglianza attraverso meccanismi vincolanti. Tale *Board* sostituirà il lavoro del Gruppo Art. 29 e sarà un organo indipendente con la propria personalità giuridica il cui ruolo primario risiede nel contribuire ad un'applicazione coerente del Regolamento in tutta l'Unione europea, nel fare da referente consultivo per la Commissione sul livello di protezione offerto da Stati terzi od organizzazioni internazionali,

e nel promuovere la cooperazione tra le autorità nazionali.

¹⁴¹ MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignty on personal data*, cit., p. 344.

¹⁴² Di fronte ai limiti che conosce classicamente la realizzazione di convenzioni internazionali, che consistono in primo luogo nella difficoltà di raccogliere un numero di adesioni sufficiente ad assicurare la reale diffusione e condivisione a livello internazionale dello strumento, constano oggi nel panorama internazionale regole dalla portata maggiormente flessibile, come le linee guida che si propongono ai Paesi membri o agli operatori, come in materia di tutela dei dati personali le sopra viste Linee Guida dell'Ocse e il *Privacy Framework* nel con-

dati personali a livello transfrontaliero, senza sacrificare per altro verso la protezione dei dati.

Di fronte alla formazione di principi e regole di conio internazionale per la protezione dei dati personali, ciò che merita attenzione sotto il profilo formale della regolazione dei fenomeni giuridici è che tali modelli di tutela dei dati personali a livello internazionale che, oggi sono *in nuce* e in via di formazione, sono espressione di un diverso e nuovo paradigma nella regolazione del trattamento dei dati personali a livello transfrontaliero rispetto a quello del passato. Essi segnano il passaggio dal dominio delle regole di diritto internazionale privato, quali sono anche quelle formulate dalle istituzioni europee quando servono a definire le norme applicabili per il trattamento ed il trasferimento dei dati nei rapporti con i Paesi terzi, verso principi e regole che si possono definire di diritto privato di formazione internazionale o di diritto privato internazionale *tout court* ¹⁴³, in quanto principi e regole di tutela dei dati personali che si propongono per essere condivise come comuni a livello globale ¹⁴⁴. Questa transizione verso un nuovo e diverso modello di regolazione del trattamento e della tutela dei dati personali nei rapporti transnazionali, come modello composto di principi e possibilmente di regole condivise a livello globale, rappresenta un passaggio che va guardato con il massimo interesse in quanto segue l'internazionalizzazione dei

testo dell'APEC (in altri ambiti si pensi alle Linee Guida Ocse indirizzate alle multinazionali per lo sviluppo della responsabilità sociale d'impresa). La medesima revisione della Convenzione n. 108 dichiara di volersi attestare al livello di formazione di regole di principio e anche l'intervento dell'UNCTAD è diretto alla formazione di regole e principi compatibili a livello internazionale.

¹⁴³ Tale idea di un diritto privato di formazione internazionale o, detto altrimenti, di un diritto privato internazionale, richiama il concetto di diritto internazionale dei privati proposto da DRAETTA, su cui si v. *supra*, nota 3. Con la differenza che nell'idea che qui si prospetta si vede classificato diversamente, a livello europeo, e non propriamente internazionale, il diritto privato di formazione europea, rispetto al quale è oramai acquisito negli ultimi decenni che esso sia andato ad integrare gli ordinamenti degli Stati membri dell'Unione europea. Se poi le norme europee di tutela dei dati personali venissero adottate a livello internazionale, perché scelte tra i diversi modelli che si propongono per la regolazione internazionale del trattamento dei dati personali, in tal caso allora ben si potrebbe par-

lare di diritto privato internazionale anche a proposito di tali norme.

¹⁴⁴ Con la precisazione di rilievo che al momento si tratta di principi e di regole di principio, e non propriamente di regole definite nel dettaglio, e così anche per la Convenzione n. 108, come si è visto *supra*, al par. 5.1. Relativamente alla formazione di un diritto privato uniforme a livello globale mette in evidenza BASEDOW, *Internationales Einheitprivatrecht im Zeitalter der Globalisierung*, in *RabelsZ*, 2017, p. 1 ss., p. 31, la sostanziale differenza tra le norme tradizionali contenute nelle convenzioni internazionali, dirette all'uniformazione, e le più recenti forme delle regole modello e dei principi che, se facilitano l'approssimazione spontanea delle norme, non procedono all'uniformazione del diritto. L'unico strumento che, come visto sopra nel testo di questo paragrafo, si propone anche per la potenziale adozione a disciplina dei rapporti a livello globale, e prevede norme definite — ruolo che associa a quello suo più immediato di procedere all'uniformazione delle regole di tutela dei dati personali a livello europeo — è il nuovo Regolamento europeo 2016/679.

rapporti giuridici della realtà contemporanea ¹⁴⁵. Merita perciò che si resti in osservazione al fine di riscontrare se dalle proposte di principi condivisi, cui oggi soprattutto si assiste, si arriverà all'adozione di vere e proprie regole di diritto di portata globale.

Abstract

Among the current most problematic issues about the protection of personal data are the transnational processing of personal data and the cross-border flows of personal data. This is a consequence of the massive use of the Internet for commercial relationships, which are often transnational, and the development of new information and communication technologies like cloud computing, big data and the Internet of Things that imply the transnational processing of personal data and their transfer abroad. The legal regulation of these situations comes from the dir. EC/95/46 and will soon come from the Reg. (EU) 2016/679 that incorporates some important decisions of the ECJ on the abovementioned topics. The new Reg. (EU) 2016/679 does not ground the implementation of the European protection of the personal data on the fact that the processing takes place in Europe — as it was under the EU dir. 95/46 — but on the fact that the offering of goods and services is directed to subjects settled in Europe or whose behaviour is monitored in Europe. The cross-border flow of personal data is grounded on the principle of adequacy of the protection of personal data in the specific foreign country and on its recognition by the European Commission through its decisions of adequacy. Furthermore, the cross-border flow can be lawful even under appropriate safeguards given by the controller or the processor.

Despite the next future implementation of the new Reg. (EU) 2016/679, a growing awareness is raising at the international level — within European and international Conferences of the Data Protection Authorities — that an effective solution for the protection of personal data can only be based upon a regulation which is given at the same international level and structured in international principles and rules. In fact, several initiatives are going on towards that objective: the renovation of the Council of Europe Convention n. 108, the OCSE Guidelines, the APEC Privacy Framework for the Asian-Pacific area, the UNCTAD Core Principles about some worldwide common core principles on

¹⁴⁵ E che si manifesta oggi anche in altri ambiti di regolazione dei diritti della persona che si dirigono verso l'internazionalizzazione delle regole, come ad esempio

quello della maternità surrogata, della raccolta, trattamento ed utilizzazione dei dati genetici, e del trapianto degli organi.

data protection. The Reg. (EU) 2016/679 offers itself a set of rules which have been thought also as a proposal for the elaboration of a common instrument for privacy protection at international level. This ongoing process shows an interesting and important development for the protection of personal data moving from rules of international private law — which are also the rules of the Reg. (EU) 2016/679 governing the transnational processing of personal data and their cross-border transfers — towards principles and rules of substantive private law protecting data created at the international level.