Consiglio dell'Unione europea

Bruxelles, 12 gennaio 2017
(OR. en)

5191/17

DATAPROTECT 3
JAI 18
RELEX 19
DIGIT 3
FREMP 2

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	12 gennaio 2017
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2017) 7 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO Scambio e protezione dei dati personali in un mondo globalizzato

Si trasmette in allegato, per le delegazioni, il documento COM(2017) 7 final.

All.: COM(2017) 7 final

COMMISSIONE
EUROPEA

Bruxelles, 10.1.2017
COM(2017) 7 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Scambio e protezione dei dati personali in un mondo globalizzato

1. INTRODUZIONE

La protezione dei dati di carattere personale è parte integrante del tessuto costituzionale comune dell'Europa ed è sancita dall'articolo 8 della Carta dei diritti fondamentali dell'UE. Da più di 20 anni riveste un ruolo fondamentale per il diritto dell'UE, dalla direttiva sulla protezione dei dati del 1995[1] ("la direttiva del 1995") all'adozione del regolamento generale sulla protezione dei dati[2] e della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia[3] nel 2016.

Come ha sottolineato il presidente Juncker nel suo discorso sullo stato dell'Unione del 14 settembre 2016, "*[e]ssere europei significa avere diritto alla protezione dei propri dati personali mediante rigorose leggi europee. [...] Perché in Europa ci teniamo alla riservatezza. Si tratta di una questione di dignità umana*."

L'esigenza di proteggere i dati personali non si limita tuttavia all'Europa. I consumatori di ogni parte del mondo hanno sempre più a cuore il valore della loro vita privata e le imprese, a loro volta, riconoscono che una solida tutela della vita privata conferisce loro un vantaggio concorrenziale, poiché accresce la fiducia nei loro servizi. Molte imprese, in particolare quelle che operano a livello mondiale, stanno allineando le loro politiche in materia di tutela della vita privata al regolamento generale sulla protezione dei dati, perché desiderano operare nell'UE e perché lo considerano un modello da seguire.

Allo stesso modo, diversi paesi e organizzazioni regionali al di fuori dell'UE, dai paesi del nostro immediato vicinato, all'Asia, all'America latina, all'Africa, stanno adottando una nuova normativa in materia di protezione dei dati o aggiornando quella vigente, al fine di cogliere le opportunità offerte dall'economia digitale a livello mondiale e di rispondere alla crescente domanda di una maggiore sicurezza dei dati e di tutela della vita privata. Anche se vi sono delle differenze tra paesi quanto all'impostazione e al livello di evoluzione normativa, ci sono segni di convergenza verso l'alto in relazione a importanti principi in materia di protezione dei dati, in particolare in determinate regioni del mondo[4]. Una maggiore compatibilità tra i diversi sistemi di protezione dei dati faciliterebbe i flussi internazionali di dati personali, anche a fini commerciali o di cooperazione tra le autorità pubbliche (come, ad esempio, per le attività volte a garantire il rispetto della legge). L'UE dovrebbe cogliere questa opportunità per

---

1 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

2 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1). Entrato in vigore il 24 maggio 2016, il regolamento si applica a decorrere dal 25 maggio 2018.

3 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89). Entrata in vigore il 5 maggio 2016, gli Stati membri dell'UE sono tenuti a recepire la direttiva nel proprio diritto nazionale entro il 6 maggio 2018.

4 Cfr. "Data protection regulations and international data flows: Implications for trade and development", UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

promuovere i suoi valori in materia di protezione dei dati e facilitare i flussi di dati incoraggiando la convergenza dei sistemi giuridici. Come annunciato nel programma di lavoro della Commissione[5], la presente comunicazione illustra quindi il quadro strategico della Commissione relativo alle "decisioni di adeguatezza", nonché ad altri strumenti per il trasferimento dei dati e a strumenti internazionali in materia di protezione dei dati.

2. IL PACCHETTO DI RIFORMA DELLA PROTEZIONE DEI DATI NELL'UE: UN QUADRO NORMATIVO MODERNO CHE ASSICURA UN ELEVATO LIVELLO DI PROTEZIONE A SOSTEGNO DEI FLUSSI INTERNAZIONALI DI DATI

La riforma della normativa dell'UE sulla protezione dei dati adottata nell'aprile 2016 istituisce un sistema che garantisce un livello elevato di protezione ed è aperto alle opportunità della società dell'informazione globale. Conferendo ai singoli un maggiore controllo sui propri dati personali, la riforma rafforza la fiducia dei consumatori nell'economia digitale. Con l'armonizzazione e la semplificazione del contesto giuridico, la riforma agevola le attività commerciali nell'UE sia per le imprese europee che estere, alleggerendone gli oneri, anche attraverso lo scambio di dati a livello internazionale. L'UE, che associa oggi l'apertura ai flussi internazionali di dati al massimo livello di protezione per le persone, ha il potenziale per diventare un centro nevralgico per i servizi di dati, i quali devono poter circolare liberamente e godere della fiducia dei cittadini.

2.1 Un quadro dell'UE in materia di protezione dei dati completo, unificato e semplificato

La riforma dell'UE istituisce un quadro completo che disciplina il trattamento dei dati personali nel settore privato e in quello pubblico, sia in ambito commerciale che in materia di attività di contrasto (rispettivamente, il regolamento generale sulla protezione dei dati e la direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia).

A norma del regolamento generale sulla protezione dei dati, da maggio 2018 vi sarà un unico insieme paneuropeo di norme a fronte delle 28 normative nazionali attuali. Il meccanismo di sportello unico di nuova costituzione garantirà che un'unica autorità per la protezione dei dati sarà responsabile della supervisione delle operazioni di trattamento dei dati a carattere transfrontaliero effettuate da un'impresa nell'UE, assicurando un'interpretazione coerente delle nuove norme. In particolare, nei casi a carattere transfrontaliero in cui sono coinvolte diverse autorità nazionali per la protezione dei dati, sarà adottata una decisione unica per assicurare che a problemi comuni corrispondano soluzioni comuni. Inoltre, il regolamento generale sulla protezione dei dati istituisce condizioni di parità fra le imprese europee e straniere, imponendo alle imprese che hanno sede fuori dell'UE di applicare le stesse regole cui sono tenute le imprese europee se offrono beni e servizi o monitorano il comportamento di persone nell'UE. Un maggiore livello di fiducia dei consumatori andrà a beneficio sia degli operatori commerciali dell'UE che di quelli esterni.

[5] Programma di lavoro della Commissione per il 2017 "Realizzare un'Europa che protegge, dà forza e difende", COM(2016) 710 final, del 25 ottobre 2016, pag. 12 e allegato I.

La direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia contempla norme comuni per il trattamento dei dati personali delle persone coinvolte in procedimenti penali, che si tratti di indiziati, vittime o testimoni, pur tenendo conto delle specificità del settore della polizia e della giustizia penale. L'armonizzazione delle norme in materia di protezione dei dati nel settore dell'attività di contrasto, in particolare le norme sui trasferimenti internazionali, faciliteranno la cooperazione transfrontaliera tra le forze di polizia e le autorità giudiziarie, sia all'interno dell'UE che con i partner internazionali, creando così le condizioni per una lotta più efficace contro la criminalità. Si tratta di un contributo importante all'Agenda europea sulla sicurezza[6].

2.2 Uno strumentario rinnovato e diversificato per i trasferimenti internazionali

Fin dai suoi esordi la normativa dell'UE sulla protezione dei dati ha predisposto una serie di meccanismi che consentono il trasferimento internazionale di dati. L'obiettivo principale di tali norme è garantire che, quando i dati personali dei cittadini europei vengono trasferiti all'estero, la tutela viaggi con loro. Nel corso degli anni queste norme hanno costituito lo standard in materia di flussi internazionali di dati in molte giurisdizioni. Pur mantenendo essenzialmente l'architettura della direttiva del 1995, la riforma delle norme sui trasferimenti internazionali chiarisce e semplifica il loro uso e introduce nuovi strumenti per i trasferimenti.

Ai sensi del diritto dell'UE, uno dei modi per trasferire dati personali all'estero è farlo sulla base di una "decisione di adeguatezza" della Commissione che stabilisce se un paese terzo offre un livello di protezione dei dati che sia "sostanzialmente equivalente"[7] a quello esistente nell'UE. L'effetto di tale decisione è consentire la libera circolazione dei dati personali verso il paese terzo in questione senza che l'esportatore dei dati debba fornire ulteriori garanzie o ottenere alcuna autorizzazione. Per i paesi o le organizzazioni internazionali interessate è disponibile un elenco preciso e dettagliato di elementi di cui la Commissione deve tenere conto nel valutare l'adeguatezza della protezione garantito dall'ordinamento di un paese terzo[8]. La Commissione può ora adottare decisioni di adeguatezza anche per il settore dell'attività di contrasto[9]. Inoltre, basandosi sulla prassi a norma della direttiva del 1995, la

---

6 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Agenda europea sulla sicurezza, COM(2015) 185 final del 28.4.2015.

7 Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, punti 73, 74 e 96. Cfr. anche il considerando 104 del regolamento generale sulla protezione dei dati e il considerando 67 della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia, che si riferiscono alla norma relativa all'equivalenza sostanziale.

8 Cfr. l'articolo 45 del regolamento generale sulla protezione dei dati. Come disposto all'articolo 45, paragrafo 2, nella sua valutazione la Commissione deve tener conto, tra gli altri elementi, dello stato di diritto, del rispetto dei diritti umani e delle libertà fondamentali e della pertinente legislazione, anche in materia di protezione dei dati, sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali. Tali elementi devono essere accompagnati da diritti effettivi e azionabili, in particolare da mezzi di ricorso amministrativo e giudiziario per le persone fisiche, e da un'autorità di vigilanza indipendente pienamente operativa che garantisca e imponga il rispetto delle norme sulla protezione dei dati. Saranno anche prese in considerazione l'adesione a convenzioni giuridicamente vincolanti, in particolare la Convenzione 108 del Consiglio d'Europa, e la partecipazione a sistemi multilaterali o regionali in materia di protezione dei dati.

9 Cfr. l'articolo 36, paragrafo 2, della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia circa gli elementi specifici della valutazione dell'adeguatezza.

riforma prevede esplicitamente la possibilità di una decisione sull'adeguatezza con riferimento a un particolare territorio di un paese terzo o a un settore specifico all'interno di un paese terzo (la cosiddetta adeguatezza "parziale")[10].

In mancanza di una decisione di adeguatezza, i trasferimenti internazionali possono avere luogo sulla base di un certo numero di strumenti alternativi di trasferimento che forniscano adeguate garanzie in materia di protezione dei dati[11]. La riforma formalizza ed amplia le possibilità di ricorso a strumenti esistenti, quali clausole contrattuali tipo[12] e norme vincolanti d'impresa[13]. Ad esempio, è ora possibile includere clausole contrattuali tipo in un contratto tra responsabili del trattamento con sede nell'UE e responsabili del trattamento con sede in un paese non appartenente all'UE (le cosiddette clausole secondo il modello "da responsabile a responsabile")[14]. Le norme vincolanti d'impresa, finora limitate agli accordi tra entità dello stesso gruppo societario, possono ora essere utilizzate da un gruppo di imprese che svolge un'attività economica comune, anche se le imprese non fanno parte dello stesso gruppo societario[15]. La riforma riduce inoltre la burocrazia abolendo i requisiti generali di notifica preventiva alle autorità di protezione dei dati e la loro autorizzazione dei trasferimenti a un paese terzo sulla base di clausole contrattuali tipo o di norme vincolanti d'impresa[16]. Ciò rappresenta un'importante semplificazione del sistema UE di trasferimenti internazionali di dati, poiché l'esistenza di tali requisiti, che attualmente variano da uno Stato membro all'altro, è spesso percepita come un ostacolo significativo per i flussi di dati, in particolare per le imprese più piccole[17].

La riforma introduce inoltre nuovi strumenti per i trasferimenti internazionali[18]. I titolari e i responsabili del trattamento potranno avvalersi, a determinate condizioni[19], di codici di condotta o meccanismi di certificazione approvati (ad esempio marchi di certificazione o

---

10 Cfr. l'articolo 45, paragrafo 1, del regolamento generale sulla protezione dei dati e l'articolo 36, paragrafo 1, della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia.

11 Cfr., per esempio, la comunicazione della Commissione al Parlamento europeo e al Consiglio relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14, (*Schrems*), COM(2015) 566 final del 6.11.2015.

12 Le clausole contrattuali tipo stabiliscono i reciproci obblighi in materia di protezione dei dati in capo, rispettivamente, all'esportatore dell'UE e all'importatore del paese terzo.

13 Le norme vincolanti d'impresa sono norme interne adottate da un gruppo societario multinazionale per effettuare trasferimenti di dati all'interno dello stesso gruppo, verso soggetti situati in paesi che non offrono un livello di protezione adeguato. Mentre le norme vincolanti d'impresa erano già in uso ai sensi della direttiva del 1995, il regolamento generale sulla protezione dei dati codifica e formalizza la loro funzione di strumento per i trasferimenti.

14 Cfr. l'articolo 46, paragrafo 2, lettere c) e d), e il considerando 168 del regolamento generale sulla protezione dei dati.

15 Cfr. l'articolo 46, paragrafo 2, lettera b), l'articolo 47 e il considerando 110 del regolamento generale sulla protezione dei dati.

16 Cfr. l'articolo 46, paragrafo 2, del regolamento generale sulla protezione dei dati.

17 Che i requisiti di registrazione costituiscano un ostacolo al commercio per molte imprese, in particolare per le PMI, è stato messo in evidenza, ad esempio, nella relazione dell'UNCTAD, pag. 34.

18 Cfr. l'articolo 46, paragrafo 2, lettere e) ed f), del regolamento generale sulla protezione dei dati.

19 I titolari del trattamento stabiliti al di fuori dell'UE potranno aderire a un codice di condotta o a un meccanismo di certificazione dell'UE assumendo l'impegno vincolante ed azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le garanzie in materia di protezione dei dati contenute in detti strumenti. Cfr. l'articolo 42, paragrafo 2, del regolamento generale sulla protezione dei dati.

"privacy seal") per predisporre "garanzie adeguate". Ciò dovrebbe consentire lo sviluppo di più soluzioni su misura per i trasferimenti internazionali di dati, che tengano conto, ad esempio, delle caratteristiche ed esigenze specifiche di un dato settore o di particolari flussi di dati. La riforma offre anche la possibilità di prevedere garanzie adeguate per i trasferimenti di dati tra autorità o organismi pubblici sulla base di accordi internazionali o di accordi amministrativi[20]. Il regolamento generale sulla protezione dei dati chiarisce infine l'uso delle cosiddette "deroghe"[21] (ad esempio il consenso, l'esecuzione di un contratto o importanti motivi di interesse pubblico) in virtù delle quali i soggetti possano effettuare, in determinate situazioni, i trasferimenti di dati in mancanza di una decisione di adeguatezza e a prescindere dall'uso di uno degli strumenti sopra citati. In particolare, esso contiene una nuova, seppur circoscritta, deroga relativa ai trasferimenti che sono ammessi se necessari per il perseguimento dei legittimi interessi[22] di un'impresa.

La riforma conferisce infine alla Commissione il potere di elaborare meccanismi di cooperazione internazionale per facilitare l'applicazione delle norme in materia di protezione dei dati, anche attraverso accordi di assistenza reciproca[23]. Viene riconosciuto il contributo che potrebbero garantire forme di collaborazione più stretta tra autorità di vigilanza a livello internazionale per una protezione più efficace dei diritti individuali e una maggiore certezza del diritto per le imprese.

3. TRASFERIMENTI INTERNAZIONALI DI DATI NEL SETTORE COMMERCIALE: FACILITARE IL COMMERCIO TUTELANDO LA VITA PRIVATA

Il rispetto della privacy è una condizione necessaria per flussi commerciali stabili, sicuri e competitivi a livello mondiale. La privacy non è una merce di scambio[24]. Internet e la digitalizzazione dei beni e dei servizi ha trasformato l'economia globale: il trasferimento transfrontaliero di dati, compresi i dati personali, è parte dell'operatività quotidiana delle imprese europee di tutte le dimensioni e in tutti i settori. Poiché gli scambi commerciali utilizzano sempre più i flussi di dati personali, la riservatezza e la sicurezza di tali dati è diventata un fattore essenziale della fiducia dei consumatori. Ad esempio, due terzi degli europei si dichiarano preoccupati del fatto che non hanno alcun controllo sulle informazioni che forniscono online, mentre la metà degli intervistati teme di essere vittima di frode[25]. Al tempo stesso, le imprese europee che operano in alcuni paesi terzi si trovano sempre più spesso a dover far fronte a restrizioni protezionistiche che non possono essere giustificate con argomentazioni legittime di tutela della sfera privata.

Pertanto, nell'era digitale, la promozione di standard elevati di protezione dei dati e la facilitazione del commercio internazionale devono necessariamente andare di pari passo. Dato

---

20 Cfr. l'articolo 46, paragrafo 2, lettera a), e l'articolo 46, paragrafo 3, lettera b), del regolamento generale sulla protezione dei dati.

21 Cfr. l'articolo 49 del regolamento generale sulla protezione dei dati.

22 Cfr. l'articolo 49, paragrafo 1, secondo comma.

23 Cfr. l'articolo 50 del regolamento generale sulla protezione dei dati.

24 Cfr., a titolo di esempio, la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Commercio per tutti – Verso una politica commerciale e di investimento più responsabile", COM(2015) 497 final del 14.10.2015, pag. 8.

25 Special Eurobarometer 431, "Data protection", giugno 2015.

che negli accordi commerciali la protezione dei dati personali non è negoziabile[26], il sistema dell'UE per il trasferimento internazionale dei dati, come evidenziato in precedenza, contempla un ampio e variegato strumentario per consentire i flussi di dati in situazioni diverse, assicurando nel contempo un livello elevato di protezione.

3.1 Decisioni di adeguatezza

L'accertamento di adeguatezza consente il libero flusso di dati personali dall'UE senza che l'esportatore di dati dell'UE debba applicare garanzie supplementari o essere soggetto a ulteriori condizioni. Nell'accertare che l'ordinamento giuridico preveda un livello di protezione adeguato, la decisione riconosce che il sistema del paese si avvicina alle legislazioni degli Stati membri dell'UE. Di conseguenza, i trasferimenti di dati verso il paese in questione saranno equiparati alle trasmissioni di dati all'interno dell'UE, così da fornire un accesso privilegiato al mercato unico dell'UE e, nel contempo, aprire canali commerciali per gli operatori dell'UE. Come spiegato sopra, questo riconoscimento richiede necessariamente un livello di tutela comparabile (o "sostanzialmente equivalente"[27]) a quello garantito all'interno dell'Unione: esso prevede una valutazione globale dei sistemi del paese terzo, compresa la normativa sull'accesso ai dati personali da parte delle pubbliche autorità preposte alle attività di contrasto, alla sicurezza personale o ad altro scopo d'interesse pubblico.

Al tempo stesso, come confermato nel 2015 dalla Corte di giustizia nella sentenza *Schrems*, il livello di adeguatezza non comporta necessariamente una duplicazione pedissequa delle norme dell'UE[28]. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero in questione, nel suo insieme, offre il necessario livello elevato di protezione. Come dimostrano le decisioni di adeguatezza adottate finora, è possibile che la Commissione proceda al riconoscimento dell'adeguatezza di un'ampia gamma di sistemi di tutela della vita privata, che rappresentano diverse tradizioni giuridiche. Tali decisioni riguardano paesi che sono strettamente integrati con l'Unione europea e i suoi Stati membri (Svizzera, Andorra, Isole Fær Øer, Guernsey, Jersey, Isola di Man), importanti partner commerciali (Argentina, Canada, Israele, Stati Uniti) e i paesi che hanno un ruolo di pioniere nell'elaborazione di leggi sulla protezione dei dati nella loro regione (Nuova Zelanda, Uruguay).

Le decisioni sul Canada e sugli Stati Uniti sono accertamenti di adeguatezza "parziale". La decisione relativa al Canada si applica solo ai soggetti privati che rientrano nel campo di applicazione della legge canadese sulla tutela delle informazioni personali e sui documenti elettronici. La decisione di recente adozione sullo scudo UE-USA per la privacy[29] è un caso specifico nel senso che, in assenza di una legislazione generale sulla protezione dei dati negli Stati Uniti[30], essa si basa sull'assunzione di impegni da parte delle imprese partecipanti ad

---

[26] Orientamenti politici del presidente Juncker *"Un nuovo inizio per l'Europa: il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico"*.

[27] Cfr. la nota a piè di pagina 7.

[28] Cfr. il punto 74 della sentenza *Schrems*.

[29] Decisione di esecuzione UE 2016/1250 del 12 luglio 2016.

[30] La Commissione esorta gli Stati Uniti a proseguire gli sforzi verso un sistema globale di protezione dei dati e della vita privata che consenta, a più lungo termine, una convergenza tra i due sistemi. Cfr. la

applicare gli elevati standard di protezione dei dati stabiliti dal presente accordo che sono, a loro volta, azionabili in forza del diritto statunitense. Inoltre, lo scudo per la privacy si fonda sulle specifiche osservazioni e garanzie espresse dal governo degli Stati Uniti per quanto riguarda l'accesso a fini di sicurezza nazionale[31], che sono alla base dell'accertamento di adeguatezza. Il rispetto degli impegni sarà oggetto di attento monitoraggio da parte della Commissione e parte integrante del riesame annuale sul funzionamento del quadro.

Negli ultimi anni un numero sempre maggiore di paesi nel mondo ha adottato o sta adottando nuove normative in materia di protezione dei dati e della vita privata. Nel 2015 il numero di paesi dotati di leggi sui dati e la privacy era pari a 109, un aumento significativo rispetto ai 76 contati a metà del 2011[32]. Inoltre, circa 35 paesi stanno attualmente elaborando leggi sulla protezione dei dati[33]. Queste normative, nuove o modernizzate, tendono a basarsi su un nucleo di principi comuni che comprende, tra l'altro, il riconoscimento della protezione dei dati quale diritto fondamentale, l'adozione di una normativa generale in questo campo, l'esistenza di diritti alla tutela della vita privata individuali e azionabili e l'istituzione di un'autorità di vigilanza indipendente. Ciò offre nuove opportunità, in particolare mediante l'accertamento di adeguatezza, per facilitare ulteriormente i flussi di dati, garantendo nel contempo il mantenimento di un livello elevato di protezione dei dati personali.

A norma del diritto dell'UE, un accertamento di adeguatezza presuppone l'esistenza di norme in materia di protezione dei dati comparabili a quelle dell'UE[34]. Ciò riguarda sia le tutele sostanziali applicabili ai dati personali che la relativa vigilanza e i meccanismi di ricorso disponibili nel paese terzo.

Nell'ambito del quadro sull'accertamento di adeguatezza, la Commissione ritiene che debbano essere presi in considerazione i seguenti criteri al momento di valutare con quali paesi terzi è opportuno instaurare un dialogo in materia di adeguatezza[35]:

i) la portata delle relazioni commerciali (esistenti o potenziali) dell'UE con un determinato paese terzo, in particolare l'esistenza di un accordo di libero scambio o di negoziati in corso;

---

comunicazione della Commissione al Parlamento europeo e al Consiglio "Trasferimenti transatlantici di dati – Ripristinare la fiducia attraverso solide garanzie", COM(2016) 117 final del 29.2.2016.

31 Ciò comprende, in particolare, l'applicazione della direttiva presidenziale 28 (PPD-28), che impone una serie di limitazioni e garanzie per le operazioni di spionaggio elettronico e la nomina di un mediatore ad hoc per i reclami da parte di cittadini dell'UE a tale riguardo.

32 G. Greenleaf, "Global data privacy laws 2015: 109 countries, with European laws now in a minority", (2015) *133 Privacy Laws & Business International Report*, pagg. 14-17.

33 Studio UNCTAD, pagg. 8 e 42 (nota 4 di cui sopra).

34 A tale riguardo, la Commissione tiene anche conto degli obblighi del paese terzo derivanti da convenzioni giuridicamente vincolanti, in particolare la sua adesione alla convenzione n. 108 e al protocollo aggiuntivo, nell'effettuare una valutazione di adeguatezza. Cfr. l'articolo 45, paragrafo 2, lettera c), e il considerando 105 del regolamento generale sulla protezione dei dati.

35 Per i paesi nei confronti dei quali vi sono pertinenti interessi per la cooperazione in materia di sicurezza interna e di applicazione della legge, la Commissione esaminerà la possibilità di specifici accertamenti di adeguatezza ai sensi della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia; cfr. la sezione 4.

ii) la portata dei flussi di dati personali provenienti dall'UE, indice di legami culturali e/o geografici;

iii) il ruolo di pioniere nel settore della protezione della vita privata e dei dati del paese terzo, che potrebbe fungere da modello per gli altri paesi della regione[36];

iv) le relazioni politiche generali con il paese terzo in questione, in particolare per quanto riguarda la promozione di valori comuni e obiettivi condivisi a livello internazionale.

Sulla base di queste considerazioni, la Commissione intende impegnarsi attivamente con i principali partner commerciali in Asia orientale e sudorientale, a partire dal Giappone e dalla Corea nel 2017[37] e, in funzione dei progressi compiuti verso la modernizzazione della normativa in materia di protezione dei dati, con l'India, ma anche con i paesi dell'America latina, in particolare con i paesi del Mercosur, e con il vicinato europeo, che hanno manifestato l'interesse a sottoporsi ad un "accertamento di adeguatezza". Inoltre, la Commissione accoglie con favore le manifestazioni di interesse da parte di altri paesi terzi disposti a impegnarsi su queste tematiche. Le discussioni su un eventuale accertamento di adeguatezza sono un dialogo interattivo durante il quale fornire tutti i necessari chiarimenti in merito alle norme UE sulla protezione dei dati ed esplorare le modalità per accrescere la convergenza della legislazione e della prassi dei paesi terzi.

In determinate situazioni, invece di adottare un approccio su scala nazionale, può essere più opportuno ricorrere ad altre opzioni, come l'adeguatezza parziale o settoriale (ad esempio per i servizi finanziari o l'informatica), che possono interessare aree geografiche o settori che costituiscono una parte importante della particolare economia di un paese terzo. Questo aspetto va considerato alla luce di elementi quali, ad esempio, la natura e lo stato di sviluppo del diritto alla tutela della vita privata (normativa autonoma o diverse leggi settoriali, ecc.), la struttura costituzionale del paese terzo o se taluni settori dell'economia sono particolarmente esposti ai flussi di dati provenienti dall'UE.

L'adozione di una decisione di adeguatezza implica l'instaurazione di un dialogo specifico e di strette forme di cooperazione con il paese terzo in questione. Le decisioni di adeguatezza sono documenti "vivi", che devono essere attentamente monitorati dalla Commissione e adattati se intervengono sviluppi che incidono sul livello di protezione garantito dal paese terzo in questione[38]. A tal fine, sarà organizzata una revisione periodica, almeno ogni quattro anni, per affrontare le questioni emergenti e scambiare le migliori pratiche tra partner che hanno stabilito una stretta cooperazione[39]. Questo approccio dinamico si applica anche alle decisioni di adeguatezza già esistenti, adottate a norma della direttiva del 1995, che dovranno essere

[36] Ciò può essere particolarmente importante per i paesi in via di sviluppo e i paesi in transizione, poiché la protezione dei dati personali è sia un elemento essenziale dello stato di diritto che un fattore determinante per la competitività economica.

[37] Recentemente il Giappone e la Corea hanno adottato nuove leggi o modernizzato la loro normativa al fine di porre in essere un regime generale di protezione dei dati.

[38] L'articolo 45, paragrafi 4 e 5, del regolamento generale sulla protezione dei dati conferisce alla Commissione il compito di controllare su base continuativa gli sviluppi nei paesi terzi e le conferisce il potere di revocare, modificare o sospendere una decisione di adeguatezza, qualora constati che il paese in questione non garantisca più un livello di protezione adeguato.

[39] Articolo 45, paragrafo 3, del regolamento generale sulla protezione dei dati.

sottoposte a riesame nel caso in cui non soddisfino più le norme in vigore[40]. I paesi terzi interessati sono pertanto invitati a informare la Commissione di qualsiasi modifica pertinente della legislazione e della prassi introdotte dopo l'adozione della decisione di adeguatezza che li riguarda. Ciò è essenziale per assicurare la continuità di tali decisioni in conformità delle nuove norme della riforma[41].

Le norme dell'UE sulla protezione dei dati non possono essere oggetto di negoziati in un accordo di libero scambio[42]. Se il dialogo con i paesi terzi in materia di protezione dei dati e i negoziati commerciali devono seguire percorsi separati, una decisione di adeguatezza, anche una parziale o settoriale, costituisce lo strumento migliore per costruire la fiducia reciproca, garantire un flusso di dati personali senza ostacoli e agevolare in tal modo gli scambi commerciali che implicano il trasferimento di dati personali verso il paese terzo in questione. Le decisioni di adeguatezza possono quindi agevolare i negoziati commerciali o integrare gli accordi commerciali esistenti, amplificandone i vantaggi. Al tempo stesso, promuovendo la convergenza del livello di protezione nell'UE e nel paese terzo, un accertamento di adeguatezza riduce il rischio che detto paese, invocando la protezione dei dati personali, imponga obblighi ingiustificati in materia di localizzazione o di stoccaggio. Oltre a ciò, come indicato nella comunicazione "Commercio per tutti", la Commissione intende utilizzare gli accordi commerciali dell'UE per stabilire una disciplina del commercio elettronico e dei flussi transfrontalieri di dati e per affrontare nuove forme di protezionismo digitale, fatta salva la normativa dell'UE sulla protezione dei dati e nel pieno rispetto della medesima[43].

---

40 L'articolo 97, paragrafo 2, lettera a), del regolamento generale sulla protezione dei dati impone alla Commissione di trasmettere una relazione di valutazione al Parlamento europeo e al Consiglio entro il 2020.

41 A seguito della sentenza *Schrems*, secondo la quale nella decisione "Approdo sicuro" la Commissione aveva oltrepassato le sue competenze limitando i poteri delle autorità di protezione dei dati di sospendere o vietare i flussi di dati, il 16 dicembre 2016 la Commissione ha adottato una decisione di modifica "*omnibus*" che sopprime le disposizioni analoghe contenute nelle decisioni di adeguatezza esistenti e le sostituisce con disposizioni che si limitano a introdurre obblighi di informazione tra gli Stati membri e la Commissione nel caso in cui un'autorità di protezione dei dati sospenda o vieti i trasferimenti di dati verso un paese terzo. La decisione "*omnibus*" introduce altresì l'obbligo per la Commissione di seguire gli sviluppi pertinenti nel paese terzo. Cfr. GU L 344 del 17.12.2016, pag. 83.

42 In particolare, un accertamento di adeguatezza è una decisione di esecuzione della Commissione a carattere unilaterale in conformità con la normativa UE sulla protezione dei dati, basata sui criteri ivi contenuti.

43 Cfr. la comunicazione "Commercio per tutti", pag. 15 (nota 24 di cui sopra).

La Commissione:

- privilegerà le discussioni sulle possibili decisioni di adeguatezza con partner commerciali chiave nell'Asia orientale e sudorientale, a partire da Giappone e Corea nel 2017, ma tenendo conto anche di altri partner strategici come l'India, nonché con i paesi dell'America latina, in particolare del Mercosur e del vicinato europeo;

- controllerà attentamente il funzionamento delle decisioni di adeguatezza esistenti, in particolare, l'attuazione del quadro dello scudo UE-USA per la privacy, segnatamente mediante il meccanismo annuale di riesame congiunto;

- collaborerà con i paesi interessati, assistendoli nell'adozione di norme rigorose in materia di protezione dei dati e sostenendone la convergenza verso i principi dell'UE in materia di protezione dei dati.

3.2 Meccanismi alternativi di trasferimento dei dati

Le norme dell'UE in materia di protezione dei dati hanno sempre riconosciuto che non esiste un approccio unico per i trasferimenti internazionali di dati. Ciò è ancora più vero per le norme introdotte dalla riforma. Mentre gli accertamenti di adeguatezza saranno disponibili solo per quei paesi terzi che soddisfano i criteri previsti, il regolamento generale sulla protezione dei dati prevede tutta una serie di meccanismi che sono sufficientemente flessibili da adattarsi a diverse situazioni di trasferimento. È possibile sviluppare strumenti che tengano conto delle peculiari esigenze o condizioni di specifici settori, modelli commerciali e/o operatori, per esempio sotto forma di clausole contrattuali tipo calibrate sui requisiti di un particolare settore (come le garanzie specifiche per il trattamento di dati sensibili in ambito sanitario) oppure di un determinato tipo di attività di trattamento diffuso in alcuni paesi terzi (come i servizi di esternalizzazione svolti per le imprese europee). Si potrebbe raggiungere questo obiettivo adottando nuovi insiemi di clausole tipo oppure integrando quelle esistenti con garanzie supplementari che possono variare dalle soluzioni tecniche a quelle organizzative, a quelle relative ai modelli commerciali[44]. Alcune specifiche esigenze settoriali possono essere soddisfatte mediante le norme vincolanti d'impresa per i gruppi di imprese coinvolti in un'attività economica comune, ad esempio nel settore dei viaggi. I trasferimenti internazionali tra responsabili del trattamento potrebbero trarre vantaggio dall'introduzione di clausole contrattuali tipo e/o norme vincolanti d'impresa secondo il modello "da responsabile a responsabile" per i responsabili del trattamento. Infine, i nuovi meccanismi di trasferimento, quali i codici di condotta approvati e le certificazioni di terzi accreditati, offrono all'industria la possibilità di introdurre soluzioni su misura per i trasferimenti internazionali pur beneficiando dei vantaggi competitivi associati, ad esempio marchi di certificazione o

[44] Cfr. l'articolo 46, paragrafo 2, lettere c) e d), e il considerando 109 del regolamento generale sulla protezione dei dati, che chiariscono la possibilità di adattare le clausole modello approvate purché non contraddicano, direttamente o indirettamente, le clausole modello o ledano i diritti o le libertà fondamentali degli individui.

"privacy seal". Alcuni di questi strumenti possono essere sviluppati come meccanismi specifici per il trasferimento o nel quadro di strumenti più generici per dimostrare la conformità a tutte le disposizioni del regolamento generale sulla protezione dei dati, come nel caso di un codice di condotta approvato.

La Commissione collaborerà con l'industria, la società civile e le autorità di protezione dei dati al fine di sfruttare appieno il potenziale dell'insieme di strumenti per i trasferimenti internazionali contenuto nel regolamento generale sulla protezione dei dati. Il dialogo in corso con le parti interessate nel quadro dell'attuazione della riforma contribuirà ad individuare gli ambiti di intervento prioritari a tale riguardo, tra cui potrebbe figurare il completamento dei lavori già avviati, tra cui l'elaborazione, in collaborazione con il gruppo di lavoro "articolo 29" (che sarà sostituito nel 2018 dal comitato europeo per la protezione dei dati), di clausole contrattuali tipo secondo il modello "da responsabile a responsabile"[45]. In questo filone si colloca lo sviluppo di nuovi elementi dell'infrastruttura dell'UE per la conformità, ad esempio con l'attribuzione alla Commissione del compito di definire i requisiti e le norme tecniche per l'istituzione e il funzionamento di meccanismi di certificazione, anche per gli aspetti relativi ai trasferimenti internazionali[46]. Alcuni di questi interventi possono essere integrati da lavori a livello internazionale, in particolare con le organizzazioni che hanno elaborato meccanismi di trasferimento simili. Ad esempio, potrebbero essere esplorate modalità per promuovere la convergenza tra le norme vincolanti d'impresa ai sensi del diritto dell'UE e le norme transfrontaliere in materia di privacy elaborate dalla cooperazione economica Asia-Pacifico (APEC)[47] per quanto riguarda sia le norme applicabili sia il processo di applicazione nell'ambito di ciascun sistema. Ciò dovrebbe contribuire a promuovere standard elevati in materia di protezione dei dati a livello mondiale e, parallelamente, a superare le differenze di approccio alla tutela della vita privata e alla protezione dei dati, ad aiutare gli operatori commerciali ad orientarsi tra i diversi sistemi e a definire politiche conformi.

La Commissione:

- collaborerà con le parti interessate per sviluppare meccanismi alternativi di trasferimento dei dati personali adeguati alle peculiari esigenze o condizioni di specifici settori, modelli e/o operatori commerciali.

[45] Attualmente non sono in vigore clausole contrattuali tipo tra responsabile del trattamento UE e responsabile del trattamento non UE.

[46] Articolo 43, paragrafi 8 e 9, del regolamento generale sulla protezione dei dati.

[47] Cfr. riferimento comune UE/APEC del 2014 relativo alla struttura delle norme vincolanti d'impresa dell'UE e al sistema delle norme transfrontaliere in materia di privacy (CBPR) della Cooperazione economica Asia-Pacifico (APEC), che raffronta i requisiti di conformità e certificazione di entrambi i sistemi: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

3.3 Cooperazione internazionale per la protezione dei dati personali

3.3.1. Promozione di norme in materia di protezione dei dati mediante strumenti e consessi multilaterali

Il quadro giuridico dell'UE in materia di protezione dei dati ha spesso costituito un punto di riferimento per i paesi terzi nell'elaborazione della normativa in questo campo. L'UE continuerà a impegnarsi attivamente nel dialogo con i partner internazionali, a livello sia bilaterale che multilaterale, al fine di promuovere la convergenza sviluppando a livello mondiale standard elevati e interoperabili in materia di protezione dei dati personali. Ciò contribuisce a una più efficace tutela dei diritti, riducendo al tempo stesso gli ostacoli alla circolazione transfrontaliera dei dati come elemento fondamentale del libero scambio.

In particolare, la Commissione incoraggia l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa n. 108 e al relativo protocollo addizionale[48]. La convenzione, che è aperta ai non membri del Consiglio d'Europa ed è già stata ratificata da 50 paesi, compresi alcuni paesi dell'Africa e dell'America del Sud[49], è l'unico strumento multilaterale vincolante in materia di protezione dei dati. Esso è attualmente in corso di revisione e la Commissione intende promuovere attivamente la rapida adozione del testo aggiornato ai fini dell'adesione dell'UE. Il testo rispecchierà gli stessi principi sanciti nelle nuove norme dell'UE sulla protezione dei dati e, di conseguenza, contribuirà alla convergenza verso un insieme di standard elevati di protezione dei dati.

La riunione del G20 nel 2017 offrirà un'ulteriore opportunità per l'UE di adoperarsi per la convergenza basata sul principio secondo cui standard elevati di protezione dei dati costituiscono una componente essenziale dell'ulteriore sviluppo di una società dell'informazione globale in grado di promuovere l'innovazione, la crescita e la prosperità sociale[50].

Inoltre, la Commissione attende con interesse di avviare un dialogo con nuovi importanti attori, come il relatore speciale delle Nazioni Unite sul diritto alla riservatezza[51], nominato di recente, e di sviluppare ulteriormente le sue relazioni di lavoro con organizzazioni regionali quali l'APEC al fine di promuovere in tutto il mondo una cultura di rispetto del diritto alla protezione della vita privata e dei dati personali.

Nel quadro più ampio degli sforzi volti a migliorare la sensibilizzazione in materia di privacy e ad aumentare le garanzie per la protezione dei dati a livello internazionale, il 15 novembre 2016 la Commissione europea ha approvato un progetto nell'ambito dello

---

48 Convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE n. 108) e protocollo addizionale del 2001 alla convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STE n. 181).

49 Maurizio, Senegal e Uruguay hanno ratificato la convenzione, mentre Capo Verde, Marocco e Tunisia sono stati invitati ad aderire.

50 Cfr. anche la dichiarazione ministeriale dell'OCSE "L'economia digitale: innovazione, crescita e prosperità sociale" (dichiarazione di Cancún) del 23 giugno 2016.

51 Cfr. http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

strumento di partenariato per rafforzare la cooperazione con i paesi partner in questo settore[52]. Lo strumento comprende il finanziamento di attività quali la formazione e la sensibilizzazione. A sua volta, nel contesto dell'applicazione della riforma, l'UE può trarre beneficio dallo scambio delle migliori pratiche e dall'esperienza di altri sistemi con nuove sfide per la tutela della vita privata e soluzioni giuridiche o tecniche emergenti, anche per quanto riguarda il controllo dell'applicazione, gli strumenti preposti alla conformità (ad esempio, i meccanismi di certificazione, le valutazioni dell'impatto sulla vita privata) o le tutele per talune specifiche serie di dati (per esempio, i dati dei minori).

3.3.2. Cooperazione nell'attività di contrasto

Rafforzare la cooperazione con le autorità dei paesi terzi preposte al controllo e all'applicazione della legge in materia di tutela della vita privata è sempre più necessario, date le dimensioni globali delle imprese multinazionali che trattano enormi quantità di dati personali in un gran numero di paesi. Spesso i problemi di non conformità con le norme sulla protezione dei dati o di violazione dei dati interessano contemporaneamente più di una giurisdizione. In questi casi la tutela delle persone fisiche può essere resa più efficace attraverso un'azione comune. Al tempo stesso, gli operatori economici trarrebbero beneficio da un contesto giuridico più chiaro se si mettessero a punto a livello mondiale strumenti di interpretazione e pratiche di applicazione della legge comuni.

Nel mondo connesso e senza frontiere dei flussi di dati, è quindi il momento di rafforzare la cooperazione tra le autorità preposte all'applicazione delle norme[53]. L'UE è pronta a fare la sua parte. Come ricordato in precedenza, il regolamento generale sulla protezione dei dati conferisce alla Commissione il potere di sviluppare meccanismi di cooperazione internazionale per facilitare l'effettiva applicazione della normativa in materia di protezione dei dati, anche attraverso accordi di assistenza reciproca. In questo contesto, si dovrebbe vagliare la possibilità di mettere a punto un accordo quadro per la cooperazione tra le autorità di protezione dei dati dell'UE e le autorità preposte all'applicazione della legge in taluni paesi terzi, basandosi anche sull'esperienza acquisita dalla Commissione in altri settori, come la concorrenza e la tutela dei consumatori.

---

[52] Decisione di esecuzione della Commissione C(2016) 7198 che approva la seconda fase del programma d'azione annuale 2016 (PAA 2016) dello strumento di partenariato.

[53] Le reti esistenti comprendono la rete globale di applicazione della legge in materia di privacy (Global Privacy Enforcement Network - GPEN), nata nel 2010 sotto l'egida dell'OCSE. Si tratta di una rete informale di autorità incaricate dell'applicazione della legge in materia di privacy, cui partecipano le autorità UE di protezione dei dati, che ha il compito, tra gli altri, di attuare una cooperazione nell'attività di contrasto, di condividere le migliori pratiche nell'affrontare le sfide transfrontaliere e di sostenere le iniziative congiunte per far applicare la legge e le campagne di sensibilizzazione. Non crea nuovi obblighi giuridicamente vincolanti per i partecipanti ed è incentrata principalmente sulla promozione della cooperazione in materia di applicazione della normativa sulla privacy che disciplina il settore privato. Cfr. https://privacyenforcement.net/.

La Commissione:

- promuoverà la rapida adozione del testo aggiornato della convenzione del Consiglio d'Europa n. 108 ai fini dell'adesione dell'UE e incoraggiare l'adesione da parte dei paesi terzi;

- si avvarrà dei consessi multilaterali quali le Nazioni Unite, il G20 e l'APEC per promuovere una cultura globale di rispetto dei diritti in materia di protezione dei dati;

- svilupperà meccanismi di cooperazione internazionale con i principali partner internazionali al fine di facilitare un'applicazione efficace delle norme.

4. UNA COOPERAZIONE PIÙ EFFICACE NELL'APPLICAZIONE DELLA LEGGE CON SOLIDE GARANZIE DI PROTEZIONE DEI DATI

Gli scambi di dati personali sono parte integrante della prevenzione, dell'indagine e del perseguimento dei reati penali. In un mondo interconnesso in cui la criminalità raramente si ferma alle frontiere nazionali, il rapido scambio di dati personali è essenziale ai fini di un'efficace cooperazione nell'attività di contrasto e di una risposta efficace alla criminalità. Gli scambi di dati devono essere associati a solide garanzie in materia di protezione dei dati, contribuendo così anche a costruire la fiducia tra le autorità incaricate dell'applicazione della legge e a rafforzare la certezza del diritto nella raccolta e/o nello scambio di informazioni.

Le norme sui trasferimenti internazionali nella direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia disciplinano lo scambio di dati tra le autorità incaricate dell'applicazione della legge di paesi UE e di paesi terzi nonché, in determinate situazioni, i trasferimenti dalle autorità di contrasto ad altri soggetti. La direttiva introduce la possibilità di accertamenti di adeguatezza nel settore dell'attività di contrasto a carattere penale. La Commissione promuoverà la possibilità di svolgere accertamenti di adeguatezza con paesi terzi idonei, in particolare con i paesi con i quali è necessaria una stretta e tempestiva cooperazione nella lotta contro la criminalità e il terrorismo e in cui sono già in atto scambi di dati personali. Su questa base, la Commissione darà la priorità al dibattito sulle decisioni di adeguatezza con i paesi terzi che sono partner fondamentali in questa impresa.

In alternativa, l'accordo quadro UE-USA sulla protezione dei dati[54] concluso nel dicembre 2016 è un buon esempio di come la cooperazione nell'attività di contrasto con un

[54] Accordo fra l'UE e gli USA sulla protezione dei dati personali trasferiti e trattati ai fini di prevenzione, indagine, accertamento o perseguimento di reati, anche di terrorismo, nel quadro della cooperazione di polizia e della cooperazione giudiziaria in materia penale. http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf ("l'accordo quadro")

importante partner internazionale possa essere migliorata tramite la negoziazione di un solido insieme di garanzie in materia di protezione dei dati. Integrando automaticamente gli strumenti giuridici esistenti sui quali si basano gli scambi di dati (in particolare gli accordi bilaterali, sia a livello dell'UE che degli Stati membri), l'accordo quadro apporta benefici immediati e diretti alle persone e rafforza la cooperazione nell'attività di contrasto agevolando lo scambio di informazioni. Inoltre, istituendo una base di riferimento per i futuri accordi di trasferimento di dati con gli Stati Uniti, l'accordo quadro elimina la necessità di rinegoziare a più riprese garanzie identiche. Prima convenzione internazionale bilaterale dotata di un catalogo completo dei diritti e dei doveri in materia di protezione dei dati in linea con l'*acquis* dell'UE, l'accordo quadro può pertanto fungere da base per negoziare accordi analoghi con i paesi terzi, non solo nel settore della cooperazione giudiziaria e di polizia, ma anche in altri settori, ad esempio la politica della concorrenza e la tutela dei consumatori. Esso riguarda sia gli scambi tra governi che i trasferimenti di dati tra imprese private e autorità incaricate dell'applicazione della legge. Potrebbe inoltre agevolare la conclusione da parte dell'Unione di accordi in materia di scambio di dati tra le pertinenti agenzie dell'UE (in particolare Europol ed Eurojust) e i paesi terzi[55]. La Commissione valuterà pertanto la possibilità di concludere analoghi accordi quadro con i principali partner incaricati dell'applicazione della legge.

La direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia prevede inoltre che le autorità incaricate dell'applicazione della legge nell'UE abbiano la possibilità, associata a rigorose garanzie e a circostanze specifiche, di richiedere informazioni direttamente a una società privata in un paese terzo e di trasmettere informazioni personali (di solito un nome o un indirizzo IP) nella richiesta[56]. Per contro, il regolamento generale sulla protezione dei dati affronta specificamente i casi in cui soggetti privati nell'UE trasmettono dati personali alle autorità incaricate dell'applicazione della legge di un paese terzo in seguito ad una richiesta: tali trasferimenti al di fuori dell'UE sono consentiti solo a determinate condizioni, ad esempio sulla base di un accordo internazionale o quando la divulgazione è necessaria per un motivo di interesse pubblico rilevante riconosciuto dal diritto dell'Unione o dello Stato membro[57].

Tale cooperazione, diventata fondamentale per la riuscita delle indagini e il perseguimento della criminalità e del terrorismo, è messa in evidenza nelle conclusioni del Consiglio sul miglioramento della giustizia penale nel ciberspazio. Il Consiglio ha invitato la Commissione ad adottare misure concrete, sulla base di un approccio comune dell'UE, per migliorare la cooperazione con i fornitori di servizi, rendere più efficiente l'assistenza giudiziaria reciproca e proporre soluzioni ai problemi relativi alla determinazione e alla competenza esecutiva nel ciberspazio[58]. Tali azioni riguardano sia gli scambi tra le autorità incaricate dell'applicazione

---

[55] La conclusione di accordi operativi con Europol ed Eurojust è stata anche un punto di riferimento nei dialoghi sulla liberalizzazione dei visti con alcuni paesi terzi, in particolare, ad esempio, nel contesto del dialogo in corso con la Turchia.

[56] Cfr. articolo 39 e considerando 73 della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia.

[57] Cfr. articolo 48 e considerando 115 del regolamento generale sulla protezione dei dati.

[58] Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciberspazio, 9 giugno 2016: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. La Commissione è

della legge e i prestatori di servizi aventi sede nell'UE, che gli scambi con le autorità di paesi terzi e le imprese. La Commissione illustrerà le opzioni per l'accesso al materiale probatorio elettronico nel giugno 2017, tenendo conto della necessità di garantire una cooperazione rapida e affidabile fondata sulle norme rigorose stabilite dalla direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia e dal regolamento generale sulla protezione dei dati, sia per le situazioni interne all'UE che per i trasferimenti internazionali.

Infine, in linea con la nuova base giuridica per Europol, la Commissione valuterà le disposizioni contenute negli accordi di cooperazione operativa tra Europol e i terzi, conclusi ai sensi della decisione 2009/371/GAI del Consiglio, incluse le disposizioni in materia di protezione dei dati[59]. Inoltre, come indicato nell'agenda europea sulla sicurezza del 2015, l'approccio futuro dell'Unione allo scambio dei dati PNR con i paesi terzi terrà conto della necessità di applicare norme coerenti e specifiche tutele dei diritti fondamentali. La Commissione lavorerà su soluzioni giuridicamente valide e sostenibili per lo scambio delle registrazioni dei nominativi dei passeggeri (PNR) con i paesi terzi, anche prendendo in considerazione un accordo modello sui dati PNR che stabilisca i requisiti che i paesi terzi devono soddisfare per poter ricevere dati PNR dall'UE. Qualsiasi politica futura in questo campo dipende tuttavia soprattutto dal prossimo parere della Corte di giustizia dell'Unione europea in merito al previsto accordo in materia di PNR tra l'UE e il Canada[60].

---

stata incaricata di presentare risultati su tali questioni al Consiglio entro giugno 2017, a seguito della sua relazione al Consiglio sullo stato di avanzamento dei lavori del dicembre 2016.

[59] Cfr. l'articolo 25, paragrafo 4, del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 25.5.2016, pag. 53). La Commissione è tenuta a presentare una relazione di valutazione entro il 14 giugno 2021 sugli accordi di cooperazione di Europol conclusi prima del 1º maggio 2017.

[60] Parere della Corte di giustizia sul progetto di accordo sui dati PNR tra l'UE e il Canada del 2014, sottoposto alla Corte di giustizia dal Parlamento europeo (parere 1/15). La Corte è stata chiamata a valutare la compatibilità del progetto di accordo con la Carta dei diritti fondamentali dell'UE.

UNA COOPERAZIONE PIÙ EFFICACE NELL'APPLICAZIONE DELLA LEGGE CON SOLIDE GARANZIE DI PROTEZIONE DEI DATI

La Commissione:

- promuoverà la possibilità di formulare decisioni di adeguatezza ai sensi della direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia con i paesi terzi idonei;

- promuoverà la negoziazione di accordi nel settore dell'applicazione della legge con importanti partner internazionali secondo il modello stabilito dall'accordo quadro con gli Stati Uniti;

- darà seguito alle conclusioni del Consiglio sul miglioramento della giustizia penale nel ciberspazio per facilitare lo scambio transfrontaliero di prove elettroniche in conformità con le norme sulla protezione dei dati.

5. CONCLUSIONE

La protezione e lo scambio dei dati personali non si escludono a vicenda. Un solido sistema di protezione dei dati agevola i flussi di dati accrescendo la fiducia dei consumatori nelle imprese che hanno a cuore le modalità di trattamento dei dati personali dei loro clienti. Standard elevati di protezione dei dati diventano così vantaggiosi per l'economia digitale globale. Lo stesso vale per la cooperazione nell'attività di contrasto: garanzie in materia di privacy sono parte integrante di un efficace e rapido scambio di informazioni nella lotta contro la criminalità, basato sulla fiducia reciproca e la certezza del diritto.

Una volta completata la riforma delle norme sulla protezione dei dati, l'Unione europea dovrebbe impegnarsi in modo proattivo con i paesi terzi in merito a tale questione, cercando di ottenere una maggiore convergenza verso l'alto dei principi in materia di protezione dei dati a livello internazionale, sia a livello bilaterale che multilaterale, nell'interesse e a vantaggio dei cittadini e delle imprese. Il nuovo quadro normativo sulla protezione dei dati fornisce all'UE gli strumenti necessari e adeguati per raggiungere tali obiettivi. Sulla base dell'approccio strategico illustrato nella presente comunicazione, la Commissione intende impegnarsi attivamente con i principali paesi terzi per valutare la possibilità di adottare accertamenti di adeguatezza, iniziando con il Giappone e la Corea nel 2017, nell'intento di promuovere la convergenza normativa verso gli standard dell'UE e di facilitare le relazioni

commerciali. Nel contempo, l'UE potrà sfruttare appieno la gamma di strumenti alternativi di trasferimento dei dati per tutelare i diritti in materia di protezione dei dati e sostenere gli operatori economici al momento del trasferimento dei dati verso paesi il cui diritto nazionale non garantisce un adeguato livello di protezione. Tali strumenti dovrebbero essere utilizzati anche per facilitare ulteriormente la cooperazione tra le autorità di contrasto e di controllo dell'UE e i loro partner internazionali. La Commissione garantirà la coerenza della dimensione interna ed esterna della politica dell'UE in materia di protezione dei dati e promuoverà una robusta protezione dei dati a livello internazionale per migliorare la cooperazione nell'attività di contrasto, contribuire al commercio libero e sviluppare elevati standard in materia di protezione dei dati personali a livello mondiale.