



Bruxelles, 27.11.2013
COM(2013) 846 final

**COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL
CONSIGLIO**

Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA

1. INTRODUZIONE — IL TRATTAMENTO DEI DATI FRA L'UE E GLI USA IN UN CONTESTO IN EVOLUZIONE

L'Unione europea e gli Stati Uniti sono partner strategici e tale partenariato è fondamentale per promuovere i valori che condividiamo, la nostra sicurezza e la nostra leadership comune sulla scena internazionale.

La fiducia in questo partenariato è stata tuttavia scossa, e deve essere ripristinata. L'UE, i suoi Stati membri e i cittadini europei hanno espresso profonde preoccupazioni in merito alle rivelazioni di programmi di raccolta di intelligence su larga scala degli Stati Uniti, in particolare per quanto riguarda la protezione dei dati personali¹. Un controllo di massa delle comunicazioni private, siano esse di cittadini, di imprese o di dirigenti politici, è inaccettabile.

I trasferimenti di dati personali sono un importante e necessario elemento delle relazioni transatlantiche. Fanno parte integrante degli scambi commerciali fra le due sponde dell'Oceano, anche per i nuovi settori emergenti del digitale come i media sociali o il cloud computing, che vedono grosse quantità di dati viaggiare dall'Unione europea agli Stati Uniti, e costituiscono anche una componente essenziale della cooperazione fra l'UE e gli USA nel campo delle attività di contrasto della criminalità, e della cooperazione fra gli Stati membri e gli USA nel settore della sicurezza nazionale. Per facilitare i flussi di dati, garantendo al tempo stesso un elevato livello di protezione come richiesto dalla normativa europea, gli USA e l'UE hanno predisposto una serie di accordi e di intese.

Gli scambi commerciali sono oggetto della decisione 2000/520/CE² (in appresso la "decisione Approdo sicuro"), che fornisce una base giuridica per il trasferimento dei dati personali dall'UE a società stabilite negli Stati Uniti che hanno aderito ai principi d'Approdo sicuro.

Lo scambio di dati personali fra l'UE e gli USA ai fini di attività di contrasto, fra cui la prevenzione e la lotta contro il terrorismo e altre forme gravi di criminalità, è disciplinato da una serie di accordi a livello UE: l'accordo sulla mutua assistenza giudiziaria³, l'accordo sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri (PNR)⁴, l'accordo sul trattamento e il trasferimento di dati di messaggistica finanziaria ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP)⁵, e l'accordo fra Europol e gli USA. Questi accordi rispondono a importanti sfide in materia di sicurezza e agli interessi comuni in tale ambito dell'UE e degli USA, garantendo al tempo stesso un livello elevato di

¹ Ai fini della presente comunicazione, l'espressione "cittadini dell'UE" si riferisce anche agli interessati, non cittadini dell'UE, che rientrano però nel campo d'applicazione della normativa dell'Unione in materia di protezione dei dati.

² Decisione 2000/520/CE della Commissione, del 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 (GU L 215 del 25.8.2000, pag. 7).

³ Decisione 2009/820/PESC del Consiglio, del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'estradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America (GU L 291 del 7.11. 2009, pag. 40).

⁴ Decisione 2012/472/UE, del 26 aprile 2012, relativa alla conclusione dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al Dipartimento degli Stati Uniti per la Sicurezza interna (GU L 215 dell'11.8.2012, pag. 4).

⁵ Decisione del Consiglio, del 13 luglio 2010, relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (GU L 195 del 27.7.2010, pag. 3).

protezione dei dati personali. Oltre a ciò, l'UE e gli USA stanno attualmente negoziando un accordo quadro sulla protezione dei dati nell'ambito della cooperazione di polizia e giudiziaria⁶ (in appresso: "accordo quadro"). Lo scopo è garantire un livello elevato di protezione dei dati per i cittadini i cui dati sono oggetto di scambi, accrescendo così la cooperazione fra l'UE e gli USA nella lotta contro la criminalità e il terrorismo sulla base di valori condivisi e di garanzie convenute di comune accordo.

Questi strumenti intervengono in un contesto in cui i flussi di dati personali stanno acquisendo sempre maggiore importanza.

Da un lato, lo sviluppo dell'economia digitale ha portato a una crescita esponenziale nella quantità, qualità, diversità e natura delle attività di trattamento dei dati. L'uso dei servizi di comunicazione elettronica da parte dei cittadini nella vita quotidiana è aumentato. I dati personali sono diventati un bene molto prezioso: il valore stimato dei dati dei cittadini dell'UE era di 315 miliardi di euro nel 2011 e potenzialmente potrebbe raggiungere il bilione di euro per il 2020⁷. Il mercato dell'analisi di grosse quantità di dati sta registrando una crescita mondiale annua del 40%⁸. Analogamente, gli sviluppi tecnologici, relativi ad esempio al cloud computing, hanno mostrato l'importanza della nozione di trasferimento internazionale di dati, poiché i flussi transfrontalieri stanno diventando una realtà quotidiana.⁹

L'aumento dell'uso dei servizi di comunicazione elettronica e di trattamento dei dati, compreso il cloud computing, ha anche considerevolmente ampliato il campo d'applicazione e la rilevanza dei trasferimenti transatlantici di dati: aspetti quali la posizione centrale delle società americane nell'economia digitale¹⁰, il routing transatlantico di gran parte delle comunicazioni elettroniche e il volume dei flussi di dati elettronici fra l'UE e gli USA sono diventati ancora più importanti.

D'altro lato, i metodi moderni di trattamento dei dati personali sollevano nuove e importanti questioni. Esse riguardano sia i nuovi mezzi di trattamento su larga scala dei dati dei consumatori a fini commerciali da parte delle società private, sia l'accresciuta capacità di controllo su larga scala dei dati delle comunicazioni da parte dei servizi di intelligence.

I programmi di raccolta di intelligence su larga scala degli Stati Uniti, come PRISM, pregiudicano i diritti fondamentali degli Europei e specificamente il diritto alla privacy e alla protezione dei dati personali. Questi programmi suggeriscono inoltre l'esistenza di un legame fra il controllo esercitato dal governo e il trattamento dei dati da parte delle società private, in particolare le società americane del settore di Internet — nel qual caso essi potrebbero anche avere un impatto economico. Il fatto che i cittadini siano preoccupati per il trattamento su larga scala dei loro dati personali da parte di società private o per il controllo dei loro dati da parte delle agenzie di intelligence in occasione dell'uso dei servizi Internet può incidere sulla loro fiducia nell'economia digitale, con potenziali conseguenze negative sulla crescita.

⁶ Il Consiglio ha adottato la decisione che autorizza la Commissione a negoziare l'accordo il 3 dicembre 2010. Si veda IP/10/1661 del 3 dicembre 2010.

⁷ Si veda: Boston Consulting Group, "The Value of our Digital Identity", novembre 2012.

⁸ Si veda: McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011.

⁹ Comunicazione: " Sfruttare il potenziale del cloud computing in Europa" (COM(2012) 529 final).

¹⁰ Ad esempio, nel giugno 2012 il numero combinato di visitatori unici europei di Microsoft Hotmail, Google Gmail and Yahoo! Mail ha superato i 227 milioni, eclissando così tutti gli altri provider. Il numero combinato di utenti unici europei che si sono collegati a Facebook e Facebook Mobile nel marzo 2012 è stato pari a 196,5 milioni, facendo così di Facebook il primo social network in Europa. Google è il principale motore di ricerca su Internet, con una percentuale del 90,2% degli internauti su scala mondiale. Nel giugno 2013, il servizio di messaggiera mobile americano What's App è stato usato dal 91% degli utenti iPhone in Germania.

Questi sviluppi espongono i flussi di dati fra l'UE e gli USA a nuove sfide, affrontate nella presente comunicazione che esamina quali strade percorrere in futuro sulla base delle conclusioni della relazione dei copresidenti dell'UE del gruppo di lavoro ad hoc UE-USA e della comunicazione relativa all'Approdo sicuro.

Essa mira a tracciare un percorso efficace per ripristinare un clima di fiducia, per rafforzare la cooperazione fra l'Unione europea e gli Stati Uniti nei settori in questione e per consolidare nel complesso la relazione transatlantica.

La presente comunicazione parte dal principio che le regole sulla protezione dei dati personali debbano essere studiate nel loro specifico contesto, senza incidere su altre dimensioni delle relazioni UE-USA, comprese le trattative in corso per un Partenariato transatlantico in materia di scambi commerciali e investimenti. Per questo motivo, le norme sulla protezione dei dati non saranno negoziate nell'ambito di tale partenariato, che le rispetterà pienamente.

È importante osservare che, se l'UE può prendere provvedimenti in settori di sua competenza, in particolare per garantire l'applicazione del diritto europeo¹¹, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro¹².

2. INCIDENZA SUGLI STRUMENTI DI TRASFERIMENTO DEI DATI

In primo luogo, per quanto riguarda i dati trasferiti a fini commerciali, l'Approdo sicuro si è rivelato un importante vettore per il passaggio di informazioni fra l'UE e gli USA. La sua rilevanza si è accresciuta a mano a mano che i flussi di dati personali hanno rivestito sempre maggiore importanza nelle relazioni commerciali transatlantiche. Negli ultimi tredici anni, il regime di Approdo sicuro si è ampliato fino ad includere più di 3 000 imprese, più della metà delle quali hanno aderito negli ultimi cinque anni. Tuttavia, le preoccupazioni sul livello di protezione dei dati personali dei cittadini UE trasferiti agli Stati Uniti nell'ambito del principio dell'Approdo sicuro sono aumentate. La natura volontaria e dichiarativa del regime ha difatti attirato grande attenzione sulla sua trasparenza e sulla sua applicazione. Se la maggioranza delle società americane ne applicano i principi, alcune imprese auto-certificate non lo fanno. La non osservanza dei principi d'Approdo sicuro da parte di alcune società auto-certificate conferisce loro un vantaggio competitivo rispetto ad imprese europee operanti sugli stessi mercati.

Il regime Approdo sicuro consente inoltre deroghe alle norme sulla protezione dei dati per motivi di sicurezza nazionale¹³, ed è sorta la questione se la raccolta e il trattamento su larga scala di informazioni di natura personale nell'ambito dei programmi di controllo americani siano necessari e proporzionati per rispondere agli interessi di sicurezza nazionale. Emerge poi chiaramente dalle conclusioni del gruppo di lavoro ad hoc UE-USA che questi programmi non conferiscono ai cittadini europei gli stessi diritti e le stesse garanzie procedurali goduti dai cittadini americani.

La portata di questi programmi di controllo, associata alla disparità di trattamento riservata ai cittadini europei, mette in questione il livello di protezione offerto dall'accordo Approdo sicuro. I dati personali dei cittadini dell'UE inviati negli USA nell'ambito di tale regime possono essere consultati e ulteriormente trattati dalle autorità americane in maniera incompatibile con i motivi per cui erano stati originariamente raccolti nell'UE e con le finalità

¹¹ Si veda la sentenza della Corte di giustizia dell'Unione europea nella causa C-300/11, *ZZ/Secretary of State for the Home Department*.

¹² Articolo 4, paragrafo 2, del TUE.

¹³ Si veda ad es. l'allegato I della decisione Approdo sicuro.

del loro trasferimento agli Stati Uniti. La maggior parte delle imprese Internet americane che risultano più direttamente interessate da questi programmi sono certificate nell'ambito del regime Approdo sicuro.

In secondo luogo, per quanto riguarda gli scambi di dati a fini di attività di contrasto, gli accordi esistenti (PNR, TFTP) si sono rivelati strumenti molto preziosi per affrontare minacce comuni alla sicurezza legate a reati gravi di natura transnazionale e al terrorismo, e che prevedono al tempo stesso garanzie di un elevato livello di protezione di dati¹⁴. Queste garanzie si applicano anche ai cittadini dell'UE, e gli accordi prevedono meccanismi per riesaminare la loro attuazione e per affrontare eventuali problemi collegati. L'accordo TFTP stabilisce anche un sistema di supervisori indipendenti che controllano come gli Stati Uniti effettuano le ricerche sui dati contemplati dall'accordo.

A seguito delle preoccupazioni sorte nell'UE sui programmi di controllo americani, la Commissione europea si è avvalsa di questi meccanismi per verificare le modalità d'attuazione degli accordi. Nel caso dell'accordo PNR è stato effettuato un riesame comune, cui hanno partecipato esperti in materia di protezione dei dati dell'UE e degli USA che ne hanno esaminato le modalità d'applicazione¹⁵. Dal riesame non è emersa alcuna indicazione del fatto che i programmi di controllo degli Stati Uniti si estendano ai dati dei passeggeri rientranti nell'accordo PNR o che abbiano una qualche incidenza su di essi. Per quanto riguarda l'accordo TFTP, la Commissione ha avviato consultazioni ufficiali dopo che i servizi di intelligence americani sono stati accusati di accedere direttamente a dati personali nell'UE, contrariamente alle disposizioni dell'accordo. Da queste consultazioni non sono emersi elementi che dimostrino una violazione dell'accordo TFTP; gli Stati Uniti sono stati comunque indotti a fornire un'assicurazione scritta del fatto che nessuna raccolta diretta di dati fosse avvenuta in violazione delle disposizioni dell'accordo.

La raccolta e il trattamento su larga scala di informazioni di carattere personale nell'ambito dei programmi americani di controllo rendono tuttavia necessario continuare in futuro uno strettissimo monitoraggio dell'attuazione degli accordi PNR e TFTP. L'UE e gli USA hanno quindi convenuto di anticipare il prossimo riesame comune dell'accordo TFTP, che avrà luogo nella primavera 2014. Nell'ambito di tale riesame comune e di quelli che seguiranno il funzionamento del sistema di supervisione e la protezione che esso offre per i dati dei cittadini europei saranno oggetto di una maggiore trasparenza. Parallelamente, verranno adottati provvedimenti per garantire che il sistema di supervisione continui a seguire da vicino le modalità di trattamento dei dati trasferiti negli Stati Uniti in virtù dell'accordo, con particolare attenzione allo scambio di tali dati fra le autorità americane.

In terzo luogo, l'aumento nel volume di trattamento dei dati personali evidenzia l'importanza delle garanzie giuridiche e amministrative applicabili. Uno degli obiettivi del gruppo di lavoro ad hoc UE-USA era stabilire quali garanzie applicare per ridurre al minimo l'impatto del trattamento sui diritti fondamentali dei cittadini europei. Sono altresì necessarie garanzie per proteggere le imprese. Alcune leggi americane, come il Patriot Act, consentono alle autorità americane di chiedere direttamente alle imprese l'accesso a dati conservati nell'UE. Pertanto le imprese europee, e le imprese statunitensi presenti nell'UE, possono vedersi

¹⁴ Si veda la relazione congiunta della Commissione e del Dipartimento statunitense del Tesoro relativa al valore dei dati forniti nell'ambito del TFTP ai sensi dell'articolo 6, paragrafo 6, dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria ai fini del programma di controllo delle transazioni finanziarie dei terroristi.

¹⁵ Si veda la relazione della Commissione: "Riesame comune dell'applicazione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento delle registrazioni dei nominativi dei passeggeri al Dipartimento degli Stati Uniti per la Sicurezza interna".

chiedere di trasferire dati negli USA in violazione del diritto dell'UE e degli Stati membri, e possono trovarsi di conseguenza di fronte ad obblighi giuridici contrastanti. L'incertezza del diritto che deriva da tali richieste dirette può ostacolare lo sviluppo di nuovi servizi digitali, come il cloud computing, che permettono di offrire soluzioni efficaci ed economiche per i cittadini e per le imprese.

3. GARANTIRE UNA PROTEZIONE EFFICACE DEI DATI

Il trasferimento di dati personali fra l'UE e gli USA è una componente essenziale delle relazioni commerciali transatlantiche. Lo scambio di informazioni è a sua volta una componente fondamentale della cooperazione UE-USA in materia di sicurezza, e riveste un'importanza centrale ai fini dell'obiettivo comune della prevenzione e della lotta contro le forme gravi di criminalità e il terrorismo. Tuttavia, le recenti rivelazioni sui programmi di raccolta di intelligence statunitensi hanno inciso negativamente sulla fiducia su cui si basa questa cooperazione. In particolare, è stata scossa la fiducia nelle modalità di trattamento dei dati personali. Per ripristinare tale fiducia nel trasferimento di dati, nell'interesse dell'economia digitale, della sicurezza dell'UE e degli USA, e delle relazioni transatlantiche in generale, occorre prendere le misure esposte in appresso.

3.1. La riforma europea in materia di protezione dei dati

La riforma della protezione dei dati proposta dalla Commissione nel gennaio 2012¹⁶ apporta risposte fondamentali per quanto riguarda la protezione dei dati personali. Cinque componenti del proposto pacchetto sulla protezione dei dati sono di particolare importanza.

In primo luogo, per quanto riguarda l'applicazione territoriale, il regolamento proposto dispone chiaramente che le imprese non stabilite nell'Unione dovranno applicare la normativa europea sulla protezione dei dati quando offrono beni e servizi ai consumatori europei o ne controllano il comportamento. In altre parole, il diritto fondamentale alla protezione dei dati sarà rispettato, indipendentemente dall'ubicazione geografica di un'impresa o dalle sue strutture di trattamento¹⁷.

In secondo luogo, per quanto riguarda la dimensione internazionale, il regolamento proposto stabilisce le condizioni a cui i dati possono essere trasferiti al di fuori dell'UE: tali trasferimenti possono essere autorizzati solo quando tali condizioni — che tutelano il diritto delle persone fisiche a un alto livello di protezione — sono rispettate¹⁸.

¹⁶ Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, Bruxelles, 25.1.2012 (COM(2012) 10 final) e Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (COM(2012) 11 final).

¹⁷ La Commissione prende nota che il Parlamento europeo ha confermato e rafforzato questo importante principio, sancito dall'articolo 3 del regolamento proposto, nel voto del 21 ottobre 2013 sulle relazioni riguardanti la riforma della protezione dei dati dei deputati Jan-Philipp Albrecht e Dimitrios Droutsas in seno alla Commissione Libertà civile, Giustizia e Affari interni (LIBE).

¹⁸ La Commissione prende nota del fatto che nel voto del 21 ottobre 2013 la Commissione LIBE del Parlamento europeo ha proposto di inserire nel futuro regolamento una disposizione, secondo cui le richieste di autorità straniere di accesso a dati personali raccolti nell'UE verrebbero subordinate all'ottenimento di un'autorizzazione preliminare di un'autorità nazionale per la tutela dei dati, qualora tali domande siano formulate al di fuori di un trattato di mutua assistenza giudiziaria o di altro accordo internazionale.

In terzo luogo, per quanto concerne l'attuazione, le norme proposte prevedono sanzioni proporzionate e dissuasive (fino al 2% del fatturato mondiale annuo dell'impresa) per garantire che le imprese rispettino il diritto dell'UE¹⁹. L'esistenza di sanzioni credibili spingerà maggiormente le imprese ad osservare le normative europee.

Quarto, il regolamento proposto comporta chiare norme sugli obblighi e le responsabilità degli incaricati del trattamento, come i fornitori di cloud computing, anche per quanto riguarda la sicurezza²⁰. Come hanno mostrato le rivelazioni sui programmi americani di raccolta di intelligence, si tratta di un punto cruciale poiché questi programmi vanno anche a toccare i dati immagazzinati nella nuvola. Inoltre, le imprese che forniscono spazio di stoccaggio nella nuvola, e a cui si chiede di fornire dati personali ad autorità straniere, non potranno sfuggire alla loro responsabilità invocando il loro status di incaricato del trattamento anziché di responsabile del trattamento.

Quinto, il pacchetto porterà a stabilire un insieme completo di norme per la protezione dei dati personali trattati a fini di attività di contrasto.

Il pacchetto dovrebbe essere rapidamente adottato nel corso del 2014²¹.

3.2. Migliorare il regime "Approdo sicuro"

Il regime Approdo sicuro è una componente importante delle relazioni commerciali UE-USA, su cui contano le imprese di entrambe le sponde dell'Atlantico.

La relazione della Commissione sul funzionamento di tale regime ha individuato una serie di punti deboli. A causa di una mancanza di trasparenza e di carenze nell'attuazione, alcuni membri auto-certificati del regime non ne osservano, in pratica, i principi. Questo ha un impatto negativo sui diritti fondamentali dei cittadini dell'UE, e mette inoltre in svantaggio le imprese europee rispetto alle loro concorrenti americane che operano nell'ambito dello stesso regime ma che in pratica non ne rispettano i principi. Questi squilibri incidono anche sulla maggior parte delle imprese americane che invece applicano correttamente il regime. Approdo sicuro funge inoltre da interfaccia per il trasferimento di dati personali di cittadini dell'UE dall'Unione europea agli Stati Uniti da parte di imprese che sono tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi. Se le carenze riscontrate non vengono corrette, si crea pertanto uno svantaggio competitivo per le imprese dell'UE e un impatto negativo sul diritto fondamentale alla protezione dei dati dei cittadini dell'Unione.

Le carenze del regime Approdo sicuro sono state sottolineate dalla reazione delle autorità europee per la protezione dei dati alle recenti rivelazioni sui programmi americani di controllo. L'articolo 3 della decisione Approdo sicuro autorizza dette autorità a sospendere, a certe condizioni, i flussi di dati verso imprese certificate.²² I Commissari tedeschi per la

¹⁹ La Commissione prende nota del fatto che nel voto del 21 ottobre 2013 la Commissione LIBE ha proposto di rafforzare la proposta della Commissione prevedendo che le ammende possano arrivare fino al 5% del fatturato mondiale annuo di una società.

²⁰ La Commissione prende nota del fatto che nel voto del 21 ottobre 2013 la Commissione LIBE ha sostenuto un rafforzamento degli obblighi e delle responsabilità degli incaricati del trattamento, in particolare in relazione all'articolo 26 del regolamento proposto.

²¹ Nelle conclusioni del Consiglio europeo dell'ottobre 2013 si legge: "È importante alimentare la fiducia di cittadini e imprese nell'economia digitale. L'adozione tempestiva di un solido quadro generale dell'UE per la protezione dei dati e della direttiva sulla sicurezza informatica è essenziale per il completamento del mercato unico digitale entro il 2015".

²² Nello specifico, ai sensi dell'articolo 3 della decisione Approdo sicuro, tale sospensione può avvenire nei casi in cui sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere

protezione dei dati hanno deciso di non rilasciare più nuove autorizzazioni di trasferimenti di dati verso paesi non UE (ad esempio per l'uso di certi servizi di cloud computing), ed esamineranno anche l'opportunità di sospendere eventualmente i trasferimenti di dati nell'ambito del regime Approdo sicuro.²³ Il rischio è che tali misure, prese a livello nazionale, creino disparità a livello di applicazione del regime, il che significa che Approdo sicuro cesserà di essere un meccanismo centrale per il trasferimento dei dati personali fra l'UE e gli USA.

Ai sensi della direttiva 95/46/CE la Commissione ha il potere di sospendere o annullare la decisione Approdo sicuro se il regime non offre più un livello di protezione adeguato. Inoltre, l'articolo 3 della decisione Approdo sicuro prevede che la Commissione possa annullare o sospendere la decisione stessa, o limitarne il campo d'applicazione, mentre l'articolo 4 dispone che essa possa adattarla in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione.

In questo contesto possono essere prese in considerazione varie opzioni, in particolare:

- mantenere lo *status quo*;
- rafforzare il regime Approdo sicuro e rivederne approfonditamente il funzionamento;
- sospendere o annullare la decisione Approdo sicuro.

Tenuto conto dei punti deboli individuati, il regime Approdo sicuro non può continuare ad essere applicato secondo le attuali modalità. Tuttavia, abrogarlo nuocerebbe agli interessi delle imprese che ne sono membri, nell'UE e negli USA. La Commissione ritiene che il regime Approdo sicuro dovrebbe piuttosto essere rafforzato.

I miglioramenti dovrebbero riguardare i punti deboli strutturali relativi alla trasparenza e all'applicazione, i principi sostanziali dell'Approdo sicuro e il funzionamento dell'eccezione per motivi di sicurezza nazionale.

Più specificamente, perché Approdo sicuro funzioni come dovrebbe, il controllo e la supervisione da parte delle autorità americane del rispetto dei principi del regime da parte delle imprese certificate deve essere più efficace e sistematico. Va inoltre migliorata la trasparenza delle politiche di tutela della sfera privata delle imprese certificate, e devono essere garantite ai cittadini dell'UE la disponibilità e l'accessibilità di meccanismi di soluzione dei contenziosi.

Come prima questione urgente, la Commissione comincerà col discutere con le autorità americane i punti deboli individuati. Sarebbe opportuno definire le misure da prendere per rimediare entro l'estate 2014 e applicarle il più rapidamente possibile. Su questa base, la Commissione procederà a un bilancio completo del funzionamento del regime Approdo sicuro. Questo ampio processo di riesame dovrebbe comportare una consultazione aperta e un dibattito in seno al Parlamento europeo e al Consiglio, così come discussioni con le autorità americane.

che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto; la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare.

²³ *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, comunicato stampa del 24 luglio 2013.

È altresì importante che l'eccezione per motivi di sicurezza nazionale prevista dalla decisione Approdo sicuro sia applicata solo in misura strettamente necessaria e proporzionata.

3.3. Rafforzare le garanzie in materia di protezione dei dati nel contesto della cooperazione fra autorità di contrasto

L'Unione europea e gli Stati Uniti stanno attualmente negoziando un accordo quadro sulla protezione dei dati relativo ai trasferimenti e al trattamento di informazioni di carattere personale nell'ambito della cooperazione di polizia e giudiziaria in materia penale. La conclusione di un tale accordo, che offre un elevato livello di protezione dei dati personali, rappresenterebbe un importante apporto al rafforzamento della fiducia fra le due sponde dell'Atlantico. Migliorando la protezione dei diritti dei cittadini dell'UE in materia di tutela dei dati, contribuirebbe a rafforzare la cooperazione transatlantica volta a prevenire e a combattere la criminalità e il terrorismo.

Conformemente alla decisione che autorizza la Commissione a negoziare l'accordo quadro, l'obiettivo delle trattative dovrebbe essere garantire un elevato livello di protezione in linea con l'acquis dell'UE sulla tutela dei dati. Questo dovrebbe tradursi in regole e garanzie concordate riguardanti, fra l'altro, la limitazione delle finalità e le condizioni e la durata della conservazione dei dati. Nell'ambito dei negoziati la Commissione dovrebbe inoltre ottenere impegni in materia di diritti applicabili, compresi i meccanismi di ricorso giudiziario, per i cittadini dell'UE non residenti negli Stati Uniti²⁴. La stretta cooperazione UE-USA per affrontare le sfide comuni in materia di sicurezza dovrebbe rispecchiarsi negli sforzi posti in atto per garantire che i cittadini godano degli stessi diritti, quando gli stessi dati sono trattati agli stessi scopi, sulle due sponde dell'Atlantico. È anche importante che vengano definite rigorosamente le deroghe fondate su motivi di sicurezza nazionale. Occorre altresì concordare a questo riguardo garanzie e limitazioni.

Queste trattative offrono l'opportunità di precisare che i dati personali detenuti da imprese private e ubicate nell'UE non saranno direttamente accessibili alle autorità di contrasto statunitensi né saranno trasferite a tali autorità al di fuori dei canali ufficiali di cooperazione, come gli accordi sulla mutua assistenza giudiziaria o gli accordi settoriali UE-USA che autorizzano questo tipo di trasferimenti. L'accesso tramite altri mezzi dovrebbe essere escluso, a meno che non avvenga in situazioni chiaramente definite, eccezionali e che possano essere sottoposte a sindacato giurisdizionale. Gli USA dovrebbero assumere impegni a tale riguardo²⁵.

²⁴ Si veda il relativo passo del comunicato stampa congiunto emanato a seguito della riunione ministeriale UE-USA "Giustizia e Affari interni" del 18 novembre 2013 a Washington: "Ci siamo quindi impegnati, come questione d'urgenza, ad avanzare rapidamente nei negoziati su un accordo quadro ampio e significativo nel campo delle attività di contrasto. Tale accordo servirebbe da base per facilitare i trasferimenti di dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale, garantendo un elevato livello di protezione dei dati personali per i cittadini degli USA e dell'UE. Ci siamo impegnati a lavorare per risolvere le restanti questioni sollevate dalle due Parti, compresa quella del ricorso giudiziario (questione fondamentale per l'UE). Il nostro obiettivo è portare a termine i negoziati sull'accordo entro l'estate 2014."

²⁵ Si veda il relativo passo del comunicato stampa congiunto emanato a seguito della riunione ministeriale UE-USA "Giustizia e Affari interni" del 18 novembre 2013 a Washington: "Sottolineiamo anche il valore dell'accordo UE-USA sulla mutua assistenza giudiziaria. Ribadiamo il nostro impegno a garantire che sia applicato ampiamente ed efficacemente per fini di ottenimento di prove nei procedimenti penali. Le discussioni hanno anche riguardato la necessità di precisare che i dati personali detenuti da entità private sul territorio dell'altra Parte non saranno accessibili alle autorità di contrasto al di fuori dei canali legalmente autorizzati. Conveniamo inoltre di riesaminare il funzionamento

Un accordo quadro convenuto in quest'ottica dovrebbe fornire la cornice generale per garantire un elevato livello di protezione dei dati personali trasferiti verso gli Stati Uniti a fini di prevenzione o di lotta contro la criminalità e il terrorismo. Accordi settoriali dovrebbero, qualora necessario data la natura dei trasferimenti di dati interessati, stabilire regole e garanzie supplementari, sul modello degli accordi PNR e TFTP fra l'UE e gli USA, che fissano condizioni rigorose per il trasferimento di dati e prevedono garanzie per i cittadini dell'UE.

3.4. Rispondere alle preoccupazioni europee nell'ambito dell'attuale processo di riforma in corso negli Stati Uniti

Il Presidente americano Obama ha annunciato una revisione delle attività delle autorità americane incaricate della sicurezza nazionale, compreso il quadro giuridico applicabile. Questo processo in corso offre un'importante opportunità di rispondere alle preoccupazioni dell'Unione europea suscitate dalle recenti rivelazioni sui programmi di raccolta di intelligence americani. I cambiamenti più importanti sarebbero: l'applicazione, ai cittadini dell'UE che non risiedono negli USA, delle stesse garanzie di cui godono i cittadini e residenti statunitensi; una maggiore trasparenza delle attività di intelligence e un rafforzamento dei controlli. Tali cambiamenti ripristinerebbero un clima di fiducia negli scambi di dati fra l'UE e gli USA, e promuovrebbero l'uso dei servizi di Internet da parte degli Europei.

Per quanto riguarda l'estensione, ai cittadini dell'UE, delle garanzie riconosciute ai cittadini e residenti statunitensi, le disposizioni giuridiche relative ai programmi di controllo americani che riservano un trattamento diverso ai cittadini USA e UE dovrebbero essere riesaminate, anche sotto l'aspetto della necessità e della proporzionalità, tenendo presente lo stretto partenariato transatlantico in materia di sicurezza, basato su valori, libertà e diritti comuni. Questo ridurrebbe le ripercussioni, sugli Europei, dei programmi di raccolta di intelligence americani.

Il controllo dei programmi americani di raccolta di intelligence potrebbe essere migliorato rafforzando il ruolo della Foreign Intelligence Surveillance Court e introducendo mezzi di ricorso per i singoli cittadini. Questi meccanismi potrebbero ridurre il trattamento di dati personali degli Europei che non sono rilevanti ai fini della sicurezza nazionale.

3.5. Promuovere norme di protezione della vita privata a livello internazionale

Le questioni sollevate dai metodi moderni di protezione dei dati non si limitano al trasferimento di informazioni fra l'UE e gli USA. Ogni persona dovrebbe vedersi garantito un livello elevato di protezione dei dati personali. Le norme dell'UE sulla raccolta, il trasferimento e il trattamento dei dati dovrebbero essere promosse a livello internazionale.

Sono state recentemente proposte una serie di iniziative per promuovere la protezione della privacy, in particolare su Internet²⁶. L'Unione europea dovrebbe garantire che tali iniziative, se portate avanti, tengano pienamente conto dei principi di protezione dei diritti fondamentali, della libertà d'espressione, dei dati personali e della vita privata quali enunciati nel diritto dell'UE e nella Strategia dell'UE per la sicurezza informatica, e non pregiudichino la libertà, l'apertura e la sicurezza del ciber spazio. Questo include un modello di governance democratico, efficiente e multilaterale.

dell'accordo sulla mutua assistenza giudiziaria, come previsto dall'accordo, e di consultarci ogniqualvolta necessario."

²⁶ Si veda a tale riguardo il progetto di risoluzione proposto all'Assemblea generale delle Nazioni Unite dalla Germania e dal Brasile, che invoca la protezione della privacy sia on-line che off-line.

Le riforme in corso della legislazione sulla protezione dei dati, nell'UE e negli USA, offrono a entrambi un'opportunità unica di stabilire norme a livello internazionale. Gli scambi di dati, fra le due sponde dell'Atlantico e al di là, trarrebbero grande vantaggio da un rafforzamento del quadro giuridico nazionale americano, inclusa l'adozione del Consumer Privacy Bill of Rights annunciato dal Presidente Obama nel febbraio 2012 come parte di un piano globale per migliorare la protezione della privacy dei consumatori. L'esistenza di una serie di regole rigorose e applicabili in materia di protezione di dati, sancite sia dall'UE che dagli USA, costituirebbe una solida base per i flussi transfrontalieri di dati.

Ai fini della promozione di norme di protezione della vita privata a livello internazionale, andrebbe favorita l'adesione alla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale ("Convenzione 108"), che è aperta a paesi che non sono membri del Consiglio d'Europa²⁷. Le salvaguardie e le garanzie convenute nelle sedi internazionali dovrebbero tradursi in un elevato livello di protezione compatibile con le esigenze del diritto dell'UE.

4. CONCLUSIONI E RACCOMANDAZIONI

Le questioni individuate nella presente comunicazione richiedono interventi sia da parte degli Stati Uniti che dell'Unione europea e dei suoi Stati membri.

Le preoccupazioni riguardanti gli scambi di dati transatlantici sono, in primo luogo, un campanello d'allarme per l'UE e gli Stati membri sull'esigenza di progredire rapidamente e in modo ambizioso sulla strada della riforma in materia di protezione dei dati. Quanto emerge è l'assoluta necessità di quadro legislativo solido, con chiare regole applicabili anche in situazioni di trasferimento di dati all'estero. Le istituzioni dell'UE dovrebbero pertanto continuare a lavorare in vista dell'adozione, entro la primavera 2014, della riforma sulla protezione di dati, per far sì che le informazioni di carattere personale siano protette in maniera effettiva e completa.

Data l'importanza dei flussi di dati transatlantici, è fondamentale che gli strumenti su cui essi si basano rispondano adeguatamente alle sfide e alle opportunità dell'era digitale e ai nuovi sviluppi tecnologici, come il cloud computing. Occorre che le disposizioni e gli accordi esistenti e futuri garantiscano la continuità di un elevato livello di protezione oltre Atlantico.

L'esistenza di un solido regime di Approdo sicuro è nell'interesse dei cittadini e delle imprese sia dell'UE che degli USA. Tale regime andrebbe rafforzato grazie a un migliore controllo e a una più efficace applicazione a breve termine e, su tali basi, con un più ampio riesame del suo funzionamento. Sono necessari miglioramenti per garantire che gli obiettivi originari della decisione Approdo sicuro — cioè continuità nella protezione dei dati, certezza del diritto e libera circolazione delle informazioni fra l'UE e gli USA — continuino ad essere realizzati.

Al centro di tali miglioramenti vi è la necessità che le autorità statunitensi sorvegliano e controllino meglio l'osservanza dei principi di Approdo sicuro in materia di riservatezza da parte delle imprese auto-certificate.

È altresì importante che l'eccezione per motivi di sicurezza nazionali prevista dalla decisione Approdo sicuro sia utilizzata solo in misura strettamente necessaria e proporzionata.

²⁷ Gli USA sono già Parte di un'altra Convenzione del Consiglio d'Europa: la Convenzione sulla criminalità informatica del 2001 (nota anche come la "Convenzione di Budapest").

Per quanto riguarda le attività di contrasto della criminalità, gli attuali negoziati sull'accordo quadro dovrebbero portare a un elevato livello di protezione per i cittadini di entrambe le sponde dell'Atlantico. Un tale accordo dovrebbe servire a rafforzare la fiducia degli Europei negli scambi di dati fra l'UE e gli USA, e dovrebbe fornire una base per sviluppare ulteriormente il partenariato e la cooperazione in materia di sicurezza UE-USA. Le trattative dovrebbero portare a stipulare impegni affinché gli Europei non residenti negli Stati Uniti godano di garanzie procedurali, compreso il ricorso giudiziario.

L'amministrazione americana dovrebbe impegnarsi a garantire che i dati personali detenuti da entità private nell'UE non siano direttamente accessibili alle autorità di contrasto USA al di fuori dei canali ufficiali di cooperazione (come gli accordi sulla mutua assistenza giudiziaria e gli accordi settoriali UE-USA come gli accordi PNR e TFTP, che autorizzano questi trasferimenti a condizioni rigorose), tranne che in situazioni chiaramente definite, eccezionali e che possano essere sottoposte a sindacato giurisdizionale.

Gli USA dovrebbero inoltre estendere ai cittadini dell'UE non residenti sul loro territorio le garanzie riconosciute ai cittadini e residenti statunitensi, dovrebbero garantire la necessità e la proporzionalità dei loro programmi, nonché una maggiore trasparenza e un maggior controllo nell'ambito del quadro giuridico applicabile alle autorità nazionali di sicurezza americane.

I settori di intervento indicati nella presente comunicazione richiederanno un impegno costruttivo da entrambe le sponde dell'Atlantico. Insieme, in quanto partner strategici, l'UE e gli USA hanno la capacità di superare le attuali tensioni nelle loro relazioni e di ripristinare un clima di fiducia nei loro scambi di dati. L'assunzione di impegni politici e giuridici sull'approfondimento della cooperazione in questi settori rafforzerà nel complesso le relazioni transatlantiche.