II

(Atti non legislativi)

DECISIONI

DECISIONE DI ESECUZIONE (UE) 2016/1250 DELLA COMMISSIONE

del 12 luglio 2016

a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy

[notificata con il numero C(2016) 4176]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la 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 ([1]), in particolare l'articolo 25, paragrafo 6,

sentito il garante europeo della protezione dei dati ([2]),

1. INTRODUZIONE

(1) La direttiva 95/46/CE stabilisce le regole per il trasferimento dei dati personali dagli Stati membri ai paesi terzi nella misura in cui tale trasferimento rientri nel suo ambito d'applicazione.

(2) L'articolo 1 e i considerando 2 e 10 della direttiva 95/46 intendono garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali ([3]).

(3) La giurisprudenza della Corte di giustizia ([4]) sottolinea l'importanza sia del diritto fondamentale al rispetto della vita privata, garantito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, sia del diritto fondamentale alla protezione dei dati personali, garantito dall'articolo 8 della stessa.

(4) A norma dell'articolo 25, paragrafo 1, della direttiva 95/46/CE, gli Stati membri sono tenuti a consentire il trasferimento di dati personali verso un paese terzo soltanto se il paese terzo garantisce un livello di protezione adeguato e se, prima del trasferimento stesso, sono rispettate le norme adottate dagli Stati membri in attuazione delle altre disposizioni della direttiva. La Commissione può constatare che un paese terzo garantisce tale livello di protezione adeguato in considerazione della sua legislazione nazionale o degli impegni internazionali che ha stipulato per proteggere i diritti delle persone. Fermo restando il rispetto delle disposizioni nazionali adottate conformemente alle altre disposizioni della direttiva, gli Stati membri possono in tale caso trasferire i dati personali senza che siano necessarie garanzie supplementari.

([1]) GU L 281 del 23.11.1995, pag. 31.
([2]) Cfr. parere n. 4/2016 relativo al progetto di decisione sull'adeguatezza del regime dello scudo UE-USA per la privacy, pubblicato il 30 maggio 2016.
([3]) Sentenza della Corte di giustizia nella causa *Maximillian Schrems contro Data Protection Commissioner* («*Schrems*»), C-362/14, ECLI:EU:C:2015:650, punto 39.
([4]) Sentenza *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, punto 47; sentenza *Digital Rights Ireland e a.*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, punto 53; sentenza *Google Spain e Google*, C-131/12, ECLI:EU:C:2014:317, punti 53, 66 e 74.

(5) A norma dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, il livello di protezione garantito da un paese terzo dovrebbe essere valutato con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati, comprese le norme di diritto, generali o settoriali, vigenti nel paese terzo in questione.

(6) La decisione 2000/520/CE della Commissione ([5]) ha considerato che, ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, i principi di approdo sicuro, attuati nel rispetto delle indicazioni fornite nelle cosiddette «domande più frequenti» pubblicate dal Dipartimento del Commercio degli Stati Uniti, garantissero un livello adeguato di protezione dei dati personali trasferiti dall'Unione alle organizzazioni stabilite negli Stati Uniti d'America.

(7) Nelle comunicazioni COM(2013) 846 final ([6]) e COM(2013) 847 final ([7]) del 27 novembre 2013, la Commissione ha affermato la necessità di rivedere e rafforzare il fondamento stesso del regime dell'approdo sicuro, in considerazione di una serie di fattori che sollevavano dubbi circa il livello di tutela che il regime era in grado di garantire, tra cui l'aumento esponenziale dei flussi di dati e la relativa importanza fondamentale per l'economia transatlantica, la rapida crescita del numero di imprese statunitensi aderenti al regime dell'approdo sicuro e le nuove informazioni disponibili sull'ampiezza e la portata di alcuni programmi di intelligence statunitensi. La Commissione ha riscontrato inoltre una serie di carenze e lacune nel regime dell'approdo sicuro.

(8) Muovendo dalle prove raccolte, tra cui le informazioni emerse dai lavori del gruppo di contatto UE-Stati Uniti sulla vita privata ([8]) e le informazioni sui programmi di intelligence statunitensi ricevute nell'ambito del gruppo di lavoro ad hoc UE-USA ([9]), la Commissione ha formulato 13 raccomandazioni per una revisione del regime dell'approdo sicuro. Le raccomandazioni chiedevano di rafforzare i principi sostanziali in materia di privacy attraverso una maggiore trasparenza delle politiche della privacy applicate delle imprese statunitensi che si autocertificano come aderenti al regime, un'azione più incisiva delle autorità statunitensi in termini di verifica, vigilanza e controllo dell'osservanza di tali principi, la disponibilità di meccanismi di composizione delle controversie di costo accessibile e la necessità di limitare alla misura strettamente necessaria e proporzionata il ricorso all'eccezione per motivi di sicurezza nazionale prevista dalla decisione 2000/520/CE.

(9) Con la sentenza del 6 ottobre 2015 nella causa C-362/14 *Maximillian Schrems contro Data Protection Commissioner* ([10]), la Corte di giustizia dell'Unione europea ha dichiarato invalida la decisione 2000/520/CE. Senza esaminare i principi dell'approdo sicuro nel merito, la Corte ha rilevato che, in tale decisione, la Commissione non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali ([11]).

(10) Al riguardo la Corte di giustizia ha chiarito che l'espressione «livello di protezione adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46/CE, pur non implicando un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, deve essere intesa nel senso che esige che il paese terzo assicuri un livello di protezione delle libertà e dei diritti fondamentali «sostanzialmente equivalente» a quello garantito all'interno dell'Unione in forza della direttiva 95/46/CE, letta alla luce della Carta dei diritti fondamentali. Anche se gli strumenti dei quali tale paese terzo si avvale al riguardo possono essere diversi da quelli attuati all'interno dell'Unione, tali strumenti devono cionondimeno rivelarsi efficaci nella prassi ([12]).

(11) La Corte di giustizia ha criticato il fatto che nella decisione 2000/520/CE manchino dichiarazioni sufficienti quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale, e quanto all'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura ([13]).

([5]) 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 28.8.2000, pag. 7).

([6]) Comunicazione della Commissione al Parlamento europeo e al Consiglio «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» — COM(2013) 846 final del 27 novembre 2013.

([7]) Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell'UE e delle società ivi stabilite — COM(2013) 847 final del 27 novembre 2013.

([8]) Cfr., ad esempio, Consiglio dell'Unione europea, Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection — documento 9831/08 del 28 maggio 2008, consultabile su Internet all'indirizzo http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection, del 27 novembre 2013 — consultabile su Internet all'indirizzo http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Cfr. nota a piè di pagina 3.

([11]) *Schrems*, punto 97.

([12]) *Schrems*, punti 73-74.

([13]) *Schrems*, punti 88-89.

(12) Nel 2014 la Commissione ha avviato un dialogo con le autorità statunitensi al fine di discutere di un rafforzamento del regime dell'approdo sicuro in linea con le 13 raccomandazioni formulate nella comunicazione COM (2013) 847 final. I colloqui si sono intensificati a seguito della sentenza *Schrems* della Corte di giustizia dell'Unione europea, nella prospettiva dell'adozione di un'eventuale nuova decisione sull'adeguatezza rispondente ai requisiti dell'articolo 25 della direttiva 95/46/CE quali interpretati dalla Corte di giustizia. I documenti allegati alla presente decisione, che saranno pubblicati anche nel Registro federale degli Stati Uniti d'America, costituiscono il risultato delle discussioni tenute. I principi in materia di privacy (allegato II) costituiscono, insieme agli impegni e alle dichiarazioni ufficiali delle varie autorità degli Stati Uniti riportati nei documenti di cui agli allegati I e da III a VII, lo «scudo UE-USA per la privacy» («scudo» o «regime»).

(13) La Commissione ha analizzato con attenzione le leggi e pratiche applicate negli Stati Uniti, compresi detti impegni e dichiarazioni ufficiali. In base alle constatazioni illustrate nei considerando 136-140, la Commissione giunge alla conclusione che gli Stati Uniti d'America assicurano un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo dall'Unione alle organizzazioni statunitensi che si sono autocertificate come aderenti al regime.

2. **SCUDO UE-USA PER LA PRIVACY**

(14) Lo scudo UE-USA per la privacy si fonda su un sistema di autocertificazione in base al quale l'organizzazione statunitense s'impegna a rispettare un insieme di principi in materia di privacy, ossia i principi del regime dello scudo UE-USA per la privacy, comprensivi dei principi supplementari (collettivamente denominati qui di seguito «principi»), emanati dal Dipartimento del Commercio degli USA e riportati nell'allegato II della presente decisione. Lo scudo si applica sia ai titolari sia ai responsabili del trattamento (procuratori), con la specificità che un contratto deve vincolare il responsabile del trattamento ad agire esclusivamente secondo le istruzioni del titolare del trattamento dell'UE e a prestargli assistenza per rispondere alle persone che esercitano i loro diritti nell'ambito dei principi ([14]).

(15) Fermo restando il rispetto delle disposizioni nazionali adottate in applicazione della direttiva 95/46/CE, la presente decisione ha l'effetto di autorizzare il trasferimento dei dati personali dai titolari o responsabili del trattamento nell'Unione alle organizzazioni presenti negli USA che si sono autocertificate come aderenti ai principi presso il Dipartimento del Commercio e si sono impegnate a conformarsi agli stessi. I principi si applicano al trattamento dei dati personali da parte di organizzazioni statunitensi esclusivamente se il trattamento da parte dell'organizzazione esula dall'ambito di applicazione della normativa dell'Unione ([15]). Lo scudo lascia impregiudicata l'applicazione della normativa dell'Unione che disciplina il trattamento dei dati personali negli Stati membri ([16]).

([14]) Cfr. allegato II, punto III.10.a. Conformemente alla definizione riportata al punto I.8.c, il titolare del trattamento dell'UE stabilisce le finalità e i mezzi del trattamento dei dati personali. Il contratto concluso col procuratore deve precisare altresì se l'ulteriore trasferimento è autorizzato (cfr. punto III.10.a.ii.2.).

([15]) Questo vale anche per i casi in cui sono trasferiti a partire dall'Unione dati relativi alle risorse umane nel contesto di un rapporto di lavoro. Nel sottolineare la «responsabilità primaria» del datore di lavoro dell'UE (cfr. allegato II, punto III.9.d.i.), i principi precisano che la condotta da questi tenuta è sottoposta alle norme applicabili nell'Unione e/o nel rispettivo Stato membro, e non ai principi medesimi (cfr. allegato II, punti III.9.a.i., b.ii., c.i., d.i).

([16]) Questo vale anche per il trattamento effettuato con strumenti situati nell'Unione ma usati da un'organizzazione stabilita al di fuori dell'Unione (cfr. articolo 4, paragrafo 1, lettera c), della direttiva 95/46/CE). A partire dal 25 maggio 2018 il regolamento generale sulla protezione dei dati si applicherà al trattamento dei dati personali i) nell'ambito delle attività di uno stabilimento del titolare del trattamento o del responsabile del trattamento nell'Unione (anche se il trattamento è effettuato negli Stati Uniti) o ii) di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione — cfr. articolo 3, paragrafi 1 e 2, del 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).

(16) La protezione dei dati personali offerta dallo scudo si applica a tutti gli interessati dell'UE ([17]) i cui dati personali sono trasferiti dall'Unione a organizzazioni degli USA che si sono autocertificate come aderenti ai principi presso il Dipartimento del Commercio.

(17) I principi si applicano immediatamente alla data di certificazione. L'unica eccezione attiene al principio sulla responsabilità in caso di ulteriore trasferimento, nell'eventualità in cui l'organizzazione che si autocertifica come aderente allo scudo intrattenga preesistenti rapporti commerciali con terzi. Dato che potrebbe essere necessario un certo tempo per conformare tali rapporti commerciali alle norme applicabili nell'ambito del principio sulla responsabilità in caso di ulteriore trasferimento, l'organizzazione è tenuta a assicurare tale conformità il più presto possibile, e comunque trascorsi non oltre nove mesi dall'autocertificazione (a condizione che questa abbia luogo nei primi due mesi successivi alla data di efficacia dello scudo). Nel corso del conseguente periodo di transizione l'organizzazione deve applicare i principi di informativa e di scelta (dando quindi all'interessato dell'UE la possibilità di rifiuto) e, se i dati personali sono trasferiti a un terzo che agisce come procuratore, deve accertarsi che questi assicuri almeno lo stesso livello di protezione richiesto dai principi ([18]). Il periodo di transizione rappresenta un equilibrio ragionevole e equo tra il rispetto del diritto fondamentale alla protezione dei dati e le legittime esigenze delle imprese in termini di disponibilità di tempo sufficiente per adattarsi al nuovo regime nei casi in cui l'adattamento interessi anche i rapporti commerciali che intrattengono con terzi.

(18) Il sistema sarà gestito e controllato dal Dipartimento del Commercio in base agli impegni da esso assunti nelle dichiarazioni della segretaria di Stato al Commercio degli USA (allegato I della presente decisione). Per quanto riguarda il controllo dell'applicazione dei principi, valgono le dichiarazioni formulate dalla Commissione federale del Commercio (FTC) e dal Dipartimento dei Trasporti, riportate negli allegati IV e V della presente decisione.

2.1. *Principi in materia di privacy*

(19) Autocertificandosi nell'ambito dello scudo UE-USA per la privacy l'organizzazione s'impegna a rispettare i principi ([19]).

(20) Secondo il *principio sull'informativa* l'organizzazione è tenuta a informare l'interessato di una serie di elementi d'importanza fondamentale per il trattamento dei dati personali che lo riguardano (ad esempio, tipo di dati raccolti, finalità del trattamento, diritto di accesso e di scelta, condizioni applicabili all'ulteriore trasferimento, responsabilità). Si applicano ulteriori garanzie, in particolare l'obbligo in capo all'organizzazione di rendere pubblica la politica della privacy seguita (che deve rispecchiare i principi) e di fornire collegamenti ipertestuali al sito web del Dipartimento del Commercio (che riporta ulteriori precisazioni sull'autocertificazione, sui diritti degli interessati e sui meccanismi di ricorso disponibili), all'elenco degli aderenti dello scudo [di cui al considerando (30)] e al sito web di un adeguato organo alternativo di composizione delle controversie.

(21) Secondo il *principio sull'integrità dei dati e la limitazione della finalità* i dati personali rilevati devono limitarsi a informazioni pertinenti ai fini del trattamento, affidabili per l'uso previsto, accurate, complete e aggiornate L'organizzazione non può trattare i dati personali in modo incompatibile con la finalità per cui sono stati raccolti in origine o con quella successivamente autorizzata dall'interessato. L'organizzazione deve assicurare che i dati personali siano affidabili per l'uso previsto, accurati, completi e aggiornati.

([17]) La presente decisione è rilevante ai fini del SEE. L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La normativa dell'Unione sulla protezione dei dati, direttiva 95/46/CE compresa, è materia contemplata dall'accordo SEE, nel cui allegato XI è stata integrata. Il Comitato misto SEE deve decidere in merito all'integrazione della presente decisione nell'accordo SEE. Una volta che la presente decisione si applicherà all'Islanda, al Liechtenstein e alla Norvegia, lo scudo UE-USA per la privacy riguarderà anche questi tre paesi e i riferimenti fatti all'UE e ai suoi Stati membri nella relativa documentazione s'intenderanno comprensivi di Islanda, Liechtenstein e Norvegia.

([18]) Cfr. allegato II, punto III.6.e.

([19]) Ai dati sulle risorse umane raccolti nel contesto di un rapporto di lavoro si applicano le regole particolari recanti garanzie supplementari previste dal principio «Dati sulle risorse umane» dei principi in materia di privacy (cfr. allegato II, punto III.9). Il datore di lavoro dovrebbe ad esempio rispettare le preferenze dei dipendenti in fatto di tutela della sfera privata limitando l'accesso ai dati personali, rendendo anonimi taluni dati o attribuendo codici o pseudonimi. Relativamente a tali dati, all'organizzazione è soprattutto imposto di collaborare con le autorità di protezione dei dati dell'Unione e di conformarsi ai loro pareri.

(22) Se il trattamento ha una finalità nuova (modificata) sostanzialmente diversa dalla finalità originaria ma comunque compatibile con essa, il *principio sulla scelta* conferisce all'interessato il diritto di rifiuto. Il *principio sulla scelta* non soppianta l'esplicito divieto di trattamento incompatibile ([20]). Al marketing diretto si applicano norme particolari che permettono di rifiutare «in qualsiasi momento» l'uso dei dati personali ([21]). Per i dati sensibili l'organizzazione deve di norma ottenere il consenso esplicito dell'interessato (facoltà di accettazione).

(23) Sempre in base al *principio sull'integrità dei dati e la limitazione della finalità*, è possibile conservare le informazioni personali in una forma che identifica o permette d'identificare l'interessato (ossia in forma di dati personali) solo per il tempo necessario per conseguire la o le finalità per cui sono stati raccolti in origine o quella o quelle successivamente autorizzate. Quest'obbligo non osta a che l'organizzazione aderente allo scudo continui a trattare le informazioni personali per periodi più lunghi, ma limitatamente al periodo e alla misura in cui il trattamento sia ragionevolmente funzionale a uno dei seguenti scopi specifici: archiviazione nel pubblico interesse, attività giornalistica, letteraria e artistica, ricerca scientifica e storica, analisi statistica. Il periodo di conservazione dei dati personali può essere prolungato per uno di tali scopi subordinatamente alla vigenza delle garanzie previste dai principi.

(24) Secondo il *principio sulla sicurezza* l'organizzazione che crea, detiene, usa o diffonde dati personali deve adottare misure di sicurezza «ragionevoli e adeguate», tenuto conto dei rischi insiti nel trattamento dei dati e nella loro natura. Se il trattamento è delegato a un terzo, l'organizzazione deve concludere con esso un contratto che garantisca lo stesso livello di protezione previsto dai principi e adottare misure per assicurarne la corretta attuazione.

(25) Secondo il *principio sull'accesso* ([22]), l'interessato ha diritto di sapere dall'organizzazione, senza dover giustificare la domanda e per un corrispettivo non eccessivo, se questa tratti dati personali che lo riguardano e di ottenerne la comunicazione entro tempi ragionevoli. Tale diritto può subire limitazioni soltanto in circostanze eccezionali: il diniego del diritto di accesso o la sua limitazione devono essere necessari e giustificati debitamente, e l'onere di dimostrare il soddisfacimento di tali condizioni incombe all'organizzazione. L'interessato deve poter correggere, modificare o cancellare le informazioni personali che lo riguardano quando non sono accurate o quando sono state trattate in violazione dei principi. Nei settori in cui è diffuso tra le imprese il ricorso al trattamento automatizzato dei dati personali per l'adozione di decisioni che si ripercuotono sulla persona (erogazione di credito, offerta di prestiti ipotecati, lavoro ecc.), la legge statunitense offre tutele specifiche contro le decisioni sfavorevoli ([23]). In base alla normativa vigente, la persona ha diritto di essere informata delle ragioni specifiche su cui si fonda decisione (ad esempio il rifiuto di erogarle un prestito), di contestare le informazioni incomplete o inesatte (e il fatto di aver basato illegittimamente la decisione su determinati fattori) e di impugnare la decisione sfavorevole. Queste norme tutelano la persona nei casi, presumibilmente assai limitati, in cui un'organizzazione aderente allo scudo adotterà in prima persona una decisione con procedura automatizzata ([24]). Poiché nell'economia digitale moderna è sempre più frequente il ricorso a un trattamento automatizzato (profilazione compresa) come base per l'adozione di decisioni che si ripercuotono sulle persone, si tratta tuttavia di un settore su cui esercitare un monitoraggio attento. Per agevolare questo monitoraggio, si è convenuto con le autorità statunitensi di comprendere nel primo riesame annuale e, secondo il caso, in quelli successivi un dialogo sul processo decisionale automatizzato, confrontandosi tra l'altro sulle analogie e sulle differenze d'impostazione tra l'UE e gli USA.

([20]) Questo vale per tutti i dati trasferiti nell'ambito dello scudo, compresi quelli raccolti nel contesto di un rapporto di lavoro. Benché possa usare, in linea di principio, i dati sulle risorse umane per finalità diverse che esulano dal rapporto di lavoro (ad esempio per talune comunicazioni commerciali), l'organizzazione statunitense autocertificatasi deve osservare il divieto di trattamento incompatibile, e comunque procedere solo nel rispetto dei *principi sull'informativa* e *sulla scelta*. Vietando all'organizzazione statunitense l'adozione di provvedimenti punitivi, compreso in forma di limitazione delle possibilità occupazionali, nei confronti del dipendente che ha esercitato tale diritto di scelta, si assicura che il dipendente, nonostante il rapporto di subordinazione e di intrinseca dipendenza, sia libero da pressioni e possa quindi compiere una scelta autenticamente libera.

([21]) Cfr. allegato II, punto III.12.

([22]) Cfr. anche il principio supplementare sull'accesso (allegato II, punto III.8).

([23]) Cfr., ad esempio, la legge sulle pari opportunità nel credito (ECOA — Codice degli Stati Uniti d'America, titolo 15, articolo 1691 e ss.), legge sull'informativa corretta nel credito (FRCA — Codice degli Stati Uniti d'America, titolo 15, articolo 1681 e ss.) o legge sulle pari opportunità negli alloggi (FHA, Codice degli Stati Uniti d'America, titolo42, articolo 3601 e ss.).

([24]) Nel contesto del trasferimento di dati personali raccolti nell'Unione, nella maggior parte dei casi la persona (il cliente) entra in un rapporto contrattuale con il titolare del trattamento dell'UE, che di norma è quindi il soggetto che adotta l'eventuale decisione basata su un trattamento automatizzato, e il titolare del trattamento dell'UE è vincolato alle norme dell'Unione in materia di protezione dei dati. Rientra in questo contesto anche l'ipotesi in cui il trattamento sia effettuato da un'organizzazione aderente allo scudo che agisce come procuratore per conto del titolare del trattamento dell'UE.

(26) Secondo il *principio su ricorso, controllo e responsabilità* ([25]), l'organizzazione aderente allo scudo deve mettere a disposizione meccanismi solidi volti a garantire il rispetto dei principi e la possibilità di ricorso per l'interessato dell'UE i cui dati personali sono stati trattati in modo non conforme, compresi mezzi di ricorso efficaci. Una volta che ha volontariamente deciso di autocertificarsi ([26]) nell'ambito dello scudo, l'organizzazione è obbligata a rispettarne effettivamente i principi. Per poter continuare a fruire dello scudo per ricevere i dati personali dall'Unione, l'organizzazione deve ricertificare ogni anno l'adesione al regime. Deve inoltre verificare ([27]) che la politica della privacy pubblicata sia conforme ai principi e applicata effettivamente. La verifica può configurarsi come autovalutazione, nel cui sistema devono essere comprese procedure interne atte a assicurare che i dipendenti ricevano una formazione sull'attuazione della politica della privacy dell'organizzazione e che la conformità sia controllata periodicamente con metodo obiettivo, oppure come verifica esterna della compatibilità, nel cui sistema possono rientrare verifiche o controlli a campione. L'organizzazione deve inoltre predisporre un meccanismo di ricorso efficace per i casi di reclamo (al riguardo cfr. anche il considerando 43) e dev'essere sottoposta all'autorità d'indagine e di controllo dell'FTC, del Dipartimento dei Trasporti o di altro ente competente per legge autorizzato negli USA che assicuri effettivamente la conformità ai principi.

(27) Al cosiddetto «ulteriore trasferimento», vale a dire il trasferimento dei dati personali da un'organizzazione a un terzo titolare del trattamento o responsabile del trattamento, si applicano norme particolari, a prescindere dal fatto che il terzo sia ubicato negli Stati Uniti o in un paese terzo rispetto agli Stati Uniti (e all'Unione). Dette norme intendono provvedere a che le tutele garantite ai dati personali degli interessati dell'UE non siano compromesse e non possano essere eluse attraverso l'inoltro dei dati a terzi. Si tratta di un aspetto particolarmente importante nelle catene di trattamento più complesse che contraddistinguono oggi l'economia digitale.

(28) Secondo il *principio sulla responsabilità in caso di ulteriore trasferimento* ([28]), questo è possibile soltanto i) per finalità determinate e limitate, ii) in base a un contratto (o analogo accordo all'interno di un gruppo societario ([29])) e iii) solo se il contratto prevede lo stesso livello di protezione garantito dai principi, compresa la condizione che permette di limitare l'applicazione dei principi soltanto se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico ([30]). Detto principio andrebbe letto in combinazione con il *principio sull'informativa* e, in caso di ulteriore trasferimento a un terzo titolare del trattamento ([31]), con il *principio sulla scelta*, secondo cui l'interessato dev'essere informato (tra l'altro) del tipo/identità di qualsiasi terzo destinatario dei dati, dello scopo dell'ulteriore trasferimento e della scelta offerta, e può opporsi all'ulteriore trasferimento (facoltà di rifiuto) o, in caso di dati sensibili, deve necessariamente dare il «consenso esplicito» allo stesso (facoltà di accettazione). Alla luce del *principio sull'integrità dei dati e la limitazione della finalità*, l'obbligo di fornire lo stesso livello di protezione garantito dai principi presuppone che il terzo possa trattare le informazioni personali trasmessegli soltanto per scopi non incompatibili con le finalità per le quali erano state raccolte in origine o con quelle successivamente autorizzate dall'interessato.

(29) L'obbligo di offrire lo stesso livello di protezione previsto dai principi si applica a ciascuno e a tutti i terzi che intervengono nel trattamento dei dati così trasferiti, ovunque siano ubicati (negli Stati Uniti o in altro paese terzo), così come si applica quando il primo terzo destinatario trasferisce a sua volta i dati ad altro terzo destinatario, cui ad esempio delega il trattamento. In tutti i casi il contratto con il terzo destinatario deve prevedere che questi informi l'organizzazione aderente allo scudo se constata di non poter più assolvere quest'obbligo. A seguito della constatazione in tal senso, il terzo cessa il trattamento oppure adotta altra misura

([25]) Cfr. anche il principio supplementare sulla composizione delle controversie e il controllo dell'applicazione (allegato II, punto III.11).
([26]) Cfr. anche il principio supplementare sull'autocertificazione (allegato II, punto III.6).
([27]) Cfr. anche il principio supplementare sulla verifica (allegato II, punto III.7).
([28]) Cfr. anche principio supplementare sui contratti obbligatori per l'ulteriore trasferimento (allegato II, punto III.10).
([29]) Cfr. anche principio supplementare sui contratti obbligatori per l'ulteriore trasferimento (allegato II, punto III.10.b). Sebbene questo principio ammetta anche il trasferimento basato su strumenti extracontrattuali (ad esempio, programmi infragruppo di conformità e controllo), il testo precisa che tali strumenti devono sempre «garant[ire] la continuità della protezione delle informazioni personali prevista dai principi». Inoltre, poiché rimane responsabile della conformità ai principi, l'organizzazione statunitense autocertificatasi come aderente è fortemente incentivata a impiegare strumenti dalla sicura efficacia pratica.
([30]) Cfr. allegato II, punto I.5.
([31]) L'interessato non gode della facoltà di rifiuto quando i dati personali sono trasmessi ad un terzo che agisce in qualità di procuratore per eseguire compiti a nome dell'organizzazione statunitense ed obbedendo ad istruzioni da essa ricevute. Questo implica tuttavia un contratto con il procuratore, e l'organizzazione statunitense è responsabile di garantire, tramite l'esercizio del potere di impartire istruzioni, l'applicazione delle tutele previste dai principi.

ragionevole e adeguata per rimediare alla situazione ([32]). Se si verificano problemi di conformità nella catena del trattamento (deleghe comprese), come indicato nel *principio su ricorso, controllo e responsabilità* l'organizzazione aderente allo scudo che agisce in qualità di titolare del trattamento dei dati personali deve dimostrare la sua estraneità all'evento che ha causato il danno; in caso contrario, incorre nella responsabilità dell'accaduto. In caso di ulteriore trasferimento a un terzo procuratore si applicano tutele supplementari ([33]).

2.2. *Trasparenza, gestione e vigilanza sullo scudo UE-USA per la privacy*

(30) Lo scudo prevede meccanismi di vigilanza e di controllo dell'attuazione atti a verificare e garantire che le imprese statunitensi autocertificatesi come aderenti al regime rispettino i principi e che qualsiasi caso di inosservanza sia affrontato. Tali meccanismi sono illustrati nei principi (allegato II) e negli impegni assunti dal Dipartimento del Commercio (allegato I), dall'FTC (allegato IV) e dal Dipartimento dei Trasporti (allegato V).

(31) Ai fini di una corretta applicazione del regime dello scudo, le parti che intervengono in tale ambito, quali gli interessati, gli esportatori di dati e le autorità nazionali di protezione dei dati, devono essere in grado di riconoscere le organizzazioni che aderiscono ai principi. A tal fine il Dipartimento del Commercio si è impegnato a tenere e mettere a disposizione del pubblico un elenco delle organizzazioni che si sono autocertificate come aderenti ai principi e che rientrano nella sfera di competenza di almeno una delle autorità di applicazione della legge di cui agli allegati I e II della presente decisione («elenco degli aderenti allo scudo» o «elenco») ([34]). Il Dipartimento del Commercio aggiorna l'elenco in funzione delle domande annuali di ricertificazione presentate dalle organizzazioni e degli eventuali ritiri o esclusioni di organizzazioni dal regime dello scudo. Tiene e mette a disposizione del pubblico anche un elenco ufficiale delle organizzazioni depennate dall'elenco, indicando per ciascuna il motivo dell'esclusione. Fornisce infine un collegamento ipertestuale all'elenco dei casi di applicazione della legge inerenti allo scudo avviati dall'FTC e caricati sul relativo sito web.

(32) Il Dipartimento del Commercio mette a disposizione del pubblico, su un apposito sito web, sia l'elenco degli aderenti allo scudo sia le domande di ricertificazione. Dal canto loro, le organizzazioni devono indicare l'indirizzo web del Dipartimento in cui è reperibile l'elenco degli aderenti allo scudo. Inoltre, se consultabile in rete, la politica della privacy dell'organizzazione deve contenere un collegamento ipertestuale al sito web dedicato allo scudo e un collegamento ipertestuale al sito web, o al modulo di presentazione del reclamo, del meccanismo di ricorso indipendente disponibile per l'istruzione dei casi irrisolti di reclamo. Nel contesto dalla certificazione e ricertificazione delle organizzazioni ai fini dello scudo, il Dipartimento del Commercio verifica sistematicamente che la politica della privacy applicata dall'organizzazione sia conforme ai principi.

(33) Il Dipartimento depenna dall'elenco degli aderenti allo scudo l'organizzazione che ha commesso reiterate inosservanze dei principi, la quale deve restituire o cancellare i dati personali ricevuti nell'ambito del regime. Negli altri casi di esclusione dall'elenco, quali il ritiro volontario dallo scudo o la mancata ricertificazione, l'organizzazione può conservare tali dati se conferma ogni anno al Dipartimento l'impegno di continuare ad applicare loro i principi oppure di proteggerli adeguatamente con altro mezzo autorizzato (ad esempio, un contratto che rispecchi totalmente le condizioni delle pertinenti clausole contrattuali tipo approvate dalla Commissione); in tal caso, l'organizzazione deve indicare al suo interno un referente per tutte le questioni relative allo scudo.

(34) Il Dipartimento del Commercio controlla le organizzazioni che, essendosi ritirate volontariamente o non avendo rinnovato la certificazione, non sono più membri dello scudo, per verificare se intendano restituire, cancellare o conservare ([35]) i dati personali ricevuti in precedenza nell'ambito del regime. Se conserva i dati, l'organizzazione

([32]) La situazione è diversa a seconda che il terzo sia titolare del trattamento o responsabile del trattamento (procuratore). Nella prima ipotesi, il contratto concluso con il terzo deve prevedere che questi cessi il trattamento oppure adotti altra misura ragionevole e adeguata per rimediare alla situazione. Nella seconda ipotesi, spetta all'organizzazione intervenire in questo senso, perché è lei il titolare del trattamento in base alle cui istruzioni opera il procuratore.

([33]) In tal caso l'organizzazione statunitense deve inoltre adottare provvedimenti ragionevoli e adeguati i) per garantire che, in concreto, il procuratore tratti le informazioni personali che gli sono trasmesse in modo conforme agli obblighi cui i principi vincolano l'organizzazione, e ii) non appena avvertita, per far cessare il trattamento non autorizzato e porvi rimedio.

([34]) Gli allegati I e II riportano informazioni sulle modalità di gestione dell'elenco degli aderenti allo scudo (punto I.3, punto I.4, III.6.d, e punto III.11.g).

([35]) Cfr., ad esempio, allegato II, punto I.3, punto III.6.f. e punto III.11.g.i.

è tenuta a continuare ad applicare loro i principi. Se ha escluso l'organizzazione dal regime per reiterate inosservanze dei principi, il Dipartimento del Commercio provvede a che essa restituisca o cancelli i dati personali ricevuti nell'ambito del regime.

(35) L'organizzazione che, per qualsiasi motivo, abbandona lo scudo deve eliminare tutte le dichiarazioni pubbliche che lasciano intendere che continui a aderirvi o a godere dei relativi benefici, in particolare i riferimenti allo scudo contenuti nella politica della privacy pubblicata. Il Dipartimento del Commercio reperisce i casi di millantata adesione allo scudo, compresi quelli che implicano ex membri, e li risolve ([36]). Se millanta pubblicamente l'adesione ai principi con dichiarazioni o pratiche fuorvianti, l'organizzazione si espone alle azioni coercitive dell'FTC, del Dipartimento dei Trasporti o di altra competente autorità di applicazione della legge degli USA; l'adesione millantata nei confronti del Dipartimento del Commercio è perseguibile in forza della legge sulle false dichiarazioni (Codice degli Stati Uniti d'America, titolo 18, articolo 1001) ([37]).

(36) Il Dipartimento del Commercio controlla ufficialmente i casi di millantata adesione allo scudo e di uso improprio del relativo marchio di certificazione e le autorità di protezione dei dati possono chiedere al referente per lo scudo istituito presso tale Dipartimento di esaminare la situazione di un'organizzazione. Quando l'organizzazione si è ritirata dal regime, non ha ricertificato l'adesione ai relativi principi o è stata depennata dall'elenco degli aderenti allo scudo, il Dipartimento del Commercio verifica su base continuativa che abbia eliminato, dalla politica sulla privacy pubblicata, qualsiasi riferimento allo scudo che lasci intendere che continua ad aderirvi e, se l'organizzazione continua a millantare l'adesione al regime, sottopone il caso all'FTC, al Dipartimento dei Trasporti o ad altra autorità competente per le azioni coercitive del caso. Invia altresì questionari alle organizzazioni la cui autocertificazione è in scadenza o che si sono ritirate volontariamente dallo scudo per verificare se l'organizzazione intenda restituire o cancellare i dati personali ricevuti quando aderiva al regime ovvero continuare ad applicare loro i principi dello scudo e, se i dati personali sono conservati, per verificare chi, all'interno dell'organizzazione, funge da referente permanente per le questioni relative allo scudo.

(37) Il Dipartimento del Commercio effettua su base continuativa controlli ufficiali della conformità ([38]) delle organizzazioni che si sono autocertificate, anche tramite l'invio di questionari particolareggiati. Procede sistematicamente a controlli anche ogni volta che riceve reclami specifici (e non futili), che l'organizzazione non risponde esaurientemente alle sue richieste oppure che prove credibili indicano la possibilità che l'organizzazione disattenda i principi. Se del caso, per tali controlli della conformità il Dipartimento del Commercio consulta anche le autorità di protezione dei dati.

2.3. *Meccanismi di ricorso, trattamento dei reclami e applicazione*

(38) Con il *principio su ricorso, controllo e responsabilità* lo scudo impone all'organizzazione aderente di mettere mezzi di ricorso a disposizione della persona lesa dall'inosservanza, offrendo quindi all'interessato dell'UE la possibilità di sporgere reclamo per mancato rispetto dei principi da parte di un'organizzazione statunitense che si è autocertificata, e di ottenere la soluzione del caso di reclamo, se necessario con una decisione che dispone un rimedio effettivo.

(39) Nell'ambito dell'autocertificazione l'organizzazione deve adempiere gli obblighi imposti dal principio su ricorso, controllo e responsabilità prevedendo meccanismi di ricorso indipendenti effettivi e di pronto impiego, atti a consentire d'istruire e dirimere, senza costi per la persona, qualsiasi reclamo da questa presentato o qualsiasi controversia insorta.

(40) L'organizzazione può scegliere meccanismi di ricorso indipendenti dell'Unione o degli Stati Uniti, compresa la possibilità di impegnarsi volontariamente a collaborare con le autorità di protezione dei dati dell'UE. Quest'ultima opzione non è tuttavia disponibile per l'organizzazione che tratta dati sulle risorse umane, perché in tal caso la

([36]) Cfr. allegato I, parte «Reperimento dei casi di millantata adesione e loro soluzione».
([37]) Cfr. allegato II, parte III.6.h. e parte III.11.f.
([38]) Cfr. allegato I.

collaborazione con le autorità di protezione dei dati è obbligatoria. Fra le altre opzioni disponibili si annoverano gli organi alternativi indipendenti di composizione delle controversie (ADR) o i *programmi per la privacy* elaborati dal settore privato nei quali sono integrati i principi dello scudo. Questi ultimi devono contemplare meccanismi di attuazione efficaci rispondenti ai requisiti indicati nel principio su ricorso, controllo e responsabilità. L'organizzazione è tenuta a sanare qualsiasi problema di non conformità. Deve altresì indicare di essere sottoposta all'autorità d'indagine e di controllo dell'FTC, del Dipartimento dei Trasporti o di altro ente competente per legge autorizzato negli USA.

(41) Lo scudo offre quindi all'interessato varie possibilità di far valere i propri diritti, di sporgere reclamo per inosservanza dei principi da parte di imprese statunitensi autocertificatesi e di ottenere la soluzione del caso di reclamo, se necessario con una decisione che dispone un rimedio effettivo. La persona può sporgere reclamo direttamente all'organizzazione, a un organo indipendente di risoluzione delle controversie da questa designato, all'autorità nazionale di protezione dei dati oppure all'FTC.

(42) Nei casi in cui nessuno di detti meccanismi di ricorso o di attuazione abbia risolto il caso di reclamo, la persona ha altresì il diritto di chiedere un arbitrato vincolante nel quadro del collegio arbitrale dello scudo (allegato 1 dell'allegato II della presente decisione). Fatta eccezione per il collegio arbitrale, cui si può rivolgere solo dopo aver esperito determinati mezzi di contestazione, la persona è libera di scegliere il meccanismo di ricorso che preferisce o di attivarli tutti, senza alcun obbligo di rivolgersi a uno piuttosto che a un altro o di seguire una determinata sequenza. È tuttavia consigliabile procedere secondo l'ordine logico esposto qui di seguito.

(43) In primo luogo, l'interessato nell'UE può sottoporre il caso di inosservanza dei principi direttamente all'*impresa statunitense che si è autocertificata come aderente allo scudo*. Per agevolare la soluzione dei casi, l'organizzazione deve predisporre un meccanismo di ricorso effettivo atto a trattare tali reclami. L'organizzazione deve quindi indicare chiaramente alle persone, nella politica della privacy, un referente, interno o esterno, incaricato del trattamento dei reclami (che può essere anche uno stabilimento presente nell'Unione in grado di rispondere alle domande o ai reclami) e informarle sui meccanismi indipendenti di trattamento dei reclami.

(44) Ricevuto il reclamo della persona, direttamente da questa o per il tramite del Dipartimento del Commercio cui l'ha sottoposto un'autorità di protezione dei dati, l'organizzazione deve rispondere all'interessato dell'UE entro il termine di 45 giorni. La risposta deve comprendere una valutazione di merito del reclamo e informazioni sul modo in cui l'organizzazione intende porre rimedio al problema. L'organizzazione è parimenti tenuta a rispondere prontamente alle richieste d'informazioni o di altro tipo riguardo all'osservanza dei principi, emananti dal Dipartimento del Commercio o da un'autorità di protezione dei dati ([39]) (se l'organizzazione si è impegnata a collaborare con tali autorità). L'organizzazione deve tenere traccia dell'attuazione della politica della privacy e, nell'ambito delle indagini o dei reclami per inosservanza dei principi, mettere le relative registrazioni, su richiesta, a disposizione del meccanismo di ricorso indipendente o dell'FTC (o di altra autorità statunitense competente delle indagini sulle pratiche sleali e ingannevoli).

(45) In secondo luogo, la persona può anche sporgere reclamo direttamente all'*organo indipendente di composizione delle controversie* (negli Stati Uniti o nell'Unione) che l'organizzazione ha designato per esaminare e risolvere i casi di reclamo individuale (a condizione che il reclamo non sia manifestamente infondato o futile) e per mettere a disposizione della persona, gratuitamente, un mezzo di ricorso adeguato. Le sanzioni e misure correttive imposte da tale organo devono essere sufficientemente severe da assicurare che l'organizzazione rispetti i principi e dovrebbero imporle di correggere o sovvertire gli effetti dell'inosservanza e, a seconda delle circostanze, di astenersi da ulteriori trattamenti dei dati personali in questione e/o di cancellarli, nonché di dare pubblicità all'inosservanza constatata. L'organo indipendente di composizione delle controversie designato da un'organizzazione è tenuto a riportare sul proprio sito web pubblico le pertinenti informazioni relative allo scudo e ai servizi che presta in tale ambito. Deve pubblicare ogni anno una relazione che presenti, in forma aggregata, i dati statistici relativi ai servizi prestati ([40]).

([39]) Si tratta dell'autorità di trattamento del caso designata dal comitato delle autorità di protezione dei dati di cui al principio supplementare «Ruolo delle autorità di protezione dei dati» (allegato II, punto III.5).

([40]) La relazione annuale deve indicare: 1) il numero complessivo dei reclami in virtù dello scudo ricevuti nell'anno di riferimento; 2) il tipo di reclami ricevuti; 3) gli elementi qualitativi collegati alla composizione delle controversie, ad esempio il tempo di trattamento dei reclami; 4) l'esito dei reclami ricevuti, in particolare il numero e il tipo delle riparazioni o delle sanzioni decretate.

(46) Le procedure di controllo della conformità seguite dal Dipartimento del Commercio prevedono la verifica del fatto che le imprese statunitensi autocertificatesi siano effettivamente registrate presso i meccanismi di ricorso indipendenti a cui dichiarano di essere registrate. Sia le organizzazioni sia i competenti meccanismi di ricorso indipendenti sono tenuti a rispondere prontamente alle richieste del Dipartimento del Commercio vertenti su informazioni relative allo scudo.

(47) Se l'organizzazione non si conforma alla decisione dell'organo di risoluzione delle controversie o dell'organo di autoregolamentazione, questo deve notificarlo al Dipartimento del Commercio e all'FTC (o a altra autorità statunitense competente delle indagini sulle pratiche sleali e ingannevoli) ovvero al giudice competente ([41]). Quando l'organizzazione rifiuta di uniformarsi alla decisione definitiva dell'ente pubblico, dell'organo di autoregolamentazione o dell'organo indipendente di composizione delle controversie competenti della privacy, ovvero quando tale ente o organo constata che l'organizzazione viola i principi frequentemente, si configura la fattispecie dell'inosservanza reiterata, con la conseguenza che il Dipartimento del Commercio, concessi all'organizzazione inadempiente un preavviso di 30 giorni e la possibilità di replica, depenna l'organizzazione dall'elenco ([42]). Se l'organizzazione depennata dall'elenco continua a millantare la certificazione allo scudo, il Dipartimento la deferisce all'FTC o altra autorità di applicazione della legge ([43]).

(48) In terzo luogo, la persona può altresì sporgere reclamo a un'*autorità di protezione dei dati* nazionale. L'organizzazione è tenuta a collaborare con l'autorità di protezione dei dati per l'esame e la risoluzione del caso di reclamo,se questo riguarda il trattamento di dati sulle risorse umane raccolti nel contesto di un rapporto di lavoro oppure se l'organizzazione ha accettato volontariamente di essere sottoposta alla supervisione delle autorità di protezione dei dati. In particolare, l'organizzazione è tenuta a rispondere alle richieste d'informazioni dell'autorità di protezione dei dati, a uniformarsi al parere da questa espresso, anche relativamente alle misure correttive o compensative, e a confermarle per iscritto l'adozione dei provvedimenti richiesti.

(49) Le autorità di protezione dei dati esprimono i pareri per il tramite di un comitato informale che le raggruppa, istituito a livello europeo ([44]), in modo da contribuire ad assicurare una linea armonizzata e coerente nel trattamento di un dato reclamo. Il parere è espresso dopo che le due parti delle controversia hanno avuto ragionevoli possibilità di formulare commenti e addurre qualsiasi elemento di prova desiderino. Il comitato esprime il parere quanto più rapidamente possibile, compatibilmente con l'esigenza di garantire l'equità del procedimento, e di norma entro un termine di 60 giorni dalla data in cui riceve il reclamo. Se l'organizzazione non si adegua al parere entro 25 giorni dalla data in cui è espresso senza fornire soddisfacenti giustificazioni del ritardo, il comitato le notifica l'intenzione di sottoporre il caso all'FTC (o ad altra autorità statunitense di applicazione della legge) ovvero di concludere che si è verificato un grave inadempimento dell'impegno a collaborare. Nel primo caso, la conseguenza può essere un'azione coercitiva ai sensi dell'articolo 5 della legge sull'FTC (o legge analoga). Nel secondo caso il comitato informa il Dipartimento del Commercio, il quale assimila il rifiuto dell'organizzazione di adeguarsi al parere del comitato delle autorità di protezione dei dati a una reiterata inosservanza che comporta il depennamento dell'organizzazione dall'elenco degli aderenti allo scudo.

(50) Se l'autorità di protezione dei dati cui è stato inviato il reclamo non è intervenuta, o non a sufficienza, per risolvere il caso, la persona può contestare l'intervento (o l'inazione) dinanzi al giudice nazionale del proprio Stato membro.

(51) La persona può sporgere reclamo all'autorità di protezione dei dati anche se l'organizzazione non ha designato il relativo comitato come organo di composizione delle controversie. In tal caso l'autorità di protezione dei dati può sottoporre il reclamo al Dipartimento del Commercio o all'FTC. Per favorire e intensificare la collaborazione sulle questioni relative ai reclami individuali e all'inosservanza da parte delle organizzazioni aderenti allo scudo, il Dipartimento del Commercio nomina al suo interno un referente incaricato dei collegamenti con le autorità di protezione dei dati e dell'assistenza alle stesse per le richieste vertenti sulla conformità delle organizzazioni ai principi dello scudo ([45]). Anche l'FTC si è impegnata a istituire un apposito referente ([46]) e a prestare alle autorità di protezione dei dati assistenza nelle attività d'indagine a norma della legge sull'Internet sicura negli USA (SAFE WEB) ([47]).

([41]) Cfr. allegato II, punto III.11.e.
([42]) Cfr. allegato II, punto III.11.g, in particolare i punti ii) e iii).
([43]) Cfr. allegato I, parte «Reperimento dei casi di millantata adesione e loro soluzione».
([44]) In considerazione della loro competenza a organizzare la propria attività e a operare in reciproca collaborazione, le autorità di protezione dei dati dovrebbero adottare il regolamento interno del comitato informale.
([45]) Cfr. allegato I, parti «Maggiore collaborazione con le autorità di protezione dei dati» e «Agevolazione della risoluzione dei casi di reclamo per inosservanza dei principi», e allegato II, punto II.7.e.
([46]) Cfr. allegato IV, pag. 6.
([47]) *ibid*.

(52) In quarto luogo, il *Dipartimento del Commercio* si è impegnato a ricevere i reclami vertenti sull'inosservanza dei principi da parte di un'organizzazione, a esaminarli e a adoperarsi al massimo per risolvere i casi. A tal fine prevede procedure particolari che permettono alle autorità di protezione dei dati di sottoporre il reclamo a un apposito referente, di seguirne l'iter e di darvi seguito presso le imprese per facilitare la soluzione del caso. Per accelerare il trattamento di ciascun reclamo, il referente affronta il caso di inosservanza in contatto diretto con la pertinente autorità di protezione dei dati e provvede, in particolare, ad aggiornarla sulla situazione entro un termine massimo di 90 giorni dalla data in cui gli è stato sottoposto il reclamo. Questo *modus operandi* permette all'interessato di sporgere reclamo per inosservanza dei principi da parte dell'impresa statunitense autocertificatasi direttamente alla pertinente autorità nazionale di protezione dei dati, che provvede poi a inoltrarla al Dipartimento del Commercio in quanto autorità di gestione dello scudo negli Stati Uniti d'America. Il Dipartimento del Commercio si è impegnato inoltre a indicare, nel quadro dell'esame annuale del funzionamento dello scudo, un'analisi in forma aggregata dei reclami ricevuti ogni anno ([48]).

(53) Se le verifiche eseguite d'ufficio annuali, i reclami o qualsiasi altra informazione portano a concludere che l'organizzazione abbia commesso reiterate inosservanze dei principi, il Dipartimento del Commercio la depenna dall'elenco degli aderenti allo scudo. Il rifiuto di uniformarsi alla decisione definitiva dell'ente pubblico, dell'organo di autoregolamentazione o dell'organo indipendente di composizione delle controversie competenti della privacy, autorità di protezione dei dati comprese, si configura come inosservanza reiterata.

(54) In quinto luogo, l'organizzazione aderente allo scudo dev'essere sottoposta all'autorità d'indagine e di controllo delle autorità statunitensi, in particolare della *Commissione federale del Commercio* ([49]), che assicura di fatto il rispetto dei principi. La FTC tratta in via prioritaria i casi d'inosservanza dei principi ad essa sottoposti da un organo indipendente di composizione delle controversie o di autoregolamentazione, dal Dipartimento del Commercio e dalle autorità di protezione dei dati (di loro iniziativa o a seguito di reclamo) per stabilire se vi sia stata violazione dell'articolo 5 della legge sull'FTC ([50]). L'FTC si è impegnata a predisporre una procedura standard per i casi che le sono sottoposti, a istituire al suo interno un referente per i casi sottoposti dalle autorità di protezione dei dati e a scambiare informazioni sui casi sottopostile. Accetta inoltre i reclami presentati direttamente dalle persone e avvia di propria iniziativa indagini nell'ambito dello scudo, in particolare nel quadro delle più ampie indagini in materia di tutela della vita privata.

(55) L'FTC può imporre il rispetto dei principi mediante un provvedimento amministrativo («ordinanza consensuale») di cui controlla sistematicamente l'esecuzione. Se l'organizzazione non si conforma al provvedimento, l'FTC ha facoltà di adire il giudice competente al fine di ottenere sanzioni civili e altre riparazioni, anche per l'eventuale danno causato dal comportamento illecito. In alternativa, può adire direttamente il giudice federale per ottenere un'ingiunzione preliminare o permanente ovvero altra misura correttiva. Ciascuna ordinanza consensuale emanata nei confronti di un'organizzazione aderente allo scudo prevede obblighi di informazione da parte dell'organizzazione ([51]), cui è imposto di rendere pubbliche le parti inerenti allo scudo delle relazioni di conformità o di valutazione presentate all'FTC. Infine, l'FTC tiene online un elenco delle imprese nei cui confronti è stata emanata un'ordinanza dell'FTC stessa o del giudice in casi collegati allo scudo.

(56) In sesto luogo, l'interessato dell'UE può chiedere l'arbitrato vincolante del *collegio arbitrale dello scudo* come extrema ratio nel caso in cui gli altri mezzi di ricorso disponibili non gli abbiano offerto una soluzione soddisfacente per il reclamo sporto. L'organizzazione deve informare la persona della possibilità di chiedere, a determinate condizioni, un arbitrato vincolante; una volta che la possibilità si concreta con l'invio dell'avviso all'organizzazione, questa è tenuta a darvi riscontro ([52]).

([48]) Cfr. allegato I, parte «Agevolazione della risoluzione dei casi di reclamo per inosservanza dei principi».

([49]) L'organizzazione aderente allo scudo deve impegnarsi pubblicamente a rispettare i principi, deve rendere pubbliche le politiche della privacy applicate conformemente ai principi e deve attuarle integralmente. L'inosservanza è perseguibile a norma dell'articolo 5 della legge sull'FTC, che proibisce gli atti sleali e ingannevoli nel commercio o aventi ripercussioni sul commercio.

([50]) Secondo le informazioni comunicate dalla stessa FTC, questa non ha il potere di effettuare ispezioni in loco nel settore della tutela della vita privata. Ha tuttavia il potere di obbligare l'organizzazione a comunicare documenti e a fornire testimonianze (cfr. articolo 20 della legge sull'FTC) e, se l'organizzazione non si conforma al suo provvedimento in tal senso, può chiederne l'esecuzione al giudice.

([51]) L'ordinanza dell'FTC o del giudice può obbligare l'impresa a attuare un programma in materia di privacy e a trasmettere periodicamente all'FTC relazioni di conformità o valutazioni effettuate da terzi indipendenti in relazione a tale programma.

([52]) Cfr. allegato II, parte II.1.xi e III.7.c.

(57) Il collegio arbitrale è composto da un gruppo di almeno 20 arbitri scelti dal Dipartimento del Commercio e dalla Commissione sulla base dell'indipendenza, dell'integrità e delle competenze in materia di diritto della privacy statunitense e di normativa dell'UE sulla protezione dei dati. Per ogni controversia le parti attingono al gruppo per selezionare un collegio di uno o di tre arbitri ([53]). La procedura è regolata da regole arbitrali standard stabilite di comune accordo da Dipartimento del Commercio e Commissione. Tali regole integrano il regime già concordato, il quale presenta vari aspetti che rendono più accessibile questo meccanismo per gli interessati dell'UE: i) l'interessato può essere assistito dalla propria autorità nazionale di protezione dei dati per la preparazione del caso da sottoporre al collegio; ii) l'arbitrato si svolge negli Stati Uniti, ma l'interessato dell'UE può optare per la partecipazione in video o via telefono, che gli è fornita gratuitamente; iii) di norma il procedimento arbitrale si svolge in lingua inglese, ma su richiesta motivata all'interessato sono di regola ([54]) fornite, gratuitamente, l'interpretazione nell'udienza arbitrale e la traduzione; iv) sebbene ciascuna parte, se rappresentata dinanzi al collegio da un avvocato, debba sopportare le proprie spese di assistenza legale, il Dipartimento del Commercio costituisce un fondo cui ciascuna organizzazione aderente allo scudo versa una quota annua a copertura dei costi ammissibili della procedura arbitrale; l'entità della quota è limitata a massimali stabiliti dalle autorità statunitensi in consultazione con la Commissione europea.

(58) Il collegio arbitrale dello scudo ha il potere di imporre il necessario «provvedimento equo, specifico alla persona e di carattere non pecuniario» ([55]) a titolo di riparazione per la violazione dei principi. Benché il collegio, nel trarre le conclusioni, tenga conto delle altre riparazioni già ottenute mediante altri meccanismi dello scudo, la persona può comunque ricorrere all'arbitrato se le reputa insufficienti. Questo permette all'interessato dell'UE di chiedere l'arbitrato in tutti i casi in cui l'intervento (o l'inazione) delle competenti autorità statunitensi (ad esempio l'FTC) non abbia offerto una soluzione soddisfacente per il suo reclamo. L'arbitrato non può essere chiesto se un'autorità di protezione dei dati ha autorità di legge per risolvere il caso di reclamo nei confronti di un'impresa statunitense autocertificatasi, ossia quando l'organizzazione è tenuta a collaborare con tale autorità e a conformarsi ai pareri da essa espressi relativamente al trattamento dei dati sulle risorse umane raccolti nel contesto di un rapporto di lavoro oppure quando si sia impegnata volontariamente in tal senso. A norma della legge federale sull'arbitrato, la persona può far valere la decisione arbitrale dinanzi al giudice statunitense nei casi in cui l'impresa non si conforma alla decisione arbitrale.

(59) In settimo luogo, se l'organizzazione viene meno all'impegno di rispettare i principi e la politica della privacy pubblicata, possono risultare percorribili altre vie di ricorso in sede giudiziaria previste da disposizioni normative degli USA, nell'ambito del diritto del risarcimento per fatto illecito e in caso di millanteria fraudolenta, atti o pratiche sleali o ingannevoli o violazione del contratto.

(60) Inoltre, anche l'autorità di protezione dei dati che, ricevuto il reclamo di un interessato dell'UE, ritiene che i dati personali che lo riguardano siano stati trasferiti ad un'organizzazione negli Stati Uniti in violazione del diritto dell'UE in materia di protezione dei dati, compreso il caso in cui l'esportatore dei dati dell'UE ha motivo di ritenere che l'organizzazione non osservi i principi, può esercitare i propri poteri nei confronti dell'esportatore dei dati e, se necessario, disporre la sospensione del trasferimento.

(61) Alla luce delle informazioni riportate nella presente sezione, la Commissione ritiene che i principi emanati dal Dipartimento del Commercio degli Stati Uniti assicurino di per sé un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito dai principi sostanziali fondamentali stabiliti nella direttiva 95/46/CE.

(62) L'effettiva applicazione dei principi è parimenti garantita sia dagli obblighi di trasparenza sia dalla gestione e dal controllo della conformità allo scudo effettuati dal Dipartimento del Commercio.

(63) La Commissione ritiene che, nel complesso, i meccanismi di vigilanza, di ricorso e di applicazione previsti dallo scudo permettano di individuare e punire nella pratica le violazioni dei principi commesse dalle organizzazioni aderenti al regime e offrano all'interessato mezzi di ricorso che gli permettono di accedere ai dati personali che lo riguardano e, in ultima analisi, di ottenerne la rettifica o cancellazione.

([53]) Il numero di arbitri nel collegio dev'essere concordato tra le parti.

([54]) Il collegio può tuttavia stabilire che, nella situazione specifica di un dato procedimento arbitrale, la copertura di queste spese comporterebbe costi ingiustificati o sproporzionati.

([55]) La persona non può chiedere il risarcimento dei danni in sede arbitrale; tuttavia, chiedere l'arbitrato non preclude la possibilità di chiedere il risarcimento dei danni al giudice ordinario statunitense.

3. ACCESSO E USO DA PARTE DELLE AUTORITÀ PUBBLICHE STATUNITENSI DEI DATI PERSONALI TRASFERITI NELL'AMBITO DELLO SCUDO

(64) Come enunciato nell'allegato II, punto I.5, il rispetto dei principi trova il suo limite se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia.

(65) La Commissione ha valutato le limitazioni e le garanzie cui la normativa statunitense subordina la facoltà delle autorità pubbliche statunitensi di accedere e usare i dati personali trasferiti nell'ambito dello scudo per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico. Il governo statunitense ha altresì comunicato alla Commissione, tramite l'Ufficio del direttore dell'intelligence nazionale (ODNI) ([56]), le dichiarazioni e gli impegni particolareggiati riportati nell'allegato VI della presente decisione. Con lettera firmata dal segretario di Stato, acclusa alla presente decisione come allegato III, il governo degli Stati Uniti si è impegnato altresì a creare un nuovo meccanismo di vigilanza sulle ingerenze per motivi di sicurezza nazionale, indipendente dai servizi di intelligence: il Mediatore dello scudo. Infine, la dichiarazione del Dipartimento della Giustizia degli USA, riportata nell'allegato VII della presente decisione, espone le garanzie e limitazioni relative all'accesso delle autorità pubbliche ai dati per finalità di contrasto e di interesse pubblico. Ai fini della trasparenza e per rispecchiare la natura giuridica di questi impegni, ciascuno dei documenti elencati e allegati alla presente decisione è pubblicato nel Registro federale degli USA.

(66) Le conclusioni cui è giunta la Commissione riguardo alle limitazioni imposte alle autorità pubbliche statunitensi quanto all'accesso e all'uso dei dati personali trasferiti dall'Unione europea agli Stati Uniti e circa l'esistenza di tutele giuridiche efficaci sono esposte in maggiore dettaglio qui di seguito.

3.1. *Accesso e uso da parte delle autorità pubbliche statunitensi per motivi di sicurezza nazionale*

(67) L'analisi della Commissione evidenzia che la normativa statunitense prevede una serie di limitazioni all'accesso e all'uso per motivi di sicurezza nazionale dei dati personali trasferiti nell'ambito dello scudo, così come meccanismi di vigilanza e di ricorso, tali da costituire garanzie sufficienti che permettono di proteggere efficacemente detti dati dall'ingerenza illecita e dal rischio di abusi ([57]). Da quando la Commissione ha pubblicato le due comunicazioni nel 2013 (cfr. il considerando 7), il quadro normativo vigente è stato rafforzato in modo significativo, come descritto di seguito.

3.1.1. Limitazioni

(68) In virtù della Costituzione degli Stati Uniti, garantire la sicurezza nazionale rientra nei poteri del presidente in qualità di comandante supremo, di capo dell'esecutivo e, per quanto riguarda l'intelligence esterna, di responsabile della conduzione degli affari esteri degli Stati Uniti ([58]). Sebbene il Congresso abbia il potere d'imporre limitazioni a queste prerogative, e di fatto sia intervenuto in tal senso sotto vari aspetti, il presidente può indirizzare le attività della comunità dell'intelligence statunitense, in particolare mediante decreti o direttive presidenziali. Questo vale naturalmente anche per i settori in cui non esistono orientamenti del Congresso. Attualmente i due strumenti giuridici centrali sono il decreto presidenziale 12333 (EO 12333) ([59]) e la direttiva presidenziale 28 (PPD-28).

([56]) Il Direttore dell'intelligence nazionale è a capo della comunità dell'intelligence e agisce in veste di consigliere principale del presidente e del Consiglio per la sicurezza nazionale (cfr. legge sulla riforma dell'intelligence e la prevenzione del terrorismo del 2004. Pub. L. 108-458 del 17.12.2004). Fra gli altri compiti l'ODNI ha quello di stabilire le esigenze dell'intelligence nazionale e di gestire e indirizzare gli incarichi, la raccolta, l'analisi, la produzione e la divulgazione dei relativi dati da parte della comunità dell'intelligence, anche attraverso l'elaborazione di orientamenti sulle modalità di accesso, uso e condivisione di tali dati. Cfr. articolo 1.3 (a), (b) del decreto presidenziale 12333.

([57]) *Schrems*, punto 91.

([58]) Costituzione degli Stati Uniti, articolo II. Cfr. anche introduzione alle PPD-28.

([59]) EO 12333: United States Intelligence Activities, Registro federale Vol. 40, n. 235 (8 dicembre 1981). Stando alla misura in cui è accessibile al pubblico, il decreto presidenziale definisce le finalità, gli indirizzi, i compiti e le responsabilità delle attività d'intelligence degli USA (compreso il ruolo dei diversi servizi della comunità dell'intelligence) e fissa i parametri generali per la condotta di tali attività (in particolare la necessità di adottare regole procedurali specifiche). A norma dell'articolo 3.2 dell'EO 12333, il presidente emana, assistito dal Consiglio per la sicurezza nazionale e dal Direttore dell'intelligence nazionale, gli orientamenti, procedure e direttive necessari per dare attuazione al decreto.

(69) La PPD-28, emanata il 17 gennaio 2014, impone una serie di limitazioni alle operazioni di «intelligence dei segnali» ([60]). La direttiva presidenziale è vincolante per le autorità di intelligence statunitensi ([61]) e resta in vigore anche quando cambia l'amministrazione degli Stati Uniti ([62]). La PPD-28, che riveste particolare importanza per i cittadini stranieri, compresi gli interessati nell'Unione europea, prevede fra l'altro quanto segue:

a) la raccolta dati nell'ambito dell'intelligence dei segnali deve basarsi sulla legge o su un'autorizzazione presidenziale e deve avvenire nel rispetto della Costituzione degli Stati Uniti (in particolare del quarto emendamento) e della legge degli Stati Uniti;

b) ognuno deve essere trattato con dignità e rispetto, a prescindere dalla cittadinanza o dal luogo di residenza;

c) ognuno ha un legittimo interesse alla tutela della propria vita privata nel quadro del trattamento delle informazioni personali che lo riguardano;

d) la tutela della vita privata e le libertà civili sono aspetti di cui tenere obbligatoriamente conto nella pianificazione delle attività di intelligence dei segnali condotte dagli USA;

e) le attività di intelligence dei segnali condotte dagli Stati Uniti devono comportare quindi adeguate garanzie per le informazioni personali di ciascuno, a prescindere dalla cittadinanza o dal luogo di residenza.

(70) A norma della PPD-28, possono essere rilevati dati dell'intelligence dei segnali solo per finalità di intelligence esterna o di controspionaggio a sostegno di missioni di sicurezza nazionale o di missioni di un dipartimento, e non per altre finalità (ad esempio, non per conferire un vantaggio concorrenziale alle imprese statunitensi). Al riguardo l'ODNI spiega che ciascun servizio della comunità dell'intelligence dovrebbe prevedere di usare, ogniqualvolta possibile, discriminanti (dispositivi specifici, selettori, identificatori ecc.) per poter concentrare la rilevazione dei dati su obiettivi o temi specifici dell'intelligence esterna ([63]). Le dichiarazioni comunicate precisano inoltre che le decisioni sulla raccolta di dati di intelligence non sono lasciate alla discrezionalità del singolo agente, ma sono prese in base alle politiche e procedure stabilite da ciascun servizio della comunità dell'intelligence statunitense in applicazione della PPD-28 ([64]). Di conseguenza, la ricerca sui selettori appropriati e la loro selezione s'iscrivono nel contesto generale del quadro delle priorità dell'intelligence nazionale (NIPF), il quale assicura che le priorità in materia di intelligence siano fissate ad alto livello politico e riesaminate periodicamente, in modo da essere sempre atte a rispondere alle minacce per la sicurezza nazionale che si pongono al momento tenuto conto dei possibili rischi, compreso per la privacy ([65]). Su questa base il personale degli enti ricerca e individua i selettori specifici che si prevede permettano di rilevare dati di intelligence esterna rispondenti alle priorità ([66]). I selettori devono essere valutati a cadenza periodica per verificare che siano sempre in grado di reperire dati d'intelligence validi rispondenti alle priorità ([67]).

([60]) A norma dell'EO 12333, il Direttore dell'Agenzia per la sicurezza nazionale (NSA) è il responsabile di funzione per l'intelligence dei segnali e, per le attività di intelligence dei segnali, dirige un'organizzazione unificata.

([61]) L'espressione «Intelligence Community» (comunità dell'intelligence) è definita all'articolo 3.5 (h) dell'EO 12333 in combinazione con il n. 1 della PPD-28.

([62]) Cfr. memorandum dell'Ufficio del Giureconsulto del Dipartimento della Giustizia al presidente Clinton, 29 gennaio 2000. Secondo questo parere giuridico, le direttive presidenziali hanno lo stesso effetto giuridico sostanziale dei decreti presidenziali.

([63]) Dichiarazioni dell'ODNI (allegato VI), pag. 3.

([64]) Cfr. articolo 4(b),(c) della PPD-28. Stando alle informazioni divulgate al pubblico, il riesame del 2015 ha confermato le sei finalità vigenti. Cfr. ODNI, Signals Intelligence Reform, 2016 Progress Report.

([65]) Dichiarazioni dell'ODNI (allegato VI), pag. 6 (in riferimento alla direttiva per la comunità dell'intelligence 204). Cfr. anche articolo 3 della PPD-28.

([66]) Dichiarazioni dell'ODNI (allegato VI), pag. 6. Cfr., ad esempio, Ufficio per la tutela della vita privata e le libertà civili dell'NSA (NSA CLPO), NSAs Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7 ottobre 2014. Cfr. ODNI Status Report 2014. Per le domande di accesso ai sensi dell'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna (FISA), le interrogazioni sono regolate dalle procedure di minimizzazione omologate dalla Corte di vigilanza sull'intelligence esterna (Corte FISA). Cfr. NSA CLPO, NSAs Implementation of Foreign Intelligence Surveillance Act Section 702, 16 aprile 2014.

([67]) Cfr. Signal Intelligence Reform, 2015 Anniversary Report. Cfr. anche dichiarazioni dell'ODNI (allegato VI), pagg. 6, 8-9 e 11.

(71) Inoltre, le condizioni previste dalla PPD-28, ossia che la rilevazione dei dati di intelligence deve sempre essere ([68])« quanto più possibile mirata» e che la comunità dell'intelligence deve privilegiare, se disponibili, altre informazioni e alternative appropriate e fattibili ([69]), rispecchiano la regola generale che impone di privilegiare la rilevazione mirata alla raccolta in blocco di dati. L'ODNI assicura in particolare che la raccolta di dati in blocco non si configura come raccolta in massa o indiscriminata e l'eccezione non fagocita la regola generale ([70]).

(72) Pur riconoscendo che, nell'ambito dell'intelligence dei segnali, talune circostanze obbligano talvolta i servizi della comunità dell'intelligence a raccogliere dati in blocco, ad esempio per poter individuare o valutare una minaccia nuova o emergente, la PPD-28 chiede a tali servizi di privilegiare le alternative che permettono di rendere mirata la raccolta dei dati in tale ambito ([71]). Ne consegue che la raccolta in blocco è effettuata solo quando, «in base a considerazioni tecniche o operative», non risulta possibile procedere alla rilevazione mirata con il filtro di discriminanti, ossia di un identificatore associato a un obiettivo specifico (quale l'indirizzo di posta elettronica dell'obiettivo o il suo numero di telefono) ([72]). Quest'obbligo vale sia per le modalità di raccolta dati nell'ambito dell'intelligence dei segnali sia per le informazioni effettivamente raccolte ([72]).

(73) Secondo le dichiarazioni dell'ODNI, anche quando non si possono usare identificatori specifici per rendere mirata la raccolta, la comunità dell'intelligence cerca di restringerla «il più possibile». A tal fine «applica filtri e altri strumenti tecnici per concentrare la raccolta sui dispositivi che presentano probabilità di contenere comunicazioni di valore nell'ambito dell'intelligence esterna» (rispondendo così ai requisiti stabiliti dai decisori politici statunitensi conformemente alla procedura illustrata al considerando 70). La raccolta di dati in blocco è quindi mirata in almeno due modi: in primo luogo, verte sempre su obiettivi specifici di intelligence esterna (ad esempio, per acquisire nell'ambito dell'intelligence dei segnali dati su un gruppo terroristico che opera in una determinata regione) e si concentra sulle comunicazioni che presentano un collegamento con tali obiettivi; al riguardo l'ODNI assicura che questo si traduce nel fatto che «le attività di intelligence dei segnali condotte dagli Stati Uniti interessano soltanto una percentuale minima delle comunicazioni che transitano su Internet» ([73]); in secondo luogo, le dichiarazioni dell'ODNI spiegano che i filtri e gli altri strumenti tecnici impiegati sono finalizzati a rendere mirata «il più precisamente possibile» la raccolta per ridurre al minimo la raccolta di «informazioni irrilevanti».

(74) Infine, anche quando gli Stati Uniti ritengono necessario raccogliere dati in blocco nell'ambito dell'intelligence dei segnali, alle condizioni indicate nei considerando 70-73, la PPD-28 limita l'uso delle informazioni così rilevate a sei finalità di sicurezza nazionale elencate specificamente, al fine di tutelare la vita privata e le libertà civili di chiunque, a prescindere dalla cittadinanza e dal luogo in cui la persona vive ([74]). Rientrano fra le finalità autorizzate le misure atte a individuare e combattere le minacce derivanti da attività di spionaggio, terrorismo,

([68]) Dichiarazioni dell'ODNI (allegato VI), pag. 3.

([69]) Si rilevi che, a norma dell'articolo 2.4 dell'EO 12333, i servizi della comunità dell'intelligence applicano le tecniche di raccolta meno intrusive praticabili negli Stati Uniti. Per quanto riguarda le limitazioni che si pongono alla sostituzione di tutte le raccolte di dati in blocco con rilevazioni mirate, cfr. il risultato di una valutazione effettuata dal Consiglio nazionale della ricerca riportato dall'Agenzia dell'Unione europea per i diritti fondamentali, Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015), pag. 18.

([70]) Dichiarazioni dell'ODNI (allegato VI), pag. 4.

([71]) Cfr. anche articolo 5(d) della PPD-28, che chiede al Direttore dell'intelligence nazionale, in coordinamento con i capi dei competenti servizi della comunità dell'intelligence e con l'Ufficio per la politica scientifica e tecnologica, di trasmettere al presidente una relazione in cui è valutata la realizzabilità di un software che renda più facile alla comunità dell'intelligence la rilevazione mirata di informazioni rispetto alla raccolta in blocco. Stando alle informazioni rese pubbliche al riguardo, la relazione giunge alla conclusione che non esiste alcuna alternativa informatizzata che possa sostituire totalmente la raccolta di dati in blocco ai fini del rilevamento di talune minacce per la sicurezza nazionale. Cfr. Signal Intelligence Reform, 2015 Anniversary Report.

([72]) Cfr. nota a piè di pagina 68.

([73]) Dichiarazioni dell'ODNI (allegato VI). Trova qui specifica risposta la preoccupazione espressa dalle autorità nazionali di protezione dei dati nel parere sul progetto di decisione sull'adeguatezza. Cfr. gruppo dell'articolo 29 per la tutela dei dati, parere 01/2016 sul progetto di decisione sull'adeguatezza dello scudo UE-USA per la privacy (adottato il 13 aprile 2016), pag. 38, n. 47.

([74]) Cfr. articolo 2 della PPD-28.

armi di distruzione di massa, le minacce alla sicurezza informatica, le minacce alle forze armate o al personale militare e le minacce criminali transnazionali inerenti alle altre cinque finalità; le finalità autorizzate sono riesaminate almeno una volta l'anno. Stando alle dichiarazioni del governo degli Stati Uniti, per conformarsi a questi requisiti i servizi della comunità dell'intelligence hanno potenziato le pratiche e i criteri analitici utilizzati per le interrogazioni sui dati non scremati ottenuti tramite l'intelligence dei segnali: le interrogazioni mirate «permettono di sottoporre all'analista soltanto i dati considerati in potenza possedere un valore a fini di intelligence» ([75]).

(75) Dette limitazioni sono particolarmente rilevanti per i dati personali trasferiti nell'ambito dello scudo, segnatamente se la raccolta dei dati personali avviene al di fuori degli USA, ad esempio durante il transito nei cavi transatlantici che collegano l'Unione agli Stati Uniti. Come confermato dalle autorità statunitensi nelle dichiarazioni dell'ODNI, le limitazioni e le garanzie ivi previste, comprese quelle fissate dalla PPD-28, si applicano a siffatta raccolta ([76]).

(76) Sebbene non formulati nei medesimi termini giuridici, nell'essenza detti principi rispecchiano i principi di necessità e di proporzionalità. È chiaramente privilegiata la rilevazione di dati mirata, mentre la raccolta in blocco è limitata alle situazioni (eccezionali) in cui motivi tecnici o operativi rendono impossibile la raccolta mirata. Anche nei casi in cui la *raccolta in blocco* è inevitabile, l'uso ulteriore, tramite l'accesso, dei dati così raccolti è *rigorosamente limitato* a precise finalità legittime di sicurezza nazionale ([77]).

(77) In quanto stabiliti in una direttiva emanata dal presidente nella sua veste di capo dell'esecutivo, detti requisiti sono vincolanti per tutta la comunità dell'intelligence e ad essi è stata data successivamente attuazione con le norme e procedure adottate dai vari enti per tradurre i principi generali in istruzioni specifiche per l'operatività quotidiana. Sebbene non sia vincolato dalla PPD-28, anche il Congresso è intervenuto per assicurare che, negli Stati Uniti, la raccolta di dati personali e l'accesso agli stessi siano mirati piuttosto che generalizzati.

(78) Dalle informazioni disponibili, comprese le dichiarazioni presentate dal governo degli Stati Uniti, risulta che, una volta che i dati sono stati trasferiti a un'organizzazione ubicata negli Stati Uniti che si è autocertificata nell'ambito dello scudo, gli enti statunitensi di intelligence possono ottenerli soltanto ([78]) se la richiesta è conforme alla legge relativa alla vigilanza sull'intelligence esterna (FISA) o se è presentata dal *Federal Bureau of Investigation* (FBI) in base a una *National Security Letter* (NSL) ([79]). La FISA prevede varie basi giuridiche utilizzabili per raccogliere (e quindi

([75]) Dichiarazioni dell'ODNI (allegato VI), pag. 4. Cfr. anche direttiva per la comunità dell'intelligence 203.
([76]) Dichiarazioni dell'ODNI (allegato VI), pag. 2. Si applicano parimenti le limitazioni previste dall'EO 12333 (ad esempio, l'obbligo che le informazioni rilevate rispondano alle priorità dell'intelligence stabilite dal presidente).
([77]) *Schrems*, punto 93.
([78]) La raccolta dati da parte dell'FBI può basarsi anche sui poteri conferiti dalla legge a fini di amministrazione della giustizia (cfr. parte 3.2 della presente decisione).
([79]) Per ulteriori delucidazioni sull'impiego delle NSL, cfr. dichiarazioni dell'ODNI (allegato VI), pagg. 13-14, n. 38. Come indicato in tali dichiarazioni, l'FBI può ricorrere all'NSL soltanto per ottenere informazioni non di contenuto pertinenti per un'indagine autorizzata di sicurezza nazionale condotta a fini di protezione dal terrorismo internazionale o da attività di intelligence clandestine. Quanto ai trasferimenti di dati nell'ambito dello scudo, il conferimento di potere più pertinente pare derivare dalla legge sulla privacy nelle comunicazioni elettroniche (Codice degli Stati Uniti d'America, titolo 18, articolo 2709), ai cui sensi la richiesta di informazioni sugli abbonati o di dati transazionali deve indicare un termine che identifica precisamente una persona, un soggetto, un numero di telefono o un *account*.

trattare) i dati personali degli interessati dell'UE trasferiti nel quadro dello scudo: oltre all'articolo 104 ([80]), che contempla la sorveglianza elettronica tradizionale personalizzata, e all'articolo 402 ([81]), relativo all'installazione di dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita, i due strumenti centrali sono l'articolo 501 (ex articolo 215 della legge U.S. PATRIOT) e l'articolo 702 ([82]).

(79) Al riguardo la legge USA FREEDOM, adottata il 2 giugno 2015, vieta la raccolta in blocco di dati in base all'articolo 402 della FISA (potere di intercettazione dei dati informativi della comunicazione in entrata e in uscita) e all'articolo 501 della FISA (ex articolo 215 della legge U.S. PATRIOT) ([83]) e mediante le *National Security Letter*, imponendo invece l'impiego di selettori specifici ([84]).

(80) Benché la FISA conferisca altri poteri di condotta di attività d'intelligence nazionale, intelligence dei segnali compresa, la Commissione valuta che, in relazione ai trasferimenti di dati nell'ambito dello scudo, tali poteri, al pari dei precedenti, limitino l'ingerenza delle autorità pubbliche alla raccolta e all'accesso mirati.

(81) Per la sorveglianza elettronica tradizionale personalizzata a norma dell'articolo 104 della FISA ([85]), detta valutazione è indubbia. Quanto all'articolo 702 della FISA, su cui si basano due importanti programmi di intelligence condotti dagli enti d'intelligence degli Stati Uniti (PRISM e UPSTREAM), la ricerca è resa mirata mediante l'impiego di singoli selettori che identificano dispositivi di comunicazione specifici, come l'indirizzo di posta elettronica o il numero di telefono dell'obiettivo, ma non parole chiave e neppure il nome degli obiettivi ([86]). Pertanto, come rilevato dall'Autorità per la tutela della vita privata e delle libertà civili (PCLOB), la

([80]) Codice degli Stati Uniti d'America, titolo 50, articolo 1804. Benché il potere conferito da quest'articolo sia subordinato a una dichiarazione in cui il richiedente espone i fatti e le circostanze che lo inducono a ritenere che l'obiettivo della sorveglianza elettronica sia una potenza straniera o un agente di una potenza straniera, tra questi ultimi può rientrare il cittadino straniero attivo nel terrorismo internazionale o nella proliferazione di armi di distruzione di massa su scala internazionale (attività preparatorie comprese) [Codice degli Stati Uniti d'America, titolo 50, articolo 1801 (B) (1)]. Il nesso con i dati personali trasferiti nell'ambito dello scudo è comunque soltanto teorico, in quanto l'esposizione dei fatti deve spiegare anche, per ciascun dispositivo o luogo interessato dalla sorveglianza elettronica, il motivo per cui si ritiene che sia usato, o sia in procinto di essere usato, da una potenza straniera o da un agente di una potenza straniera. In ogni caso, l'esercizio di questo potere è subordinato a una pronuncia della Corte FISA, la quale valuta, tra l'altro, se dai fatti esposti risultino motivi plausibili per ritenere fondata l'ipotesi di un uso a detti fini.

([81]) Codice degli Stati Uniti d'America, titolo 50, articolo 1842 in combinato disposto con l'articolo 1841(2), e titolo 18, articolo 3127. Il potere conferito da quest'articolo non riguarda il contenuto delle comunicazioni, bensì le informazioni sul cliente o sull'abbonato che usa un dato servizio (ad esempio, nome, indirizzo, numero di abbonato, durata/tipo del servizio ricevuto, fonte/modalità di pagamento). Il suo esercizio implica un provvedimento della Corte FISA (o di un magistrato giudice (*Magistrate Judge*) statunitense) e l'uso di un selettore specifico ai sensi dell'articolo 1841(4), ossia di un termine che identifica precisamente una persona, un *account* ecc., impiegato per limitare al minimo ragionevolmente possibile la gamma delle informazioni ricercate.

([82]) L'articolo 501 (ex articolo 215 della legge U.S. PATRIOT) autorizza l'FBI a chiedere al giudice un provvedimento che ingiunga di mettere a disposizione beni materiali (in particolare metadati telefonici, ma anche documenti aziendali) per scopi di intelligence esterna, mentre l'articolo 702 permette ai servizi della comunità dell'intelligence statunitense di chiedere l'accesso a informazioni, compresi i contenuti delle comunicazioni via Internet, che, seppur raccolte all'interno degli USA, riguardano determinati cittadini stranieri che si trovano al di fuori degli Stati Uniti.

([83]) In base a questa disposizione l'FBI può chiedere beni materiali (ad esempio, documenti e carte) dimostrando alla Corte FISA l'esistenza di ragionevoli motivi per ritenere che siano pertinenti ai fini di una sua specifica indagine. Per la ricerca l'FBI deve impiegare uno o più selettori approvati da tale Corte che, in base a un sospetto ragionevole e circostanziabile, sono associati a una o più potenze straniere o loro agenti attivi nel terrorismo internazionale o nelle relative attività preparatorie (cfr. Autorità per la tutela della vita privata e delle libertà civili (PCLOB), Sec. 215 Report, pag. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15 gennaio 2016, pagg. 4-6.

([84]) Dichiarazioni dell'ODNI (allegato VI), pag. 13 (n. 38).

([85]) Cfr. nota a piè di pagina 81.

([86]) PCLOB, Sec. 702 Report, pagg. 32-33 con ulteriori rimandi. Secondo il suo Ufficio per la tutela della vita privata, l'NSA deve verificare che esista un collegamento tra l'obiettivo e il selettore, deve documentare le informazioni di intelligence esterna che prevede di acquisire, le quali devono essere verificate e approvate da due analisti esperti dell'NSA, e dev'essere garantita la tracciatura dell'intero processo ai fini dei successivi controlli della conformità da parte dell'ODNI e del Dipartimento della Giustizia. Cfr. NSA CLPO, NSAs Implementation of Foreign Intelligence Act Section 702, 16 aprile 2014.

sorveglianza a norma dell'articolo 702 si esplica totalmente in una concentrazione delle rilevazioni su determinate persone [straniere] selezionate su base personalizzata ([87]). Poiché è prevista una clausola di caducità, l'articolo 702 della FISA dovrà essere riesaminato nel 2017, data alla quale la Commissione dovrà valutare nuovamente le garanzie disponibili per gli interessati dell'UE.

(82) Nelle sue dichiarazioni il governo degli Stati Uniti ha inoltre assicurato esplicitamente alla Commissione che la comunità dell'intelligence statunitense «non effettua una sorveglianza indiscriminata su nessuno, e quindi neppure sul comune cittadino europeo» ([88]). Per quanto riguarda i dati personali raccolti negli Stati Uniti, quest'affermazione è corroborata da prove empiriche del fatto che le *domande di accesso* presentate mediante NSL e ai sensi della FISA, considerate singolarmente e collettivamente, riguardano soltanto un numero relativamente basso di obiettivi rispetto al flusso complessivo di dati su Internet ([89]).

(83) Per quanto riguarda l'*accesso* ai dati rilevati e la *sicurezza dei dati*, la PPD-28 impone che l'accesso sia limitato al personale autorizzato che ha necessità di conoscere le informazioni per svolgere la propria missione e che le informazioni personali siano trattate e archiviate in condizioni tali da offrire una protezione adeguata e impedire l'accesso da parte di persone non autorizzate, in linea con le garanzie applicabili alle informazioni sensibili. Al personale addetto all'intelligence è impartita una formazione adeguata e sufficiente ai principi enunciati nella PPD-28 ([90]).

(84) Per quanto riguarda infine l'*archiviazione* e l'ulteriore *divulgazione* dei dati personali di interessati dell'UE raccolti dalle autorità di intelligence statunitensi, la PPD-28 afferma che ognuno (stranieri compresi) dev'essere trattato con dignità e rispetto, che ognuno ha un legittimo interesse alla tutela della propria vita privata nel quadro del trattamento dei dati personali che lo riguardano e che, quindi, i servizi della comunità dell'intelligence devono adottare politiche che offrano per tali dati garanzie adeguate «ragionevolmente intese a ridur[n]e al minimo la divulgazione e la conservazione» ([91]).

([87]) PLCOB, Sec. 702 Report, pag. 111. Cfr. anche dichiarazioni dell'ODNI (allegato VI), pag. 9 (A norma dell'articolo 702 della [FISA], le informazioni non possono essere rilevate in massa e indiscriminatamente: la raccolta deve limitarsi strettamente ai dati di intelligence esterna ricavati da obiettivi identificati individualmente e legittimamente) e pag. 13, n. 36 (con riferimento a un parere della Corte FISA del 2014); NSA CLPO, NSÀs Implementation of Foreign Intelligence Act Section 702, 16 aprile 2014. Anche nell'ambito di UPSTREAM l'NSA può chiedere l'intercettazione delle sole comunicazioni elettroniche dirette a, provenienti da o relative ai selettori attivati.

([88]) Dichiarazioni dell'ODNI (allegato VI), pag. 18. Cfr. anche pag. 6, dove si legge che le procedure applicabili «indicano un impegno chiaro a impedire la rilevazione arbitraria e indiscriminata di informazioni nell'ambito dell'intelligence dei segnali e a applicare, a partire dai massimi livelli del governo statunitense, il principio della ragionevolezza».

([89]) Cfr. Statistical Transparency Report Regarding Use of National Security Authorities, 22 aprile 2015. Per il flusso complessivo di dati su Internet, cfr., ad esempio, Agenzia per i diritti fondamentali, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), pagg. 15-16. Quanto al programma UPSTREAM, un parere declassificato della Corte FISA del 2011 afferma che le comunicazioni elettroniche acquisite ai sensi dell'articolo 702 della FISA s'inquadrano per oltre il 90 % nel programma PRISM e per meno del 10 % nel programma UPSTREAM [cfr. Corte FISA, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (consultabile all'indirizzo http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf)].

([90]) Cfr. articolo 4(a)(ii) della PPD-28. Cfr. anche ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, luglio 2014, pag. 5, secondo cui i servizi della comunità dell'intelligence dovrebbero potenziare le pratiche e i criteri analitici, nel senso che l'analista deve adoperarsi per strutturare l'interrogazione o altro termine o tecnica di ricerca in modo da reperire le informazioni di intelligence d'interesse ai fini di un compito valido di intelligence o di applicazione della legge, per rendere mirate le interrogazioni relative alle persone sulle categorie di informazioni d'intelligence che rispondono a un requisito di intelligence o di applicazione della legge e per ridurre al minimo l'analisi delle informazioni personali irrilevanti ai fini delle esigenze di intelligence o di applicazione della legge. Cfr., ad esempio. CIA, Signals Intelligence Activities, pag. 5; FBI, Presidential Policy Directive 28 Policies and Procedures, pag. 3. Stando al Progress Report on the Signals Intelligence Reform del 2016, i servizi della comunità dell'intelligence (tra cui FBI, CIA e NSA) hanno preso provvedimenti per sensibilizzare il personale agli obblighi imposti dalla PPD-28 introducendo nuove politiche formative o modificando quelle esistenti.

([91]) Stando alle dichiarazioni dell'ODNI, queste limitazioni si applicano a prescindere dal metodo di acquisizione delle informazioni (raccolta in blocco o rilevazione mirata) e dalla cittadinanza della persona.

(85) Il governo degli Stati Uniti ha spiegato che, in base al requisito della ragionevolezza, i servizi della comunità dell'intelligence non sono tenuti a adottare «qualsiasi misura possibile in linea teorica», ma piuttosto a trovare nelle loro attività un «punto di equilibrio fra i legittimi interessi di tutela della vita privata e delle libertà civili e le esigenze concrete delle attività di intelligence dei segnali» ([92]). In tale contesto i cittadini stranieri ricevono lo stesso trattamento riservato ai cittadini statunitensi o residenti negli USA, in linea con le procedure approvate dal Procuratore generale ([93]).

(86) In base a dette norme, in linea di principio i dati possono essere conservati per un massimo di cinque anni, salvo se la conservazione per un periodo più lungo è ritenuta nell'interesse della sicurezza nazionale in base a una considerazione di diritto o a una decisione esplicita del Direttore dell'intelligence nazionale, maturata dopo un'attenta valutazione degli aspetti legati alla privacy e sentiti il responsabile della tutela delle libertà civili dell'ODNI e i responsabili della tutela della vita privata e delle libertà civili degli enti ([94]). La divulgazione è limitata ai casi in cui le informazioni sono pertinenti alla finalità stessa della raccolta, e rispondono quindi a un'esigenza autorizzata di intelligence esterna o di applicazione della legge ([95]).

(87) Il governo degli Stati Uniti assicura che le informazioni personali non possono essere divulgate per il solo motivo che riguardano un cittadino straniero e che «i dati ricavati dall'intelligence dei segnali sulle attività abituali di uno straniero non possono essere considerati intelligence esterna da poter divulgare o conservare in via permanente per il solo fatto che riguardano uno straniero, a meno che rispondano altrimenti a un'esigenza autorizzata di intelligence esterna» ([96]).

(88) In base alle considerazioni che precedono, la Commissione giunge alla conclusione che negli Stati Uniti vigono regole intese a limitare a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato qualsiasi ingerenza per motivi di sicurezza nazionale nei diritti fondamentali della persona i cui dati personali sono trasferiti dall'Unione europea verso gli Stati Uniti nell'ambito dello scudo.

(89) Come emerge dall'analisi che precede, la legge degli Stati Uniti, garantisce che le misure di sorveglianza siano attuate soltanto per l'ottenimento di informazioni di intelligence esterna — il che è un obiettivo politico legittimo ([97]) — e siano il più possibile mirate. In particolare, la raccolta di dati in blocco è autorizzata soltanto in

([92]) Cfr. dichiarazioni dell'ODNI (allegato VI).

([93]) Cfr. articolo 4(a)(i) della PPD-28 in combinato disposto con l'articolo 2.3 dell'EO 12333.

([94]) Cfr. articolo 4(a)(i) della PPD-28. Dichiarazioni dell'ODNI (allegato VI), pag. 7. Ad esempio, per le informazioni personali raccolte ai sensi dell'articolo 702 della FISA, le procedure di minimizzazione dell'NSA, omologate dalla Corte FISA, prevedono che, in linea di principio, i metadati e i contenuti non scremati siano conservati al massimo per cinque anni per il programma PRISM e al massimo per due anni per il programma UPSTREAM. L'NSA rispetta questi limiti di archiviazione attraverso un processo automatizzato che cancella i dati raccolti al termine del rispettivo periodo di conservazione. Cfr. NSA Sec. 702 FISA Minimization Procedures, articolo 7 in combinato disposto con l'articolo 6(a)(1); NSA CLPO, NSÀs Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. Anche per i dati raccolti ai sensi dell'articolo 501 della FISA (ex articolo 215 della legge U.S. PATRIOT) la conservazione è limitata a cinque anni, a meno che i dati rientrino in una divulgazione debitamente autorizzata di informazioni d'intelligence esterna o che il Dipartimento della Giustizia informi per iscritto l'NSA del fatto che al riguardo è stato emesso un provvedimento conservativo in un contenzioso pendente o imminente. Cfr. NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15 gennaio 2016.

([95]) In particolare le informazioni personali possono essere divulgate soltanto: nel caso dell'articolo 501 della FISA (ex articolo 215 della legge U.S. PATRIOT), per scopi di antiterrorismo o come prove di un reato; nel caso dell'articolo 702 della FISA, in presenza di una finalità valida di intelligence esterna o di applicazione della legge. Cfr. NSA CLPO, NSÀs Implementation of Foreign Intelligence Surveillance Act Section 702, 16 aprile 2014. Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15 gennaio 2016. Cfr. anche NSÀs Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7 ottobre 2014.

([96]) Dichiarazioni dell'ODNI (allegato VI), pag. 7 (in riferimento alla direttiva per la comunità dell'intelligence 203).

([97]) La Corte di giustizia ha precisato che la sicurezza nazionale costituisce un obiettivo politico legittimo (cfr. *Schrems*, punto 88). Cfr. anche sentenza *Digital Rights Ireland e altri*, punti 42-44 e 51, in cui la Corte di giustizia ha rilevato come l'efficacia della lotta contro la criminalità grave, in particolare contro la criminalità organizzata e il terrorismo, possa dipendere in larga misura dall'uso delle moderne tecniche di indagine. Inoltre, a differenza delle indagini penali che, per loro stessa natura, riguardano la determinazione in retrospettiva di responsabilità e colpe per un comportamento passato, le attività di intelligence mirano spesso a prevenire le minacce per la sicurezza nazionale prima che si verifichi il danno. Spesso è pertanto possibile che debbano riguardare una gamma più vasta di soggetti possibili (gli «obiettivi») e un'area geografica più ampia [cfr. Corte europea dei diritti dell'uomo, *Weber e Saravia c. Germania*, decisione del 29 giugno 2006, n. 54934/00, punti 105-118 (relativi al cosiddetto «monitoraggio strategicof»)].

via eccezionale, quando la rilevazione mirata non è fattibile, ed è accompagnata da garanzie supplementari atte a ridurre al minimo la quantità di dati raccolti e il successivo accesso agli stessi (che dev'essere mirato e consentito solo per finalità specifiche).

(90) Nella valutazione della Commissione gli Stati Uniti operano quindi in modo conforme ai criteri stabiliti dalla Corte di giustizia nella sentenza *Schrems*, in base ai quali la normativa che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve imporre «requisiti minimi» ([98]) e in cui si afferma che «non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta» ([99]). Gli Stati Uniti non intendono procedere a una raccolta e archiviazione illimitate dei dati relativi a tutti senza limitazione alcuna né intendono consentire un accesso illimitato agli stessi. Inoltre, le dichiarazioni che gli USA hanno trasmesso alla Commissione, tra cui l'assicurazione che le attività di intelligence dei segnali condotte dagli Stati Uniti interessano soltanto una percentuale minima delle comunicazioni che transitano su Internet, escludono un accesso «in maniera generalizzata» ([100]) al contenuto delle comunicazioni elettroniche.

3.1.2. Tutele giuridiche efficaci

(91) La Commissione ha valutato sia i meccanismi di vigilanza esistenti negli Stati Uniti riguardo all'ingerenza delle autorità di intelligence statunitensi nei dati personali trasferiti negli Stati Uniti, sia i mezzi di ricorso individuale di cui dispone l'interessato dell'UE.

Vigilanza

(92) La comunità dell'intelligence statunitense è sottoposta a vari meccanismi di controllo e di vigilanza dipendenti dai tre poteri dello Stato: organi interni e esterni dell'esecutivo, varie commissioni del Congresso e, per le attività contemplate dalla legge relativa alla vigilanza sull'intelligence esterna (FISA), vigilanza del potere giudiziario.

(93) In primo luogo, l'esecutivo esercita una consistente vigilanza sulle attività di intelligence condotte dalle autorità statunitensi.

(94) A norma della PPD-28, articolo 4 (a) (iv), le politiche e procedure dei servizi della comunità dell'intelligence devono prevedere misure adeguate per facilitare la vigilanza sull'attuazione delle garanzie a protezione delle informazioni personali, tra cui misure che dispongono verifiche periodiche ([101]).

([98]) *Schrems*, punto 91, con ulteriori rimandi.
([99]) *Schrems*, punto 93.
([100]) *Schrems*, punto 94.
([101]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, pag. 7. Cfr., ad esempio CIA, Signals Intelligence Activities, pag. 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12 gennaio 2015, Sec. 8.1, 8.6(c).

(95) A tal fine sono stati predisposti vari livelli di vigilanza: addetti alla tutela della vita privata o alle libertà civili, ispettori generali, Ufficio per la tutela della vita privata e le libertà civili dell'ODNI, PCLOB e Autorità presidenziale di vigilanza sull'intelligence. In tutti gli enti del governo lavorano addetti alla conformità che assistono questi organi di vigilanza ([102]).

(96) Come spiegato dal governo degli Stati Uniti ([103]), *addetti alla tutela della vita privata o alle libertà civili*, con responsabilità di vigilanza, operano nei diversi dipartimenti che hanno competenze d'intelligence e negli enti d'intelligence ([104]). Benché i poteri precisi degli addetti possano variare leggermente in funzione dell'atto costitutivo, in ciascun caso è compresa tipicamente la vigilanza sulle procedure, per assicurare che il dipartimento/ente tenga adeguatamente conto degli aspetti inerenti alla privacy e alle libertà civili e abbia predisposto procedure adeguate per trattare i reclami sporti dalle persone che denunciano una violazione della loro privacy o delle loro libertà civili (in alcuni casi, come all'ODNI, gli addetti stessi sono abilitati a esaminare i reclami ([105])). Il capo del dipartimento/dell'ente deve provvedere a che l'addetto riceva tutte le informazioni e abbia accesso a tutta la documentazione necessaria per poter svolgere le proprie funzioni. Gli addetti alla tutela della vita privata e alle libertà civili riferiscono periodicamente al Congresso e alla PCLOB, indicando tra l'altro il numero e la natura dei reclami ricevuti dal dipartimento/dall'ente e fornendo una sintesi del trattamento loro riservato, delle verifiche effettuate e delle indagini condotte, nonché degli effetti delle attività svolte dall'addetto stesso ([106]). Le autorità nazionali di protezione dei dati valutano «abbastanza rigorosa» la vigilanza interna esercitata dagli addetti alla tutela della vita privata o alle libertà civili, che a loro parere non garantisce tuttavia il necessario grado di indipendenza ([107]).

(97) Oltre agli addetti, ciascun servizio della comunità dell'intelligence ha il proprio *ispettore generale*, incaricato, tra l'altro, di vigilare sulle attività di intelligence esterna ([108]). L'articolazione del sistema comprende, presso l'ODNI, un Ufficio dell'ispettore generale con competenza generale su tutta la comunità dell'intelligence, autorizzato a esaminare i reclami o le informazioni inerenti a presunti comportamenti illeciti o abusi di potere compiuti in relazione con i programmi e attività dell'ODNI e/o della più ampia comunità dell'intelligence ([109]). L'ispettore generale è un'unità, indipendente per legge ([110]), responsabile dei controlli e delle indagini riguardanti i programmi e le operazioni condotte dall'ente per scopi di intelligence nazionale, compreso in caso di abuso o violazione della legge ([111]). È autorizzato a accedere a tutti i dati, relazioni, verifiche, esami, documenti, carte, raccomandazioni o altro materiale pertinente, se necessario mediante l'emanazione di una citazione, e può

([102]) Ad esempio, la Direzione Conformità dell'NSA conta oltre 300 addetti. Cfr. dichiarazioni dell'ODNI (allegato VI), pag. 7.

([103]) Cfr. meccanismo di mediazione (allegato III), punto 6(b) (i)-(iii).

([104]) Cfr. Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee-1. È il caso, ad esempio, del Dipartimento di Stato, del Dipartimento della Giustizia (FBI compresa), del Dipartimento della Sicurezza interna, del Dipartimento della Difesa, dell'NSA, della CIA e dell'ODNI.

([105]) Stando alle informazioni comunicate dal governo degli Stati Uniti, quando riceve un reclamo l'Ufficio per la tutela della vita privata e le libertà civili dell'ODNI provvede anche a coordinarsi anche con gli altri servizi della comunità dell'intelligence per decidere l'ulteriore trattamento da riservargli in tale ambito. Cfr. meccanismo di mediazione (allegato III), punto 6(b) (ii).

([106]) Cfr. Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee-1 (f)(1),(2).

([107]) Gruppo dell'articolo 29 per la tutela dei dati, parere 01/2016 sul progetto di decisione sull'adeguatezza dello scudo UE-USA per la privacy (adottato il 13 aprile 2016), pag. 41.

([108]) Dichiarazioni dell'ODNI (allegato VI), pag. 7. Cfr. ad esempio, NSA, PPD-28 Section 4 Procedures, 12 gennaio 2015, Sec. 8.1; CIA, Signals Intelligence Activities, pag. 7 (Responsibilities).

([109]) L'ispettore generale (IG), istituito a ottobre 2010, è nominato dal presidente e confermato dal Senato e può essere destituito soltanto dal presidente, non dal Direttore dell'intelligence nazionale.

([110]) L'ispettore generale è nominato a tempo indeterminato e può essere rimosso dall'incarico solo dal presidente, il quale deve comunicare per iscritto al Congresso i motivi della destituzione. Questo non implica necessariamente che sia totalmente svincolato da qualsiasi istruzione. Se considerato necessario per tutelare importanti interessi di sicurezza nazionale, il capo del dipartimento può in alcuni casi vietargli di avviare, svolgere o completare una verifica o un'indagine. Quando tale prerogativa è esercitata, il Congresso deve tuttavia esserne informato e potrebbe al riguardo chiamare in causa la responsabilità del direttore. Cfr., ad esempio, legge sugli ispettori generali del 1978, articolo 8 (IG del Dipartimento della Difesa); articolo 8E (IG del Dipartimento della Giustizia), articolo 8G (d)(2)(A),(B) (IG dell'NSA); Codice degli Stati Uniti d'America, titolo 50, articolo 403 q (B) (IG della CIA); legge autorizzativa dell'intelligence per l'esercizio finanziario 2010, articolo 405(f) (IG per la comunità dell'intelligence). Nella valutazione delle autorità nazionali di protezione dei dati, gli ispettori generali paiono soddisfare il criterio dell'indipendenza organizzativa, quale definitivo dalla Corte di giustizia dell'Unione europea e dalla Corte europea dei diritti dell'uomo, perlomeno a partire dal momento in cui si applicherà a tutti la nuova procedura di nomina. Cfr. gruppo dell'articolo 29 per la tutela dei dati, parere 01/2016 sul progetto di decisione sull'adeguatezza dello scudo UE-USA per la privacy (adottato il 13 aprile 2016), pag. 40.

([111]) Cfr. dichiarazioni dell'ODNI (allegato VI), pag. 7. Cfr. anche legge sugli ispettori generali del 1978 e successive modifiche, Pub. L. 113-126 del 7 luglio 2014.

assumere testimonianze ([112]). Sebbene l'ispettore generale possa formulare soltanto raccomandazioni non vincolanti di azioni correttive, i rapporti che redige, anche sugli interventi con cui vi si è dato seguito (o sull'assenza di tali interventi), sono resi pubblici e, soprattutto, trasmessi al Congresso, che su tale base può esercitare la sua funzione di vigilanza ([113]).

(98) Inoltre, l'*Autorità per la tutela della vita privata e delle libertà civili* (PCLOB), ente indipendente ([114]) inquadrato nell'esecutivo e composto di cinque membri provenienti dai ranghi di entrambi i partiti ([115]), nominati dal presidente per un mandato di sei anni con l'approvazione del Senato, ha responsabilità in materia di tutela della privacy e delle libertà civili nelle politiche dell'antiterrorismo e relativa attuazione. Per controllare le attività della comunità dell'intelligence ha facoltà di accedere a tutti i dati, relazioni, verifiche, documenti, carte e raccomandazioni dell'ente interessato, comprese le informazioni classificate, di procedere a interrogatori e di assumere testimonianze. Riceve le relazioni trasmesse dagli addetti alla tutela della vita privata e alle libertà civili di vari dipartimenti/enti federali ([116]), può rivolgere loro raccomandazioni e riferisce periodicamente alle commissioni del Congresso e al presidente ([117]). Nei limiti del suo mandato, la PCLOB è inoltre incaricata di redigere una relazione di valutazione dell'attuazione della PPD-28.

(99) I meccanismi di vigilanza citati sono infine completati dall'*Autorità di vigilanza sull'intelligence*, istituita nell'ambito del Comitato presidenziale consultivo sull'intelligence che vigila sul rispetto della Costituzione e di tutte le applicabili norme da parte delle autorità di intelligence degli Stati Uniti.

(100) Per facilitare l'esercizio della vigilanza, i servizi della comunità dell'intelligence sono incoraggiati a sviluppare sistemi informatici che permettano il monitoraggio, la registrazione e la verifica delle interrogazioni o altre ricerche di informazioni personali ([118]). Gli organi di vigilanza e di controllo della conformità controllano periodicamente le pratiche seguite dai servizi della comunità dell'intelligence per proteggere le informazioni personali contenute nell'intelligence dei segnali e il rispetto delle relative procedure ([119]).

(101) Le funzioni di vigilanza sono sostenute anche da ampi obblighi di segnalazione dei casi di inosservanza. In particolare, le procedure dell'ente devono garantire che, quando si pone un serio problema di conformità che, indipendentemente dalla cittadinanza della persona, interessa informazioni personali rilevate nell'ambito dell'intelligence dei segnali, il caso debba essere segnalato prontamente al capo del servizio della comunità dell'intelligence in questione, che ne informa a sua volta il Direttore dell'intelligence nazionale cui, in virtù della PPD-28, spetta stabilire se siano necessarie azioni correttive ([120]). Inoltre, a norma dell'EO 12333, tutti i servizi della comunità dell'intelligence sono tenuti a segnalare i casi di inosservanza all'Autorità di vigilanza sull'intelligence ([121]). Questi meccanismi garantiscono che la questione sia affrontata ai massimi livelli della comunità dell'intelligence. Se sono

([112]) Cfr. legge sugli ispettori generali del 1978, articolo 6.
([113]) Cfr. dichiarazioni dell'ODNI (allegato VI), pag. 7. Cfr. legge sugli ispettori generali del 1978, articoli 4(5) e 5. A norma dell'articolo 405 (b)(3),(4) della legge autorizzativa dell'intelligence per l'esercizio finanziario 2010, Pub. L. 111-259 del 7 ottobre 2010, l'ispettore generale per la comunità dell'intelligence tiene informato il Direttore dell'intelligence nazionale e il Congresso della necessità di misure correttive e del relativo iter.
([114]) Le autorità nazionali di protezione dei dati ritengono che in passato la PCLOB abbia dimostrato di esercitare i propri poteri in indipendenza. Cfr. gruppo dell'articolo 29 per la tutela dei dati, parere 01/2016 sul progetto di decisione sull'adeguatezza dello scudo UE-USA per la privacy (adottato il 13 aprile 2016), pag. 42.
([115]) La PCLOB ha inoltre in organico una ventina di dipendenti — cfr. https://www.pclob.gov/about-us/staff.html.
([116]) Tra cui almeno il Dipartimento della Giustizia, il Dipartimento della Difesa, il Dipartimento della Sicurezza interna, il Direttore dell'intelligence nazionale e la *Central Intelligence Agency*, cui si aggiungono tutti gli altri dipartimenti, enti o servizi dell'esecutivo che la PCLOB ha ritenuto opportuno contemplare.
([117]) Cfr. Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee. Cfr. meccanismo di mediazione (allegato III), punto 6(b) (iv). La PCLOB è tenuta a segnalare, fra gli altri, i casi in cui il suo parere è disatteso da un ente dell'esecutivo.
([118]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, pagg. 7-8.
([119]) Ibid. pag. 8. Cfr. anche dichiarazioni dell'ODNI (allegato VI), pag. 9.
([120]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, pag. 7. Cfr., ad esempio, NSA, PPD-28 Section 4 Procedures, 12 gennaio 2015, Sec. 7.3, 8.7(c), (d); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); CIA, Signals Intelligence Activities, pag. 6 (Compliance) e pag. 8 (Responsibilities).
([121]) Cfr. EO 12333, articolo 1.6(c).

interessate informazioni personali relative a un cittadino straniero, il Direttore dell'intelligence nazionale stabilisce, in consultazione con il segretario di Stato e il capo del dipartimento o ente segnalante, se occorra intervenire per informare il relativo governo straniero, ferma restando la necessità di proteggere la fonte, il metodo e il personale degli USA ([122]).

(102) In secondo luogo, oltre ai citati meccanismi di vigilanza inquadrati nell'esecutivo, il Congresso degli Stati Uniti d'America, e più precisamente le *commissioni Giustizia e Intelligence della Camera dei rappresentanti e del Senato*, ha competenze di vigilanza sulle attività d'intelligence esterna condotte dagli USA, intelligence dei segnali compresa. A norma della legge sulla sicurezza nazionale, il presidente provvede a che le commissioni del Congresso che si occupano di intelligence siano tenute perfettamente informate e aggiornate sulle attività d'intelligence condotte dagli USA, comprese, come richiesto dal pertinente sottocapo della legge, le attività d'intelligence rilevanti previste per il futuro ([123]). Il presidente deve inoltre assicurare che tali commissioni del Congresso siano informate prontamente di qualsiasi attività d'intelligence illegale e delle misure correttive adottate o previste al riguardo ([124]). I membri di tali commissione hanno accesso alle informazioni classificate e ai metodi e programmi d'intelligence ([125]).

(103) Gli obblighi di segnalazione sono stati ampliati e perfezionati con le leggi adottate successivamente, per quanto riguarda sia i servizi della comunità dell'intelligence sia i pertinenti ispettori generali e il Procuratore generale. La FISA chiede ad esempio al Procuratore generale di informare perfettamente le commissioni Intelligence e Giustizia del Senato e della Camera dei rappresentanti circa le attività svolte dal governo ai sensi di determinati suoi articoli ([126]). Chiede inoltre al governo di trasmettere alle commissioni del Congresso copia di ogni decisione, ordinanza o parere pronunciati dalla Corte FISA, o dalla Corte di controllo della vigilanza sull'intelligence esterna, in cui è riportata una spiegazione o interpretazione rilevante di una disposizione della FISA. Per quanto riguarda in particolare la sorveglianza a norma dell'articolo 702 della FISA, la vigilanza si esplica nell'obbligo di presentare le relazioni previste dalla legge alle commissioni Intelligence e Giustizia e nelle frequenti audizioni e riunioni informative, tra cui: la relazione semestrale in cui il Procuratore generale riferisce sull'applicazione dell'articolo 702 della FISA, corredata di documenti giustificativi, tra i quali, in particolare, le relazioni sulla conformità del Dipartimento della Giustizia e dell'ODNI e la descrizione dei casi di inosservanza ([127]), e la distinta valutazione semestrale in cui il Procuratore generale e il Direttore dell'intelligence nazionale riferiscono sul rispetto delle procedure atte a rendere mirata e a minimizzare la raccolta dati, comprese le procedure volte a garantire che i dati siano raccolti per una finalità valida di intelligence esterna ([128]). Il Congresso riceve inoltre le relazioni degli ispettori generali che sono autorizzati a valutare il rispetto delle procedure atte a rendere mirata e a minimizzare la raccolta dati da parte degli enti, e gli orientamenti del Procuratore generale.

(104) A norma della legge USA FREEDOM del 2015, il governo statunitense deve comunicare ogni anno al Congresso (e al pubblico) il numero delle ordinanze e delle direttive ai sensi della FISA chieste e ottenute, così come, tra l'altro, la stima del numero di cittadini statunitensi o residenti negli USA e di cittadini stranieri sottoposti a sorveglianza ([129]). La legge impone altre comunicazioni pubbliche circa il numero di *National Security Letter*

([122]) PPD-28, articolo 4(a)(iv).
([123]) Cfr. articolo 501(a)(1) (Codice degli Stati Uniti d'America, titolo 50, articolo 413(a)(1)]. Questa disposizione prevede i requisiti generali in materia di vigilanza del Congresso nel settore della sicurezza nazionale.
([124]) Cfr. articolo 501(b) [Codice degli Stati Uniti d'America, titolo 50, articolo 413(b)].
([125]) Cfr. articolo 501(d) [Codice degli Stati Uniti d'America, titolo 50, articolo 413(d)].
([126]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articoli 1808, 1846, 1862, 1871, 1881f.
([127]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1881f.
([128]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1881a(l)(1).
([129]) Cfr. legge USA FREEDOM del 2015, Pub. L. No. 114-23, articolo 602(a). Inoltre, ai sensi dell'articolo 402, il Direttore dell'intelligence nazionale effettua, in consultazione con il Procuratore generale, una verifica ai fini della declassificazione di ogni decisione, ordinanza o parere pronunciati dalla Corte FISA o dalla Corte di controllo della vigilanza sull'intelligence esterna (secondo la definizione riportata nell'articolo 601(e)] in cui è riportata una spiegazione o interpretazione rilevante di una disposizione di legge, compresa l'eventuale spiegazione o interpretazione inedita o rilevante dell'espressione «selettore specifico», e, coerentemente con tale verifica, rende pubblici, nella massima misura possibile, la decisione, l'ordinanza o il parere pertinenti.

emanate, anche in questo caso nei confronti sia di cittadini statunitensi o residenti negli USA sia di cittadini stranieri (permettendo nel contempo al destinatario di un'ordinanza o certificazione ai sensi della FISA, o di una richiesta di NSL, di pubblicare, a determinate condizioni, rapporti sulla trasparenza) ([130]).

(105) In terzo luogo, le attività d'intelligence condotte dalle autorità pubbliche statunitensi a norma della FISA sono subordinate alla verifica, e in alcuni casi all'autorizzazione preventiva, della *Corte FISA* ([131]), giudice indipendente ([132]) le cui decisioni possono essere impugnate dinanzi alla Corte di controllo della vigilanza sull'intelligence esterna (FISCR) ([133]) e, in ultima istanza, dinanzi alla Corte suprema degli Stati Uniti d'America ([134]). Per l'autorizzazione preventiva, l'autorità richiedente (FBI, NSA, CIA ecc.) deve presentare un progetto di domanda all'ufficio legale del Dipartimento della sicurezza nazionale del Dipartimento della Giustizia, che la esamina e, se necessario, chiede ulteriori informazioni ([135]). Una volta messa a punto, la domanda dev'essere approvata dal Procuratore generale, dal Viceprocuratore generale o dal Procuratore generale aggiunto per la sicurezza nazionale ([136]). Il Dipartimento della Giustizia trasmette quindi la domanda alla Corte FISA, che la valuta e stabilisce in via preliminare come procedere ([137]). Se è organizzata un'udienza, la Corte FISA ha il potere di assumere testimonianze, eventualmente anche in forma di pareri di esperti ([138]).

(106) La Corte FISA (così come la FISCR) è coadiuvata da un comitato permanente formato da cinque persone di chiara esperienza in materia di sicurezza nazionale e di libertà civili ([139]). Scegliendo fra queste persone la Corte ne designa una per il ruolo di *amicus curiae*, col compito di prestare assistenza nell'esame di una domanda di ordinanza o riesame che, a parere della Corte, comporta un'interpretazione rilevante o inedita della legge; la Corte può prescindere dalla designazione se non la ritiene opportuna ([140]). Il sistema permette in particolare di assicurare che la valutazione della Corte tenga adeguatamente conto degli aspetti inerenti alla privacy. Se lo reputa opportuno, la Corte può anche designare una persona o un'organizzazione per il ruolo di *amicus curiae*, anche per assisterla con perizie tecniche, così come può dare, alla persona o all'organizzazione che lo richiede, la facoltà di presentare una memoria in qualità di *amicus curiae* ([141]).

([130]) Legge USA FREEDOM, articoli 602(a), 603(a).

([131]) Per alcuni tipi di sorveglianza, un magistrato giudice (*Magistrate Judge*) statunitense nominato pubblicamente dal presidente della Corte suprema (*Chief Justice*) degli Stati Uniti può essere abilitato a conoscere delle domande e a emanare ordinanze.

([132]) La Corte FISA è composta di undici giudici nominati dal presidente della Corte suprema degli Stati Uniti fra i giudici dei tribunali distrettuali statunitensi in esercizio, a loro volta precedentemente nominati dal presidente e confermati dal Senato. I giudici, che sono nominati a vita e possono essere rimossi dall'incaricato solo per giusta causa, siedono alla Corte FISA per periodi scaglionati di sette anni. A norma della FISA, i giudici devono essere scelti in almeno sette circoscrizioni giudiziarie diverse degli Stati Uniti [cfr. articolo 103 FISA — Codice degli Stati Uniti d'America, titolo 50, articolo 1803 (a)]; PCLOB, Sec. 215 Report, pagg. 174-187). I giudici sono coadiuvati da assistenti giudiziari di vasta esperienza, che costituiscono il personale legale della Corte e preparano l'analisi giuridica delle richieste di raccolta dati. (cfr. Autorità per la tutela della vita privata e delle libertà civili (PCLOB), Sec. 215 Report, pag. 178; Lettera di Reggie B. Walton, presidente della Corte di vigilanza sull'intelligence esterna degli USA, a Patrick J. Leahy, presidente della Commissione Giustizia del Senato degli Stati Uniti, del 29 luglio 2013 («lettera di Walton»), pagg. 2-3.

([133]) La FISCR è composta di tre giudici nominati dal presidente della Corte suprema degli Stati Uniti fra i giudici dei tribunali distrettuali o delle corti d'appello distrettuali statunitensi, che siedono alla FISCR per periodi scaglionati di sette anni [cfr. articolo 103 della FISA — Codice degli Stati Uniti d'America, titolo 50, articolo 1803(b)].

([134]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articoli 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([135]) Ad esempio, ulteriori elementi fattuali circa l'obiettivo della sorveglianza, informazioni tecniche sul metodo di sorveglianza tecnica o metodologia oppure garanzie circa il modo in cui saranno usate e divulgate le informazioni ottenute. Cfr. PCLOB, Sec. 215 Report, pag. 177.

([136]) Codice degli Stati Uniti d'America, titolo 50, articoli 1804 (a), 1801 (g).

([137]) La Corte FISA può approvare la domanda, chiedere ulteriori informazioni, decidere che è necessaria un'udienza o indicare il possibile rigetto della domanda. In base alle decisioni preliminari della Corte il governo presenta la domanda definitiva, che, modificata alla luce delle osservazioni preliminari del giudice, può essere molto diversa da quella iniziale. La Corte FISA approva un'alta percentuale delle domande definitive, ma gran parte di queste sono considerevolmente modificate rispetto alla domanda originaria (ad esempio, 24 % delle domande approvate nel periodo da luglio a settembre 2013) (cfr. PCLOB, Sec. 215 Report, pag. 179; lettera di Walton, pag. 3).

([138]) PCLOB, Sec. 215 Report, pag. 179, n. 619.

([139]) Codice degli Stati Uniti d'America, titolo 50, articolo 1803 (i)(1),(3)(A). Questa nuova normativa ha attuato le raccomandazioni della PCLOB di creare un *pool* di esperti in materia di privacy e di libertà civili che possano intervenire in veste di *amicus curiae* per presentare alla Corte argomentazioni giuridiche a favore della privacy e delle libertà civili (cfr. PCLOB, Sec. 215 Report, pagg. 183-187).

([140]) Codice degli Stati Uniti d'America, titolo 50, articolo 1803 (i)(2)(A). Secondo le informazioni comunicate dall'ODNI, sono già state effettuate nomine di questo tipo (cfr. Signals Intelligence Reform, 2016 Progress Report).

([141]) Codice degli Stati Uniti d'America, titolo 50, articolo 1803 (i)(2)(B).

(107) Quanto ai due conferimenti di potere in materia di sorveglianza previsti dalla FISA che sono maggiormente rilevanti ai fini dei trasferimenti di dati nell'ambito dello scudo, la vigilanza esercitata dalla Corte FISA sull'uno differisce da quella esercitata sull'altro.

(108) Nell'ambito dell'articolo 501 della FISA ([142]), che consente l'acquisizione di beni materiali (compresi libri, registri, carte, documenti e altro), la domanda presentata alla Corte FISA deve comprendere un'esposizione dei fatti che indichi i ragionevoli motivi per i quali si ritiene che i beni materiali richiesti siano pertinenti per un'indagine autorizzata (e non per la valutazione di una minaccia), condotta per l'ottenimento di informazioni di intelligence esterna che non riguardano un cittadino statunitense o residente negli USA oppure per la protezione contro il terrorismo internazionale o attività di intelligence clandestine. La domanda deve altresì elencare le procedure di minimizzazione adottate dal Procuratore generale relativamente alla conservazione e alla divulgazione dei dati d'intelligence raccolti. ([143])

(109) Per converso, nell'ambito dell'articolo 702 della FISA ([144]) la Corte FISA non autorizza singole misure di sorveglianza, ma piuttosto programmi di sorveglianza (quali PRISM e UPSTREAM) basandosi sulle certificazioni annuali preparate dal Procuratore generale e dal Direttore dell'intelligence nazionale. L'articolo 702 della FISA consente di prendere a obiettivo persone che si ritiene ragionevolmente si trovino al di fuori degli Stati Uniti, al fine di acquisire informazioni di intelligence esterna ([145]). Per l'individuazione degli obiettivi l'NSA procede in due fasi. Primo, gli analisti dell'NSA individuano i cittadini stranieri all'estero che, nella loro valutazione, se sorvegliati porteranno a ottenere i pertinenti dati d'intelligence esterna indicati nella certificazione. Secondo, una volta individuate le persone e approvata, al termine di un processo ampio di verifica interno all'NSA ([146]), la sorveglianza su di esse, sono «attivati» (ossia sviluppati e applicati) i selettori che identificano i dispositivi di comunicazione (come gli indirizzi di posta elettronica) usati da tali obiettivi ([147]). Come indicato in precedenza, le certificazioni che la Corte FISA deve approvare non contengono informazioni sul singolo potenziale obiettivo, ma indicano piuttosto categorie di informazioni di intelligence esterna ([148]). La Corte FISA non valuta, in base a elementi plausibili né a altro criterio, se la persona costituisca un obiettivo adatto per acquisire informazioni di intelligence esterna ([149]); il suo controllo verte piuttosto sulla condizione che uno degli scopi rilevanti dell'acquisizione dev'essere quello di ottenere informazioni di intelligence esterna ([150]). Ai sensi dell'articolo 702 della FISA, infatti, l'NSA è autorizzata a rilevare le comunicazioni di cittadini stranieri al di fuori degli Stati Uniti solo se si può ragionevolmente ritenere che un determinato mezzo di comunicazione sia usato per comunicare informazioni di intelligence esterna (ad esempio in relazione al terrorismo internazionale, alla proliferazione nucleare o ad attività informatiche ostili). Le decisioni al riguardo sono soggette a sindacato giurisdizionale ([151]). Le certificazioni devono prevedere anche procedure atte a rendere mirata e a minimizzare la raccolta ([152]). Il

([142]) Codice degli Stati Uniti d'America, titolo 50, articolo 1861.
([143]) Codice degli Stati Uniti d'America, titolo 50, articolo 1861 (b).
([144]) Codice degli Stati Uniti d'America, titolo 50, articolo 1881.
([145]) Codice degli Stati Uniti d'America, titolo 50, articolo 1881a (a).
([146]) PCLOB, Sec. 702 Report, pag. 46.
([147]) Codice degli Stati Uniti d'America, titolo 50, articolo 1881a (h).
([148]) Codice degli Stati Uniti d'America, titolo 50, articolo1881a (g). Stando alla PCLOB, finora le categorie hanno riguardato principalmente il terrorismo internazionale e aspetti quali l'acquisizione di armi di distruzione di massa. Cfr. PCLOB, Sec. 702 Report, pag. 25.
([149]) PCLOB, Sec. 702 Report, pag. 27.
([150]) Codice degli Stati Uniti d'America, titolo 50, articolo 1881a.
([151]) «Liberty and Security in a Changing World», Rapporto e raccomandazioni del gruppo presidenziale di verifica dell'intelligence e tecnologie della comunicazione, 12 dicembre 2013, pag. 152.
([152]) Codice degli Stati Uniti d'America, titolo 50, articolo1881a (i)

Procuratore generale e il Direttore dell'intelligence nazionale verificano la conformità e gli enti sono tenuti a segnalare i casi di inosservanza alla Corte FISA ([153]) (così come al Congresso e all'Autorità presidenziale di vigilanza sull'intelligence), che su tale base può modificare l'autorizzazione ([154]).

(110) Per aumentare l'efficacia della vigilanza da parte della Corte FISA, l'amministrazione statunitense ha deciso di dare attuazione a una raccomandazione della PCLOB trasmettendo a tale Corte la documentazione relativa alle decisioni atte a rendere mirata la raccolta dati a norma dell'articolo 702, compreso un campione casuale delle schede di attivazione, al fine di consentirle di valutare il modo in cui è assolto nella pratica l'obbligo di avere una finalità d'intelligence esterna ([155]). Al tempo stesso l'amministrazione statunitense ha accettato di rivedere le procedure dell'NSA atte a rendere mirata la raccolta dati e ha adottato misure al riguardo, nell'intento di documentare meglio i motivi d'intelligence esterna su cui si basano le decisioni di scelta dell'obiettivo ([156]).

Ricorso individuale

(111) La legge degli USA offre all'interessato dell'UE vari mezzi per sapere se i servizi della comunità dell'intelligence statunitense abbiano trattato dati personali che lo riguardano (o li abbiano raccolti, vi abbiano avuto accesso ecc.) e, in caso affermativo, se siano state rispettate le limitazioni applicabili a norma della legge statunitense. Gli aspetti interessati sono essenzialmente tre: ingerenze ai sensi della FISA, accesso intenzionale illecito ai dati personali da parte di agenti del governo, e accesso alle informazioni ai sensi della legge sulla libertà di informazione (FOIA) ([157]).

(112) In primo luogo, la legge relativa alla vigilanza sull'intelligence esterna (FISA) prevede una serie di mezzi, a disposizione anche dei cittadini stranieri, per contestare la sorveglianza elettronica illecita ([158]), offrendo alla persona la possibilità di avviare una causa civile contro gli USA per ottenere un risarcimento pecuniario quando le informazioni che la riguardano sono state usate o divulgate illecitamente e con dolo ([159]), di adire le vie legali contro agenti del governo statunitense, nella loro capacità personale («abuso di potere») per ottenere un risarcimento pecuniario ([160]), e di contestare la legalità della sorveglianza (chiedendo anche di sopprimere le informazioni) quando il governo degli Stati Uniti intende usare o divulgare le informazioni raccolte o ricavate dalla sorveglianza elettronica contro la persona in un procedimento giudiziario o amministrativo negli Stati Uniti ([161]).

(113) In secondo luogo, il governo degli Stati Uniti ha rimandato la Commissione a una serie di ulteriori possibilità di cui l'interessato dell'Unione europea potrebbe valersi per adire le vie legali contro agenti del governo in caso di

([153]) A norma dell'articolo 13 (b) del regolamento di procedura della Corte FISA, il governo deve avvisare per iscritto la Corte non appena scopre che un potere o un'approvazione da questa accordato è stato attuato in maniera non conforme all'autorizzazione o approvazione o non conforme alla legge applicabile. Il governo deve comunicare per iscritto alla Corte anche i fatti e le circostanze pertinenti all'inosservanza. In genere il governo trasmette l'avviso definitivo a norma dell'articolo 13 (a) una volta che sono noti i fatti e che i dati raccolti al di fuori dell'autorizzazione sono stati distrutti (cfr. lettera di Walton, pag. 10).

([154]) Codice degli Stati Uniti d'America, titolo 50, articolo 1881 (l). Cfr. anche PCLOB, Sec. 702 Report, pagg. 66-76. NSA CLPO, NSÀs Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. La raccolta di dati personali per finalità di intelligence a norma dell'articolo 702 della FISA è soggetta a vigilanza interna ed esterna nell'esecutivo. La vigilanza interna comprende fra l'altro programmi interni di conformità per valutare e verificare il rispetto delle procedure atte a rendere mirata e a minimizzare la raccolta dati, la segnalazione dei casi d'inosservanza, all'interno e esternamente all'ODNI, al Dipartimento della Giustizia, al Congresso e alla Corte FISA, e la trasmissione di verifiche annuali agli stessi organi. La vigilanza esterna consiste principalmente in verifiche delle procedure atte a rendere mirata e a minimizzare la raccolta dati effettuate dall'ODNI, dal Dipartimento della Giustizia e dagli ispettori generali, i quali riferiscono a loro volta al Congresso e alla Corte FISA segnalando anche i casi di inosservanza. I casi di inosservanza rilevanti devono essere segnalati alla Corte FISA immediatamente, gli altri in rapporti trimestrali (cfr. PCLOB, Sec. 702 Report, pagg. 66-77).

([155]) PCLOB, Recommendations Assessment Report, 29 gennaio 2015, pag. 20.

([156]) PCLOB, Recommendations Assessment Report, 29 gennaio 2015, pag. 16.

([157]) A questo si aggiunte il disposto dell'articolo 10 della legge sulle procedure applicabili alle informazioni classificate, in base al quale, nelle azioni penali in cui devono stabilire se il materiale costituisce informazioni classificate (ad esempio, perché per motivi di sicurezza nazionale dev'essere tutelata dalla divulgazione non autorizzata), gli Stati Uniti notificano all'imputato le parti del materiale su cui prevedono ragionevolmente di basarsi per stabilire l'elemento legato a informazioni classificate del reato.

([158]) Per quanto segue cfr. dichiarazioni dell'ODNI (allegato VI), pag. 16.

([159]) Codice degli Stati Uniti d'America, titolo 18, articolo 2712.

([160]) Codice degli Stati Uniti d'America, titolo 50, articolo 1810.

([161]) Codice degli Stati Uniti d'America, titolo 50, articolo 1806.

accesso o uso illecito dei dati personali da parte del governo, anche per asserite finalità di sicurezza nazionale, ossia la legge sulle frodi e gli abusi informatici ([162]), la legge sulla privacy nelle comunicazioni elettroniche ([163]) e la legge sul diritto alla privacy finanziaria ([164]). Tutti questi motivi per adire le vie legali riguardano dati, obiettivi e/o tipi di accesso specifici (ad esempio, accesso a un computer in remoto via Internet) e sono disponibili a determinate condizioni (ad esempio, condotta intenzionale/dolosa, abuso di potere, danno) ([165]). Una possibilità di ricorso più generale è offerta dalla legge sulle procedure amministrative (Codice degli Stati Uniti d'America, titolo 5, articolo 702), in base alla quale chiunque subisca un illecito, un inconveniente o un torto a causa dell'azione di un ente pubblico ha diritto di ricorrere al sindacato giurisdizionale, anche chiedendo al giudice di dichiarare illegittime e annullare le azioni, constatazioni e conclusioni dell'ente che risultano arbitrarie o illogiche, viziate da abuso di potere o altrimenti non conformi alla legge ([166]).

(114) Infine, il governo statunitense ha indicato nella FOIA un mezzo con cui il cittadino straniero può chiedere l'accesso ai dati esistenti degli enti federali, anche quando contengono dati personali che lo riguardano ([167]). Data la materia trattata, la FOIA non offre una possibilità di ricorso individuale contro l'ingerenza nei dati personali in sé, ma potrebbe in linea di principio permettere alla persona di accedere alle informazioni al riguardo detenute dagli enti d'intelligence nazionali. Le possibilità paiono comunque limitate anche in quest'ultima ipotesi, perché l'ente può negare l'accesso alle informazioni che rientrano in una serie elencata di eccezioni, tra cui l'accesso alle informazioni classificate in materia di sicurezza nazionale e alle informazioni relative a indagini dei servizi di contrasto ([168]). Detto questo, quando l'ente d'intelligence nazionale applica una di tali eccezioni, la persona può presentare ricorso per via amministrativa e per via giudiziaria.

(115) Pertanto, sebbene la persona, compreso l'interessato dell'UE, sottoposta a sorveglianza (elettronica) illecita per finalità di sicurezza nazionale disponga di una serie di possibilità di ricorso, altrettanto pacifico è che queste non contemplano almeno alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi (ad esempio l'EO 12333). Inoltre, anche quando la possibilità di ricorso per via giudiziaria è effettivamente offerta, in linea di principio, anche al cittadino straniero, come ad esempio in caso di sorveglianza ai sensi della FISA, i motivi per cui si possono adire le vie legali sono limitati ([169]) e l'istanza presentata da una persona (compresi i cittadini statunitensi o residenti negli USA) è dichiarata irricevibile se questa non è in grado di dimostrare la propria legittimazione ad agire ([170]), il che limita di fatto l'accesso al giudice ordinario ([171]).

(116) Per offrire a tutti gli interessati dell'UE un'ulteriore via di ricorso, il governo statunitense ha deciso di creare il nuovo meccanismo di mediazione illustrato nella lettera del segretario di Stato degli USA alla Commissione, riportata nell'allegato III della presente decisione. Benché si fondi sulla nomina in seno al Dipartimento di Stato, ai sensi della PPD-28, di un Primo coordinatore (a livello di Sottosegretario) a referente per i governi stranieri che si pongono interrogativi sulle attività di intelligence dei segnali condotte dagli Stati Uniti d'America, il meccanismo si spinge ben oltre quest'idea che ne è all'origine.

([162]) Codice degli Stati Uniti d'America, titolo 18, articolo 1030.
([163]) Codice degli Stati Uniti d'America, titolo 18, articoli 2701-2712.
([164]) Codice degli Stati Uniti d'America, titolo 12, articolo 3417.
([165]) Dichiarazioni dell'ODNI (allegato VI), pag. 17.
([166]) Codice degli Stati Uniti d'America, titolo 5, articolo 706(2)(A).
([167]) Codice degli Stati Uniti d'America, titolo 5, articolo 552. Leggi analoghe vigono a livello di Stati federati.
([168]) In questo caso, di norma la persona riceve soltanto una risposta standardizzata in cui l'ente si rifiuta di confermare o di smentire l'esistenza dei dati [cfr. *American Civil Liberties Union/CIA*, 710 F.3d 422 (D.C. Cir. 2014)].
([169]) Cfr. dichiarazioni dell'ODNI (allegato VI), pag. 16. Stando alle spiegazioni fornite, i motivi per adire le vie legali implicano l'esistenza di un *danno* (Codice degli Stati Uniti d'America, titolo 18, articolo 2712; Codice degli Stati Uniti d'America, titolo 50, articolo 1810) oppure la dimostrazione del fatto che *il governo intende usare o divulgare le informazioni* ottenute o ricavate dalla sorveglianza elettronica della persona contro questa stessa persona *in un procedimento giudiziario o amministrativo negli Stati Uniti* (Codice degli Stati Uniti d'America, titolo 50, articolo 1806). Tuttavia, come la Corte di giustizia ha più volte rilevato, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (cfr. *Schrems*, punto 89, con ulteriori rimandi).
([170]) Criterio di ricevibilità derivante dal requisito del «caso o controversia» stabilito dalla Corte suprema degli Stati Uniti in applicazione dell'articolo III della Costituzione degli Stati Uniti.
([171]) Cfr. *Clapper/Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). Quanto all'impiego delle *National Security Letter*, a norma della legge USA FREEDOM (articoli 502(f)-503) occorre sottoporre periodicamente a riesame gli obblighi di non divulgazione e informare il *destinatario* dell'NSL se i fatti non giustificano più l'obbligo di non divulgazione (cfr. dichiarazioni dell'ODNI (allegato VI), pag. 13). Questo non garantisce tuttavia che l'interessato dell'UE sia informato del fatto che è stato sottoposto a indagine.

(117) In particolare, stante agli impegni assunti dal governo degli Stati Uniti, il meccanismo di mediazione intende assicurare che ogni reclamo riceva un esame e un trattamento adeguati e che una fonte indipendente confermi alla persona che le leggi degli Stati Uniti sono state rispettate o, se sono state violate, che l'inosservanza è stata nel frattempo sanata ([172]). Il meccanismo comprende il «Mediatore dello scudo», ossia il Sottosegretario e altro personale, e altri organi di vigilanza competenti a controllare i vari servizi della comunità dell'intelligence, sulla cui collaborazione il Mediatore dello scudo fa affidamento per il trattamento dei reclami. In particolare, se il reclamo della persona verte sulla compatibilità della sorveglianza con la legge statunitense, il Mediatore può contare su organi di vigilanza indipendenti dotati di poteri di indagine (quali gli ispettori generali o la PCLOB). In ogni caso il segretario di Stato provvede a che il Mediatore disponga dei mezzi per garantire che la risposta apportata alla richiesta prenda in considerazione tutte le informazioni necessarie.

(118) Questa struttura composita permette al meccanismo di mediazione di garantire una vigilanza indipendente e la possibilità di ricorso individuale. La collaborazione con altri organi di vigilanza assicura altresì l'accesso alle necessarie conoscenze tecniche. Obbligando il Mediatore dello scudo a confermare la conformità o la riparazione dell'inosservanza, il meccanismo rispecchia infine l'impegno del governo statunitense nel suo insieme a trattare i reclami presentati da persone dell'UE e a risolverli.

(119) In primo luogo, a differenza di un meccanismo schiettamente intergovernativo, il Mediatore dello scudo riceve singoli reclami e vi risponde. Il reclamo può essere sporto presso l'autorità di vigilanza che, nello Stato membro, è competente della vigilanza sui servizi di sicurezza nazionali e/o del trattamento dei dati personali da parte delle autorità pubbliche, la quale lo sottopone a un organo centralizzato a livello dell'UE da cui viene poi inoltrato al Mediatore dello scudo ([173]). Questa procedura torna a vantaggio delle persone dell'UE, che possono rivolgersi nella propria lingua a un'autorità nazionale «vicino casa», cui spetta assistere la persona per la trasmissione al Mediatore dello scudo di una richiesta che, riportando le informazioni essenziali, possa essere considerata «completa». La persona non è tenuta a dimostrare che il governo degli USA abbia effettivamente avuto accesso, nell'ambito delle attività di intelligence dei segnali, ai dati personali che la riguardano.

(120) In secondo luogo, il governo degli Stati Uniti s'impegna a garantire che, nell'esercizio delle sue funzioni, il Mediatore dello scudo possa contare sulla collaborazione di altri meccanismi di vigilanza e di controllo della conformità previsti dalla legge statunitense. In alcuni casi, questo implica il coinvolgimento delle autorità nazionali di intelligence, in particolare se la domanda va interpretata come richiesta di accesso a documenti ai sensi della legge sulla libertà d'informazione. In altri, in particolare quando la domanda verte sulla compatibilità della sorveglianza con la legge statunitense, sono coinvolti nella collaborazione organi di vigilanza indipendenti (ad esempio, gli ispettori generali) che hanno la competenza e il potere di svolgere indagini approfondite (in particolare potendo accedere a tutti i documenti pertinenti e esercitando il potere di chiedere informazioni e dichiarazioni) e di risolvere i casi di inosservanza ([174]). Il Mediatore dello scudo ha inoltre facoltà di sottoporre la questione all'esame della PCLOB ([175]). Se uno degli organi di vigilanza riscontra un'inosservanza, il servizio della comunità dell'intelligence responsabile (ad esempio un ente di intelligence) deve porvi rimedio, perché solo così il Mediatore può dare alla persona la risposta «positiva» (ossia che l'inosservanza è stata sanata) cui il governo degli

([172]) Se il reclamante chiede l'accesso a documenti detenuti da un'autorità pubblica statunitense, si applicano le regole e procedure previste dalla legge sulla libertà d'informazione, tra cui la possibilità di rivolgersi, alle condizioni ivi stabilite, all'autorità giudiziaria (piuttosto che a un organo di vigilanza indipendente) in caso di rigetto della domanda.

([173]) In base al meccanismo di mediazione (allegato III), punto 4(f), il Mediatore comunica direttamente con l'organo di trattamento e trasmissione dei reclami presentati da persone dell'UE, cui compete di comunicare a sua volta con la persona che ha presentato la domanda. Le comunicazioni dirette che s'iscrivono nei processi che potrebbero sfociare nella riparazione richiesta (ad esempio, domanda di accesso ai sensi della FOIA, cfr. parte 5) si svolgono secondo le procedure vigenti.

([174]) Cfr. meccanismo di mediazione (allegato III), punto 2(a). Cfr. anche il considerando 0-0.

([175]) Cfr. meccanismo di mediazione (allegato III), punto 2(c). Secondo le spiegazioni trasmesse dal governo degli USA, la PCLOB tiene costantemente sotto controllo le politiche e le procedure (con la relativa attuazione) seguite dalle autorità statunitensi competenti dell'antiterrorismo, per stabilire se «garantiscano una tutela adeguata della vita privata e delle libertà civili e siano conformi alle leggi, ai regolamenti e alle politiche applicabili in materia». Inoltre, «riceve e esamina segnalazioni e altre informazioni dagli addetti alla tutela della vita privata e dagli addetti alle libertà civili, a cui rivolge, se del caso, raccomandazioni riguardo alle attività svolte».

Stati Uniti si è impegnato. Nel quadro della collaborazione il Mediatore dello scudo è altresì informato dell'esito dell'indagine; a tal fine, dispone dei mezzi che gli assicurano di ricevere tutte le informazioni necessarie per elaborare la risposta.

(121) Infine, il Mediatore dello scudo è indipendente dalla comunità dell'intelligence statunitense, quindi svincolato da qualsiasi sua istruzione ([176]). Quest'aspetto riveste grande importanza, dato che il Mediatore deve confermare. i) che il reclamo è stato esaminato adeguatamente; e ii) che è stata rispettata la legge statunitense applicabile, comprese in particolare le limitazioni e le garanzie illustrate nell'allegato VI, oppure, se non è stata rispettata, che l'inosservanza è stata nel frattempo sanata. Per poter dare tale conferma indipendente, il Mediatore deve ricevere le informazioni sull'esame del reclamo che gli sono necessarie per valutare l'accuratezza della risposta. Il segretario di Stato ha assunto l'impegno di assicurare che il Sottosegretario svolga la funzione di Mediatore dello scudo con obiettività e senza indebite ingerenze che possano influire sulla risposta apportata.

(122) Nel complesso, il meccanismo assicura che ciascun caso di reclamo sia esaminato a fondo e risolto e che, almeno relativamente alla sorveglianza, siano coinvolti autorità di vigilanza indipendenti dotate delle competenze tecniche e dei poteri d'indagine necessari e un Mediatore in grado di svolgere le proprie funzioni senza indebite ingerenze, in particolare di ordine politico. Inoltre, la persona può sporgere reclamo senza dover dimostrare di essere stata sottoposta a sorveglianza, e anzi senza dover neppure fornire indicazioni al riguardo ([177]). Alla luce delle caratteristiche descritte la Commissione ritiene che vigano garanzie adeguate ed effettive contro gli abusi.

(123) In base alle considerazioni esposte la Commissione giunge alla conclusione che gli Stati Uniti offrono una tutela giuridica efficace contro le ingerenze delle autorità d'intelligence nei diritti fondamentali della persona i cui dati sono trasferiti dall'Unione agli Stati Uniti nell'ambito dello scudo UE-USA per la privacy.

(124) Al riguardo la Commissione prende atto della sentenza della Corte di giustizia nella causa *Schrems*, secondo cui «una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta» ([178]). La valutazione effettuata dalla Commissione ha confermato la disponibilità di siffatti rimedi giuridici negli Stati Uniti d'America, anche grazie all'introduzione del meccanismo di mediazione, che prevede una vigilanza indipendente corredata di poteri di indagine. La Commissione verifica l'efficacia di detto meccanismo nel quadro del monitoraggio continuo dello scudo, fra l'altro anche tramite l'analisi annuale comune cui parteciperà anche il Mediatore.

3.2. *Accesso e uso da parte delle autorità pubbliche statunitensi per finalità di contrasto e di interesse pubblico*

(125) Relativamente all'ingerenza nei dati personali trasferiti nell'ambito dello scudo UE-USA per la privacy compiuta a fini di applicazione della legge, il governo degli Stati Uniti ha fornito (per il tramite del Dipartimento della Giustizia) rassicurazioni circa le limitazioni e garanzie applicabili; nella valutazione della Commissione queste evidenziano un livello di protezione adeguato.

([176]) Cfr. Corte europea dei diritti dell'uomo (Grande Camera), sentenza del 4 dicembre 2015 nella causa *Roman Zakharov/Russia*, n. 47143/06, punto 275 (secondo cui, benché sia auspicabile, in linea di principio, affidare la vigilanza a un giudice, può essere considerata compatibile con la convenzione la vigilanza esercitata da un organo extragiudiziale, a condizione che sia indipendente dalle autorità che effettuano la sorveglianza e che gli siano conferiti poteri di vigilanza effettivi e sufficienti).

([177]) Cfr. Corte europea dei diritti dell'uomo, sentenza del 18 maggio 2010 nella causa *Kennedy/Regno Unito*, n. 26839/05, punto 167.

([178]) *Schrems*, punto 95. Come risulta dai punti 91 e 96 della sentenza, il punto 95 verte sul livello di protezione garantito dall'ordinamento giuridico dell'Unione, al quale il livello di protezione assicurato nel paese terzo dev'essere «sostanzialmente equivalente». Secondo i punti 73 e 74 della sentenza, questo non implica che il livello di protezione o gli strumenti dei quali il paese terzo si avvale debbano essere identici a quelli dell'UE, ma che gli strumenti debbano cionondimeno rivelarsi efficaci nella prassi.

(126) Stando a dette informazioni, il quarto emendamento della Costituzione degli Stati Uniti ([179]) dispone che le autorità di contrasto possano, in via di principio ([180]), procedere a perquisizioni e sequestri soltanto con un mandato del giudice ottenuto dimostrando una fondata supposizione. Nei pochi casi eccezionali, stabiliti precisamente, in cui il mandato non è necessario ([181]), l'applicazione della legge è subordinata a una prova di «ragionevolezza» ([182]): per stabilire se la perquisizione o il sequestro sia «ragionevole» occorre valutarne, da un lato, il grado di intrusività nella privacy della persona e, dall'altro, il grado di necessità ai fini della promozione degli interessi legittimi del governo ([183]). Su un piano più generale, il quarto emendamento garantisce la privacy e la dignità e tutela dagli atti arbitrari e invasivi degli agenti del governo ([184]). Questi principi rispecchiano i principi di necessità e di proporzionalità del diritto dell'Unione. Quando l'autorità di contrasto non ne ha più bisogno come prove, le cose sequestrate devono essere restituite ([185]).

(127) Sebbene il quarto emendamento non li contempli, i cittadini stranieri che non sono residenti negli Stati Uniti godono comunque, indirettamente, delle tutele che garantisce: poiché i dati personali sono detenuti da imprese statunitensi, in ogni caso le autorità di contrasto devono ottenere l'autorizzazione del giudice (o almeno rispettare il requisito di ragionevolezza) ([186]). Ulteriori tutele sono garantite da poteri particolari conferiti per legge e dagli orientamenti del Dipartimento della Giustizia, che limitano l'accesso delle autorità di contrasto ai dati in base a criteri equivalenti a quelli della necessità e della proporzionalità (ad esempio, imponendo all'FBI di applicare metodi di indagine meno intrusivi possibile, tenendo conto dell'effetto sulla vita privata e sulle libertà civili) ([187]). Secondo le dichiarazioni trasmesse dal governo degli Stati Uniti, tutele equivalenti o superiori vigono per le indagini delle autorità di contrasto a livello di Stati federati (per le indagini svolte a norma di leggi dello Stato federato) ([188]).

(128) Sebbene non in tutti i casi sia necessaria l'autorizzazione giudiziaria preliminare del tribunale o del *grand jury* (ramo investigativo di un tribunale, formato da giurati scelti da un magistrato o giudice) ([189]), la citazione amministrativa è limitata a casi specifici ed è soggetta a sindacato giurisdizionale indipendente, perlomeno nei casi in cui il governo si rivolge al giudice per ottenerne l'esecuzione ([190]).

([179]) Secondo il quarto emendamento, il diritto dei cittadini a godere della sicurezza per quanto riguarda la loro persona, la loro casa, le loro carte e le loro cose, contro perquisizioni e sequestri ingiustificati, non può essere violato; e nessun mandato giudiziario può essere emesso, se non in base a fondate supposizioni, appoggiate da un giuramento o da una dichiarazione sull'onore e con descrizione specifica del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare. Soltanto il (magistrato) giudice può emettere il mandato di perquisizione. I mandati federali relativi alla riproduzione di informazioni conservate su supporto elettronico sono disciplinati anche dalla norma 41 delle norme federali di procedura penale.

([180]) La Corte suprema ha fatto più volte riferimento alle perquisizioni senza mandato come fatto «eccezionale»: cfr., ad esempio, *Johnson/Stati Uniti*, 333 U.S. 10, 14 (1948); *McDonald/Stati Uniti*, 335 U.S. 451, 453 (1948); *Camara/Tribunale municipale*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp./Stati Uniti*, 429 U.S. 338, 352-53, 355 (1977). Nella stessa linea la Corte suprema sottolinea sistematicamente che la norma costituzionale fondante in questa materia è che la perquisizione effettuata al di fuori di una procedura giudiziaria, senza essere stata preliminarmente approvata da un giudice o magistrato, è per sua stessa natura «irragionevole» ai sensi del quarto emendamento, tranne in pochi casi eccezionali stabiliti con precisione e circoscritti. Cfr., ad esempio, *Coolidge/New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp./Stati Uniti*, 429 U.S. 338, 352-53, 358 (1977).

([181]) *City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010).

([182]) PCLOB, Sec. 215 Report, pag. 107, con riferimento a *Maryland/King*, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB, Sec. 215 Report, pag. 107, con riferimento a *Samson/California*, 547 U.S. 843, 848 (2006).

([184]) *City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Cfr., ad esempio, *Stati Uniti/Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Cfr. Corte europea dei diritti dell'uomo (Grande Camera), sentenza del 4.12.2015 nella causa *Roman Zakharov/Russia*, n. 47143/06, punto 269, secondo cui l'obbligo di esibire un'autorizzazione di intercettazione al prestatore di servizi di comunicazione prima di ottenere l'accesso alle comunicazioni della persona è una delle garanzie importanti contro eventuali abusi da parte delle autorità preposte all'applicazione della legge, che assicura l'ottenimento di un'autorizzazione in debita forma in tutti i casi di intercettazione.

([187]) Dichiarazioni del Dipartimento della Giustizia (allegato VII), pag. 4,con ulteriori rimandi.

([188]) Dichiarazioni del Dipartimento della Giustizia (allegato VII), n. 2.

([189]) Stando alle informazioni pervenute alla Commissione e prescindendo da determinati settori verosimilmente irrilevanti per i trasferimenti dei dati nell'ambito dello scudo (ad esempio, frodi mediche, abusi su minori o casi che implicano sostanze controllate), si tratta principalmente di taluni poteri conferiti a norma della legge sulla privacy nelle comunicazioni elettroniche (ECPA): richieste relative alle informazioni di base sull'abbonato, la sessione e la fatturazione (Codice degli Stati Uniti d'America, titolo 18, articolo 2703 (c)(1), (2) — ad esempio indirizzo, durata/tipo del servizio) e richieste relative al contenuto di messaggi di posta elettronica che risalgono a oltre 180 giorni prima [Codice degli Stati Uniti d'America, titolo 18, articolo 2703 (a), (b)]. In quest'ultimo caso, deve tuttavia essere data comunicazione alla persona, che ha quindi la possibilità di contestare la richiesta dinanzi al giudice (cfr. anche il quadro generale in Dipartimento della Giustizia, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3: The Stored Communications Act, pagg. 115-138.

([190]) Secondo le dichiarazioni del governo degli Stati Uniti, il destinatario della citazione amministrativa può contestarla dinanzi al giudice in quanto irragionevole, vale a dire eccessivamente ampia o vessatoria o eccessivamente gravosa Cfr. dichiarazioni dell'DOJ (allegato VII), pag. 2.

(129) Le stesse considerazioni valgono per la citazione amministrativa usata per finalità d'interesse pubblico. Secondo le dichiarazioni del governo statunitense, si applicano limitazioni sostanziali analoghe anche per il fatto che l'ente può chiedere l'accesso soltanto ai dati d'interesse per la materia rientrante nella sua competenza, soddisfacendo sempre il criterio di ragionevolezza.

(130) Quando un'autorità pubblica tratta dati personali, la legge degli Stati Uniti offre alla persona varie vie di ricorso giudiziario nei confronti dell'autorità pubblica stessa o di un suo agente. Fatto salvo il soddisfacimento delle condizioni applicabili, queste vie di ricorso, che comprendono in particolare la legge sulle procedure amministrative (APA), la legge sulla libertà d'informazione (FOIA) e legge sulla privacy nelle comunicazioni elettroniche (ECPA), sono aperte a tutti, indipendentemente dalla cittadinanza.

(131) In generale, a norma delle disposizioni sul sindacato giurisdizionale previste dalla legge sulle procedure amministrative ([191]), chiunque subisca un illecito, un inconveniente o un torto a causa dell'azione di un ente pubblico ha diritto di ricorrere al sindacato giurisdizionale ([192]), anche chiedendo al giudice di dichiarare illegittime e annullare le azioni, constatazioni e conclusioni dell'ente che risultano arbitrarie o illogiche, viziate da abuso di potere o altrimenti non conformi alla legge ([193]).

(132) Più precisamente, instaurando un sistema di diritti alla privacy sanciti per legge, il titolo II della legge sulla privacy nelle comunicazioni elettroniche ([194]) disciplina l'accesso ai contenuti delle comunicazioni orali, via cavo o elettroniche conservati da terzi fornitori di servizi ([195]). Decreta la punibilità dell'accesso illecito (ossia non autorizzato dal giudice o altrimenti permesso) a tali comunicazioni e offre alla persona lesa la possibilità di avviare, contro l'agente del governo che ha volontariamente commesso tale illecito o contro gli Stati Uniti d'America, un'azione civile dinanzi a un giudice federale statunitense per ottenere il risarcimento dei danni effettivi e punitivi e una riparazione equa o dichiarativa.

(133) A norma della legge sulla libertà di informazione (FOIA, Codice degli Stati Uniti d'America, titolo 5, articolo 552), ognuno ha il diritto di accedere ai dati degli enti federali e, esauriti i ricorsi amministrativi, di far valere tale diritto dinanzi al giudice, a meno che tali dati rientrino in un'eccezione che ne impedisce la divulgazione pubblica o in un'esclusione particolare per motivi di applicazione della legge ([196]).

([191]) Codice degli Stati Uniti d'America, titolo 5, articolo 702.

([192]) In generale è soggetta a sindacato giurisdizionale soltanto l'azione finale dell'ente, e non l'azione preliminare, procedurale o intermedia (cfr. Codice degli Stati Uniti d'America, titolo 5, articolo 704).

([193]) Codice degli Stati Uniti d'America, titolo 5, articolo 706(2)(A).

([194]) Codice degli Stati Uniti d'America, titolo 18, articoli 2701-2712.

([195]) La legge sulla privacy nelle comunicazioni elettroniche tutela le comunicazioni detenute da due categorie precise di prestatori di servizi di rete, ossia i prestatori di: i) servizi di comunicazione elettronica, ad esempio telefonia o posta elettronica; e ii) servizi di informatica in remoto, quali archiviazione o trattamento.

([196]) Le esclusioni sono tuttavia circoscritte. A norma del Codice degli Stati Uniti d'America, titolo 5, articolo 552(b)(7), i diritti conferiti dalla FOIA sono preclusi per i dati o le informazioni compilati per finalità di contrasto, ma solo per quanto la comunicazione di tali dati o informazioni: a) possa ragionevolmente comportare un'ingerenza nel procedimento di applicazione della legge; b) privi una persona del diritto a un processo equo o a un giudizio imparziale; c) possa ragionevolmente comportare un'intrusione ingiustificata nella privacy personale; d) possa ragionevolmente comportare la rivelazione dell'identità di una fonte confidenziale, compresi l'ente o autorità statale, locale o estero, ovvero il soggetto privato, che ha fornito informazioni in forma confidenziale e, per i dati o informazioni compilati da un'autorità di contrasto penale nel corso di un'indagine penale o da un ente che conduce un'indagine lecita d'intelligence legata alla sicurezza nazionale, la rivelazione delle informazioni fornite da una fonte confidenziale; e) riveli le tecniche e procedure usate nelle indagini e nei procedimenti giudiziari legati ad attività di contrasto oppure gli orientamenti emanati al riguardo, laddove tale rivelazione possa ragionevolmente comportare un rischio di elusione della legge, oppure f) possa ragionevolmente comportare un rischio per la vita o l'incolumità fisica di una persona. L'ente può inoltre considerare, solo per il periodo in cui la circostanza di esclusione perdura, che i dati sfuggano agli obblighi previsti da detto articolo se la richiesta di accesso riguarda dati per cui è ragionevole supporre che, se comunicati, comportino un'ingerenza nel procedimento di applicazione della legge e se: a) l'indagine o il procedimento implica una possibile violazione di diritto penale, e b) vi è motivo di ritenere che: i) la persona non sia al corrente del fatto che nei suoi confronti è in corso un'indagine o un procedimento; e ii) la rivelazione dell'esistenza dei dati possa ragionevolmente comportare un'ingerenza nel procedimento di applicazione della legge [Codice degli Stati Uniti d'America, titolo 5, articolo 552 (c)(1)].

(134) Varie altre leggi conferiscono alla persona il diritto di agire in giustizia contro un'autorità pubblica o un funzionario pubblico statunitense a motivo del trattamento dei dati personali che la riguardano: legge sulle intercettazioni ([197]), legge sulle frodi e gli abusi informatici ([198]), legge federale sulle rivendicazioni per fatti illeciti ([199]), legge sul diritto alla privacy finanziaria ([200]) e legge sull'informativa corretta nel credito ([201]).

(135) La Commissione giunge pertanto alla conclusione che negli Stati Uniti vigono regole intese a limitare a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato qualsiasi ingerenza per motivi di applicazione della legge ([202]) o altro scopo d'interesse pubblico nei diritti fondamentali della persona i cui dati personali sono trasferiti dall'Unione europea verso gli Stati Uniti nell'ambito dello scudo, e che contro le ingerenze di tale natura esiste una tutela giuridica efficace.

4. LIVELLO DI PROTEZIONE ADEGUATO NELL'AMBITO DELLO SCUDO UE-USA PER LA PRIVACY

(136) Alla luce delle considerazioni che precedono, la Commissione ritiene che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo dall'Unione alle organizzazioni statunitensi che si sono autocertificate come aderenti al regime.

(137) In particolare, la Commissione ritiene che i principi emanati dal Dipartimento del Commercio degli Stati Uniti assicurino nel complesso un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito dai principi fondamentali stabiliti nella direttiva 95/46/CE.

(138) L'effettiva applicazione dei principi è inoltre garantita sia dagli obblighi di trasparenza sia dalla gestione dello scudo da parte del Dipartimento del Commercio.

(139) La Commissione ritiene che, nel complesso, i meccanismi di vigilanza e di ricorso previsti dallo scudo permettano di individuare e punire nella pratica le violazioni dei principi commesse dalle organizzazioni aderenti al regime e offrano all'interessato mezzi di ricorso che gli consentono di accedere ai dati personali che lo riguardano e, in ultima analisi, di ottenerne la rettifica o cancellazione.

(140) In base alle informazioni sull'ordinamento giuridico statunitense disponibili, comprese le dichiarazioni e gli impegni del governo statunitense, la Commissione ritiene che l'ingerenza nei diritti fondamentali della persona i cui dati sono trasferiti dall'Unione verso gli Stati Uniti nell'ambito dello scudo, compiuta dall'autorità pubblica statunitense per esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico, e le conseguenti limitazioni relative al rispetto dei principi imposte alle organizzazioni che si sono autocertificate come aderenti al regime, si limitino a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato e che contro le ingerenze di tale natura esiste una tutela giuridica efficace.

([197]) Codice degli Stati Uniti d'America, titolo 18, articolo 2510 e ss.. A norma della legge sulle intercettazioni (Codice degli Stati Uniti d'America, titolo 18, articolo 2520), la persona la cui comunicazione orale, via cavo o elettronica è intercettata, divulgata o usata intenzionalmente può avviare un'azione civile per violazione di tale legge, in talune circostanze anche contro il singolo funzionario del governo o contro gli Stati Uniti d'America. Per la raccolta delle informazioni sugli indirizzi e di altre informazioni non di contenuto (ad esempio, indirizzo IP, indirizzo del mittente/destinatario del messaggio di posta elettronica), cfr. anche il capitolo relativo ai dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita del titolo 18 (Codice degli Stati Uniti d'America, titolo 18, articoli 3121-3127 e, per l'azione civile, articolo 2707).

([198]) Codice degli Stati Uniti d'America, titolo 18, articolo 1030. A norma della legge sulle frodi e gli abusi informatici, la persona può intentare contro chiunque una causa per accesso intenzionale non autorizzato (o abuso dell'accesso autorizzato) finalizzato a ottenere informazioni da un istituto finanziario, da un sistema informatico del governo statunitense oppure da altro computer determinato, in talune circostanze anche contro il singolo funzionario del governo.

([199]) Codice degli Stati Uniti d'America, titolo 28, articolo 2671 e ss.. A norma della legge federale sulle rivendicazioni per fatti illeciti, in talune circostanze la persona può intentare contro gli Stati Uniti d'America causa per azione o omissione, illecita o dovuta a negligenza, compiuta da un dipendente del governo nell'adempimento della sua funzione o servizio.

([200]) Codice degli Stati Uniti d'America, titolo 12, articolo 3401 e ss. A norma della legge sul diritto alla privacy finanziaria, in talune circostanze la persona può intentare contro gli Stati Uniti d'America causa per acquisizione o divulgazione di dati finanziari protetti, in violazione di tale legge. Al governo è in linea di massima vietato accedere ai dati finanziari protetti, a meno che lo richieda nell'ambito di una citazione o di un mandato di perquisizione legittimi oppure, fatte salve le limitazioni applicabili, presenti per iscritto una richiesta ufficiale, che è notificata alla persona di cui sono chieste le informazioni.

([201]) Codice degli Stati Uniti d'America, titolo 15, articoli 1681-1681x. A norma della legge sull'informativa corretta nel credito, la persona può intentare causa per raccolta, divulgazione e uso di rapporti di credito sui consumatori contro chiunque non rispetti gli obblighi applicabili (in particolare la necessità di autorizzazione legittima) o, in determinate circostanze, contro un ente del governo.

([202]) La Corte di giustizia ha riconosciuto che l'amministrazione della giustizia costituisce un obiettivo politico legittimo — cfr. sentenza *Digital Rights Ireland e a.*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, punto 42; cfr. anche articolo 8, paragrafo 2, della Convenzione europea dei diritti dell'uomo e sentenza della Corte europea dei diritti dell'uomo, *Weber e Saravia c. Germania*, n. 54934/00, punto 104.

(141) La Commissione giunge alla conclusione che sono soddisfatti i criteri dell'articolo 25 della direttiva 95/46/CE, interpretati alla luce della Carta dei diritti fondamentali dell'Unione europea sulla scorta delle delucidazioni apportate dalla Corte di giustizia, in particolare nella sentenza *Schrems*.

5. AZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI E INFORMAZIONE DELLA COMMISSIONE

(142) Nella sentenza *Schrems* la Corte di giustizia ha precisato che la Commissione non ha la competenza di limitare i poteri che le autorità di protezione dei dati traggono dall'articolo 28 della direttiva 95/46/CE (compreso il potere di sospendere il trasferimento dei dati) nel caso in cui una persona, in occasione di una domanda basata su tale disposizione, rimetta in discussione la compatibilità di una decisione della Commissione sull'adeguatezza con la tutela del diritto fondamentale alla protezione della vita privata e dei dati ([203]).

(143) Per permetterle di monitorare con efficacia il funzionamento dello scudo, gli Stati membri dovrebbero informare la Commissione delle azioni pertinenti intraprese dalle autorità di protezione dei dati.

(144) La Corte di giustizia ha inoltre rilevato che, in linea con l'articolo 25, paragrafo 6, secondo comma, della direttiva 95/46/CE, gli Stati membri e i loro organi devono adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, che si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità. Di conseguenza, la decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE è vincolante per tutti gli organi degli Stati membri che ne sono i destinatari, comprese le autorità di controllo indipendenti ([204]). Nell'ipotesi in cui siffatta autorità abbia ricevuto un reclamo che rimette in discussione la conformità di una decisione di adeguatezza della Commissione con la tutela del diritto fondamentale al rispetto della vita privata e alla protezione dei dati e reputi fondate le censure sollevate, la normativa nazionale deve prevedere mezzi di ricorso che le consentano di far valere tali censure dinanzi a un giudice nazionale, il quale, in caso di dubbio, deve sospendere il procedimento e disporre un rinvio pregiudiziale alla Corte di giustizia ([205]).

6. RIESAME PERIODICO DELL'ACCERTAMENTO DI ADEGUATEZZA

(145) Alla luce del fatto che il livello di protezione assicurato dall'ordinamento giuridico statunitense può evolversi, successivamente all'adozione della presente decisione la Commissione verifica periodicamente se le constatazioni relative al livello di protezione assicurato dagli Stati Uniti nell'ambito dello scudo continuino ad essere giustificate in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando la Commissione acquisisce nuove informazioni che fanno sorgere un dubbio giustificato al riguardo ([206]).

(146) La Commissione monitora pertanto su base continuativa il regime complessivo istituito dallo scudo per il trasferimento dei dati personali e la conformità dell'operato delle autorità statunitensi con le dichiarazioni e gli impegni riportati nei documenti allegati alla presente decisione. Per agevolare questo processo, gli Stati Uniti si sono impegnati a informare la Commissione, se pertinenti ai fini dello scudo, degli sviluppi rilevanti della normativa statunitense in materia di tutela dei dati personali e di limitazioni e salvaguardie applicabili all'accesso ai dati personali da parte delle autorità pubbliche. La presente decisione è altresì oggetto di un'analisi annuale comune vertente su tutti gli aspetti del funzionamento dello scudo UE-USA per la privacy, comprese le eccezioni ai principi per motivi di sicurezza nazionale e di amministrazione della giustizia. Poiché sull'accertamento di adeguatezza può influire anche l'evoluzione del diritto dell'Unione, la Commissione valuta il livello di protezione offerto dallo scudo anche una volta entrato in vigore il regolamento generale sulla protezione dei dati.

(147) Ai fini dell'analisi annuale comune di cui agli allegati I, II e VI, la Commissione si riunisce con il Dipartimento del Commercio e la FTC, se del caso accompagnati da altri dipartimenti e enti che intervengono nell'attuazione del regime dello scudo, così come, per le questioni relative alla sicurezza nazionale, rappresentanti dell'ODNI e di altri servizi della comunità dell'intelligence e il Mediatore. Alla riunione possono partecipare le autorità di protezione dei dati dell'UE e rappresentanti del gruppo dell'articolo 29.

([203]) *Schrems*, punti 40 e ss., 101-103.
([204]) *Schrems*, punti 51, 52 e 62.
([205]) *Schrems*, punto 65.
([206]) *Schrems*, punto 76.

(148) In sede di analisi annuale comune la Commissione chiede al Dipartimento del Commercio di comunicare informazioni complete su tutti gli aspetti pertinenti del funzionamento dello scudo, tra cui informazioni sui casi sottopostigli dalle autorità di protezione dei dati e i risultati dei controlli ufficiali della conformità. La Commissione chiede altresì spiegazioni su qualsiasi questione o tema riguardante lo scudo e il relativo funzionamento emerso dalle informazioni disponibili, compresi i rapporti sulla trasparenza consentiti a norma della legge USA FREEDOM, le relazioni pubblicate dalle autorità nazionali di intelligence degli Stati Uniti, le autorità di protezione dei dati, i gruppi che si occupano di privacy, i mezzi di comunicazione o qualsiasi altra fonte. Per agevolarla in questo compito, gli Stati membri dovrebbero informare la Commissione dei casi in cui l'intervento degli organi incaricati di garantire l'osservanza ai principi negli Stati Uniti è risultato vano e di qualsiasi indicazione lasci supporre che l'operato delle autorità pubbliche statunitensi responsabili della sicurezza nazionale o della prevenzione, indagine, accertamento e perseguimento dei reati non assicura il livello di protezione richiesto.

(149) La Commissione elabora, in base all'analisi annuale comune, una relazione da presentare al Parlamento europeo e al Consiglio.

7. **SOSPENSIONE DELLA DECISIONE DI ADEGUATEZZA**

(150) Se, in base alle verifiche o alle altre informazioni disponibili, la Commissione constata che il livello di protezione offerto dallo scudo non può più essere considerato sostanzialmente equivalente a quello dell'Unione, o se vi sono chiare indicazioni del fatto che potrebbe non essere più possibile assicurare negli Stati Uniti l'effettivo rispetto dei principi o che l'operato delle autorità pubbliche statunitensi responsabili della sicurezza nazionale o della prevenzione, indagine, accertamento e perseguimento dei reati non assicura il livello di protezione richiesto, la Commissione ne informa il Dipartimento del Commercio e chiede l'adozione di misure adeguate per risolvere rapidamente, entro un termine stabilito e ragionevole, i potenziali casi di inosservanza dei principi. Se, scaduto il termine stabilito, le autorità statunitensi non hanno dimostrato in modo convincente che lo scudo continua a garantire il rispetto effettivo dei principi e un livello di protezione adeguato, la Commissione avvia la procedura per la sospensione o abrogazione totale o parziale della presente decisione ([207]). In alternativa, la Commissione può proporre di modificare la presente decisione, ad esempio limitando la portata dell'accertamento di adeguatezza ai soli trasferimenti di dati sottoposti a condizioni supplementari.

(151) In particolare, la Commissione avvia la procedura di sospensione o revoca se si verifica una delle ipotesi seguenti:

a) indicazioni del fatto che le autorità statunitensi non rispettano le dichiarazioni e gli impegni riportati nei documenti allegati alla presente decisione, anche relativamente alle condizioni e limitazioni applicabili all'accesso ai dati personali trasferiti nell'ambito dello scudo cui le autorità pubbliche statunitensi hanno proceduto per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico;

b) mancata soluzione efficace dei casi di reclamo presentati da interessati dell'UE; al riguardo la Commissione prende in considerazione tutte le circostanze rilevanti ai fini della possibilità dell'interessato dell'UE di far valere i propri diritti, compreso in particolare l'impegno, assunto volontariamente dall'impresa statunitense che si è autocertificata come aderente allo scudo, di collaborare con le autorità di protezione dei dati e di conformarsi al parere da queste espresso;

c) mancata risposta tempestiva e adeguata del Mediatore dello scudo alle domande presentate dagli interessati dell'UE.

(152) La Commissione vaglia l'ipotesi di avviare la procedura di modifica, sospensione o abrogazione della presente decisione anche se, in sede di analisi annuale comune del funzionamento dello scudo o in altro contesto, il Dipartimento del Commercio o altro dipartimento o ente che interviene nell'attuazione del regime dello scudo, o, per le questioni relative alla sicurezza nazionale, i rappresentanti della comunità dell'intelligence o il Mediatore non comunicano le informazioni o spiegazioni necessarie per valutare il rispetto dei principi, l'efficacia delle procedure di trattamento dei reclami o l'abbassamento del livello di protezione richiesto risultante dall'operato

([207]) A decorrere dalla data di applicazione del regolamento generale sulla protezione dei dati, la Commissione si avvarrà del suo potere di adottare, per imperativi motivi di urgenza debitamente giustificati, un atto di esecuzione che sospende la presente decisione, il quale si applica immediatamente senza dover seguire il pertinente iter di comitatologia e resta in vigore per un periodo non superiore a sei mesi.

delle autorità nazionali di intelligence degli Stati Uniti, in particolare in conseguenza di una raccolta di dati personali e/o a un accesso agli stessi che sono andati al di là di quanto necessario e proporzionato. Al riguardo la Commissione tiene conto della misura in cui le informazioni d'interesse possono essere ottenute da altre fonti, tra cui i rapporti delle società statunitensi autocertificate consentiti dalla legge USA FREEDOM.

(153) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha pubblicato il parere sul livello di protezione offerto dallo scudo UE-USA per privacy ([208]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(154) Il Parlamento europeo ha adottato la risoluzione sui flussi di dati transatlantici ([209]).

(155) Le misure previste dalla presente decisione sono conformi al parere del comitato istituito ai sensi dell'articolo 31, paragrafo 1, della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, gli Stati Uniti d'America assicurano un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo dall'Unione alle organizzazioni statunitensi.

2. Lo scudo UE-USA per la privacy («scudo») è costituito dai principi emanati dal Dipartimento del Commercio degli Stati Uniti il 7 luglio 2016, riportati nell'allegato II, e dalle dichiarazioni e impegni ufficiali riportati nei documenti di cui agli allegati I e da III a VII.

3. Ai fini del paragrafo 1, sono trasferiti nell'ambito dello scudo i dati personali trasferiti dall'Unione a organizzazioni presenti negli Stati Uniti che figurano nell'elenco degli aderenti allo scudo tenuto e pubblicato dal Dipartimento del Commercio degli Stati Uniti in conformità delle parti I e III dei principi enunciati nell'allegato II.

Articolo 2

Ad eccezione dell'articolo 25, paragrafo 1, la presente decisione lascia impregiudicata l'applicazione delle disposizioni della direttiva 95/46/CE relative al trattamento dei dati personali negli Stati membri, in particolare l'articolo 4.

Articolo 3

Lo Stato membro informa senza indugio la Commissione quando, al fine di tutelare le persone con riguardo al trattamento dei loro dati personali, la sua autorità competente esercita i poteri conferitile dall'articolo 28, paragrafo 3, della direttiva 95/46/CE in vista della sospensione o del divieto definitivo del flusso di dati verso un'organizzazione statunitense che figura nell'elenco degli aderenti allo scudo in conformità delle parti I e III dei principi enunciati nell'allegato II.

Articolo 4

1. La Commissione sottopone a monitoraggio continuo il funzionamento dello scudo per verificare se gli Stati Uniti continuino a garantire un livello di protezione adeguato dei dati personali trasferiti in tale ambito dall'Unione verso organizzazioni presenti negli Stati Uniti.

([208]) Parere n. 01/2016 relativo al progetto di decisione sull'adeguatezza del regime dello scudo UE-USA per la privacy, adottato il 13 aprile 2016.
([209]) Risoluzione del Parlamento europeo del 26 maggio 2016 sui flussi di dati transatlantici [2016/2727(RSP)].

2. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui risulta che gli organi del governo degli Stati Uniti cui la legge conferisce il potere di far rispettare i principi enunciati nell'allegato II non mettono a disposizione meccanismi efficaci di rilevamento e di vigilanza che consentano d'individuare le violazioni dei principi e di punirle nella pratica.

3. Gli Stati membri e la Commissione si informano reciprocamente di qualsiasi indicazione del fatto che le ingerenze nel diritto delle persone alla protezione dei dati personali che le riguardano, compiute dalle autorità pubbliche statunitensi competenti della sicurezza nazionale, dell'applicazione della legge o di altro interesse pubblico, vadano oltre quanto strettamente necessario e/o che contro le ingerenze di tale natura non esista una tutela giuridica efficace.

4. Entro un anno dalla data di notifica della presente decisione agli Stati membri e successivamente a cadenza annuale, la Commissione verifica la constatazione enunciata all'articolo 1, paragrafo 1, in base a tutte le informazioni disponibili, comprese quelle ricevute nell'ambito dell'analisi annuale comune di cui agli allegati I, II e VI.

5. La Commissione riferisce tutte le constatazioni pertinenti al comitato istituito a norma dell'articolo 31 della direttiva 95/46/CE.

6. La Commissione presenta, secondo la procedura prevista all'articolo 31, paragrafo 2, della direttiva 95/46/CE, progetti di misure volte a sospendere, modificare o abrogare la presente decisione o a limitarne l'ambito di applicazione, tra l'altro, se si verifica una delle ipotesi seguenti:

— le autorità pubbliche statunitensi non rispettano le dichiarazioni e gli impegni riportati nei documenti allegati alla presente decisione, anche relativamente alle condizioni e limitazioni applicabili all'accesso ai dati personali trasferiti nell'ambito dello scudo cui le autorità pubbliche statunitensi hanno proceduto per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico,

— manca sistematicamente una soluzione efficace dei casi di reclamo presentati da interessati dell'UE,

— manca sistematicamente la risposta tempestiva e adeguata del Mediatore dello scudo alle domande presentate dagli interessati dell'UE prescritta dall'allegato III, punto 4(e).

La Commissione presenta detti progetti di misure anche quando la mancanza di collaborazione da parte degli organi incaricati di assicurare il funzionamento dello scudo negli Stati Uniti le impedisce di stabilire se la constatazione di cui all'articolo 1, paragrafo 1, sia compromessa.

Articolo 5

Gli Stati membri adottano tutte le disposizioni necessarie per conformarsi alla presente decisione.

Articolo 6

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 12 luglio 2016

Per la Commissione
Věra JOUROVÁ
Membro della Commissione

ALLEGATO I

Lettera della segretaria al Commercio degli USA Penny Pritzker

7 luglio 2016

Věra Jourová
Commissaria per la Giustizia, i consumatori e la parità di genere
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissaria Jourová,

mi pregio di trasmetterLe, a nome degli Stati Uniti d'America, la documentazione relativa allo scudo UE-USA per la privacy scaturita dai due anni di proficue discussioni intercorse tra i nostri rispettivi uffici. Assieme al materiale altrimenti accessibile da fonti pubbliche, la documentazione acclusa getta una solida base per un nuovo accertamento di adeguatezza da parte della Commissione europea ([1]).

Abbiamo entrambi di che andare fieri dei miglioramenti apportati al regime: lo scudo per la privacy si fonda su principi che godono di un forte sostegno unanime su entrambe le sponde dell'Atlantico, e noi ne abbiamo rafforzato il funzionamento. Grazie al lavoro compiuto insieme, abbiamo un'effettiva possibilità di migliorare la tutela della vita privata in tutto il mondo.

La documentazione relativa allo scudo per la privacy comprende i principi che lo governano e, nell'allegato 1, una lettera in cui l'Amministrazione del commercio internazionale (ITA) del Dipartimento del Commercio, responsabile della gestione del programma, illustra gli impegni assunti da tale Dipartimento per assicurare l'efficacia di funzionamento dello scudo. Completa la documentazione l'allegato 2, nel quale sono esposti gli ulteriori impegni assunti dal Dipartimento del Commercio circa il nuovo modello arbitrale previsto dallo scudo.

Ho chiesto espressamente al personale del Dipartimento d'impiegare tutte le risorse necessarie per dare un'attuazione rapida e integrale al regime dello scudo per la privacy e per assicurare l'assolvimento tempestivo di tutti gli impegni illustrati negli allegati 1 e 2.

La documentazione relativa allo scudo per la privacy comprende anche i documenti emananti da altre autorità statunitensi di cui segue l'elenco:

— lettera in cui la Commissione federale del Commercio (FTC) descrive le proprie modalità di esecuzione dello scudo,

— lettera in cui il Dipartimento dei Trasporti descrive le proprie modalità di esecuzione dello scudo,

— due lettere dell'Ufficio del direttore dell'intelligence nazionale (ODNI) sulle garanzie e limitazioni applicabili alle autorità di sicurezza nazionale degli USA,

— lettera del Dipartimento di Stato e memorandum di accompagnamento in cui è illustrato l'impegno del Dipartimento di istituire, nel quadro dello scudo per la privacy, la nuova figura del Mediatore, a cui potranno essere rivolte le richieste d'informazioni riguardanti le pratiche di intelligence dei segnali seguite dagli Stati Uniti,

— lettera del Dipartimento della Giustizia sulle garanzie e limitazioni relative all'accesso del governo degli Stati Uniti ai dati per finalità di contrasto e di interesse pubblico.

Mi preme sottolineare la serietà con cui gli Stati Uniti d'America tengono conto di questi impegni.

([1]) Se la decisione della Commissione europea sull'adeguatezza della tutela offerta dallo scudo UE-USA per la privacy si applicherà anche a Islanda, Liechtenstein e Norvegia, la presente documentazione riguarderà anche tali tre paesi oltre all'Unione europea.

Entro 30 giorni dall'approvazione definitiva della decisione sull'adeguatezza, la documentazione integrale relativa allo scudo per la privacy sarà trasmessa al Registro federale per la pubblicazione.

Il Dipartimento del Commercio attende con interesse di collaborare con la Commissione europea quando lo scudo sarà attuato e quando, insieme, passeremo alla fase successiva di questo processo.

La prego di accogliere, signora Commissaria,
i sensi della mia più alta stima.

Penny Pritzker

Allegato 1

Lettera del Sottosegretario al Commercio internazionale ad interim Ken Hyatt

Věra Jourová
Commissaria per la Giustizia, i consumatori e la parità di genere
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissaria Jourová,

mi pregio di illustrare, a norme dell'Amministrazione del commercio internazionale, la protezione rafforzata dei dati personali offerta dal regime dello scudo UE-USA per la privacy («scudo» o «regime») e gli impegni assunti dal Dipartimento del Commercio («Dipartimento») per assicurare l'efficacia di funzionamento dello scudo. La conclusione di quest'accordo storico rappresenta un grande risultato per la tutela della vita privata e per le imprese di entrambe le sponde dell'Atlantico. Nelle persone fisiche («persone») dell'UE infonde fiducia circa la protezione dei dati che le riguardano e la disponibilità di mezzi di ricorso per risolvere gli eventuali casi problematici. La certezza che offre contribuirà a far crescere l'economia transatlantica permettendo a migliaia di imprese europee e statunitensi di continuare a investire e fare impresa attraverso le nostre frontiere. Lo scudo è il risultato di oltre due anni di lavoro intenso che ci hanno visto collaborare coi colleghi della Commissione europea («Commissione»), con la quale attendiamo con interesse di continuare la collaborazione per assicurare che lo scudo funzioni come previsto.

Abbiamo lavorato con la Commissione allo sviluppo dello scudo per permettere alle organizzazioni stabilite negli Stati Uniti di soddisfare i requisiti di adeguatezza previsti dal diritto dell'UE in materia di protezione dei dati. Il nuovo regime recherà numerosi e rilevanti benefici alle persone e alle imprese. In primo luogo, alle persone dell'UE offre un insieme importante di tutele circa la privacy dei dati: impone infatti alle organizzazioni statunitensi aderenti di stabilire una politica di tutela della vita privata conforme al regime, di impegnarsi pubblicamente a rispettare i principi dello scudo in modo che l'impegno assunto sia azionabile in virtù della legge statunitense, di ricertificare ogni anno al Dipartimento la conformità al regime, di mettere a disposizione delle persone dell'UE, a titolo gratuito, un meccanismo indipendente di composizione delle controversie e di assoggettarsi all'autorità della Commissione federale del Commercio (FTC), del Dipartimento dei Trasporti (DOT) o di altro ente competente. In secondo luogo, lo scudo permetterà a migliaia di imprese negli Stati Uniti, e di filiali di imprese europee negli Stati Uniti, di ricevere dati personali dall'Unione europea, facilitando i flussi di dati a sostegno del commercio transatlantico. Le relazioni economiche transatlantiche vantano già il volume più grande del mondo, implicando la metà della produzione economica mondiale e quasi mille miliardi di dollari in scambi di beni e servizi, a sostegno di milioni di posti di lavoro su entrambe le sponde dell'Atlantico. Le imprese che fanno affidamento sui flussi di dati transatlantici rappresentano tutti i comparti industriali e comprendono sia grandi imprese citate in Fortune 500 sia numerose piccole e medie imprese (PMI). Grazie ai flussi di dati transatlantici le organizzazioni statunitensi sono in grado di elaborare i dati necessari per offrire beni, servizi e possibilità di lavoro agli europei. Lo scudo offre supporto ai principi condivisi sulla tutela della vita privata venendo a colmare le differenze tra l'impostazione giuridica europea e quella statunitense e favorendo nel contempo il conseguimento di obiettivi commerciali ed economici per le due parti.

Sebbene l'autocertificazione di conformità al nuovo regime sia per le imprese una decisione facoltativa, una volta che l'impresa si vincola pubblicamente allo scudo, l'impegno assunto diventa azionabile, in virtù della legge statunitense, dalla Commissione federale del Commercio o dal Dipartimento dei Trasporti, a seconda che l'organizzazione aderente allo scudo sia subordinata all'autorità dell'una o dell'altro.

Miglioramenti introdotti dallo scudo

Lo scudo rafforza la tutela della vita privata in vari modi:

— prevedendo, nel principio sull'informativa, di comunicare alle persone informazioni aggiuntive, comprese la dichiarazione in cui l'organizzazione attesta l'adesione allo scudo, la dichiarazione che afferma il diritto della persona di accedere ai dati personali e l'indicazione del competente organo indipendente di composizione delle controversie,

— aumentando la protezione dei dati personali che l'organizzazione aderente allo scudo trasmette a un terzo titolare del trattamento, tramite l'obbligo per le parti di concludere un contratto in base al quale tali dati possono essere trattati solo per finalità determinate e limitate, conformemente al consenso dato dalla persona, e il destinatario offre lo stesso livello di protezione previsto dai principi,

— aumentando la protezione dei dati personali che un'organizzazione aderente allo scudo trasmette a un terzo procuratore, anche imponendo all'organizzazione di: adottare provvedimenti ragionevoli e adeguati per garantire che, in concreto, il procuratore tratti le informazioni personali che gli sono trasmesse in modo conforme agli obblighi cui i principi vincolano l'organizzazione; non appena avvertita, adottare misure ragionevoli e adeguate per far cessare il trattamento non autorizzato e porvi rimedio; a richiesta del Dipartimento, fornirgli un sunto o un estratto rappresentativo delle pertinenti disposizioni sulla tutela della vita privata contenute nel contratto concluso con il procuratore,

— prevedendo che l'organizzazione aderente allo scudo sia responsabile del trattamento delle informazioni personali ricevute in tale ambito e inoltrate a un terzo che agisce come suo procuratore, e che, in base ai principi, resti responsabile qualora il procuratore tratti le informazioni personali in modo non conforme ai principi, salvo se l'organizzazione è in grado di dimostrare la sua estraneità all'evento che ha causato il danno,

— precisando che le organizzazioni aderenti allo scudo devono limitare le informazioni personali ai dati d'interesse ai fini del trattamento,

— imponendo all'organizzazione che esce dallo scudo e sceglie di conservare i dati ricevuti mentre vi aderiva di certificare ogni anno al Dipartimento l'impegno di applicare i principi ai dati ricevuti nel periodo dell'adesione,

— prevedendo di mettere a disposizione delle persone, a titolo gratuito, meccanismi di ricorso indipendenti,

— imponendo alle organizzazioni e ai rispettivi meccanismi di ricorso indipendenti di rispondere prontamente alle richieste del Dipartimento vertenti su informazioni relative allo scudo,

— imponendo alle organizzazioni di rispondere in tempi rapidi ai reclami sul rispetto dei principi inoltrati da autorità degli Stati membri dell'UE per il tramite del Dipartimento,

— imponendo all'organizzazione aderente allo scudo alla quale è contestata un'inosservanza dei principi, tramite un ordine emesso dall'FTC o da un giudice, di rendere pubbliche le parti inerenti allo scudo delle relazioni di conformità o di valutazione presentate all'FTC.

Gestione e supervisione del programma «Scudo per la privacy» da parte del Dipartimento del Commercio

Il Dipartimento ribadisce l'impegno a tenere e mettere a disposizione del pubblico un elenco ufficiale delle organizzazioni statunitensi che si sono autocertificate presso di esso impegnandosi a rispettare i principi dello scudo («elenco degli aderenti allo scudo» o «elenco»). Il Dipartimento tiene aggiornato l'elenco depennando le organizzazioni che abbandonano volontariamente il programma o che non completano le procedure per la ricertificazione annuale presso di esso o per le quali si sono riscontrate reiterate inosservanze dei principi. Il Dipartimento tiene e mette a disposizione del pubblico anche un elenco ufficiale delle organizzazioni statunitensi che si erano autocertificate presso di esso ma che sono state depennate dall'elenco, comprese quelle depennate per reiterate inosservanze dei principi. Per ciascuna organizzazione depennata dall'elenco il Dipartimento indica il motivo che ne ha determinato l'esclusione.

Il Dipartimento s'impegna a rafforzare la gestione e la supervisione dello scudo, in particolare attuando quanto segue.

Informazioni supplementari sul sito web dello scudo

— Tenuta dell'elenco degli aderenti allo scudo e di un registro delle organizzazioni che si erano precedentemente autocertificate impegnandosi a rispettare i principi, ma che non possono più contare sui benefici derivanti dallo scudo

— Dichiarazione posta in evidenza in cui è precisato che tutte le organizzazioni depennate dall'elenco non possono più contare sui benefici derivanti dallo scudo, ma che devono comunque continuare ad applicare i principi alle informazioni personali ricevute quando vi aderivano, fintantoché le conserveranno

— Collegamento ipertestuale all'elenco dei casi inerenti allo scudo avviati dall'FTC e caricati sul suo sito web.

Verifica del soddisfacimento dei requisiti per l'autocertificazione

— Prima di perfezionare l'autocertificazione (o la ricertificazione annuale) di un'organizzazione e inserire questa nell'elenco, verifica del fatto che l'organizzazione:

  — abbia comunicato le necessarie informazioni di contatto,

  — abbia descritto le attività svolte in rapporto alle informazioni personali pervenute dall'UE,

  — abbia indicato le informazioni personali contemplate dall'autocertificazione,

  — se dispone di un sito web pubblico, abbia indicato l'indirizzo Internet al quale è consultabile la politica della privacy seguita, e tale politica sia effettivamente accessibile all'indirizzo indicato; in alternativa, se non dispone di un sito web pubblico, abbia indicato il luogo in cui il pubblico può prendere visione della politica della privacy seguita,

  — abbia inserito nella politica della privacy una dichiarazione che afferma l'adesione ai principi e, se tale politica è consultabile in rete, un collegamento ipertestuale al sito web del Dipartimento dedicato allo scudo,

  — abbia indicato lo specifico organo competente per legge a conoscere delle azioni intentate contro l'organizzazione per possibili pratiche sleali o ingannevoli e violazioni di leggi o regolamenti che disciplinano la tutela della vita privata (ferma restando l'elencazione nei principi o in un futuro allegato ai principi),

  — se sceglie di conformarsi ai requisiti del principio su ricorso, controllo e responsabilità, lettera a), punti i) e iii), impegnandosi a collaborare con le competenti autorità di protezione dei dati dell'UE, abbia manifestato l'intenzione di collaborare con esse per istruire e dirimere i reclami presentati nell'ambito dello scudo, segnatamente rispondendo alle loro richieste d'informazioni nei casi in cui gli interessati dell'UE hanno presentato il reclamo direttamente all'autorità di protezione dei dati del proprio paese,

  — abbia indicato i programmi sulla privacy di cui è membro,

  — abbia indicato il metodo con cui verifica la conformità ai principi (ad esempio, verifica interna o verifica a opera di terzi),

  — abbia indicato, sia nell'autocertificazione presentata sia nella politica della privacy, il meccanismo di ricorso indipendente disponibile per istruire e dirimere i reclami,

  — abbia inserito nella pertinente politica della privacy, se disponibile online, un collegamento ipertestuale al sito web o al modulo di presentazione del reclamo del meccanismo di ricorso indipendente disponibile per l'istruzione dei casi irrisolti di reclamo,

  — se ha manifestato l'intenzione di ricevere informazioni sulle risorse umane trasmesse dall'UE per usarle nel contesto del rapporto di lavoro, si sia impegnata a collaborare con le autorità di protezione dei dati, e a conformarsi alle loro regole, per dirimere i reclami legati alle sue attività relative a tali dati, abbia trasmesso al Dipartimento copia della propria politica della privacy relativamente alle risorse umane e abbia comunicato il luogo in cui i dipendenti interessati possono prendere visione di detta politica.

— Collaborazione con i meccanismi di ricorso indipendenti per verificare che, laddove sia richiesta la registrazione, le organizzazioni si siano effettivamente registrate presso il meccanismo indicato nell'autocertificazione presentata.

Maggiori sforzi nei confronti delle organizzazioni depennate dall'elenco degli aderenti allo scudo

— Comunicazione alle organizzazioni depennate dall'elenco per «reiterate inosservanze dei principi» del fatto che non hanno diritto a conservare le informazioni raccolte nell'ambito dello scudo.

— Invio di questionari alle organizzazioni la cui autocertificazione è in scadenza o che si sono ritirate volontariamente dallo scudo per verificare se l'organizzazione intenda restituire o cancellare le informazioni personali ricevute quando aderiva al regime ovvero continuare ad applicare loro i principi dello scudo e, se le informazioni personali sono conservate, per verificare chi, all'interno dell'organizzazione, funge da referente permanente per le questioni relative allo scudo.

Reperimento dei casi di millantata adesione e loro soluzione

— Esame delle politiche della privacy delle organizzazioni che precedentemente aderivano allo scudo ma che ne sono state rimosse, per reperire gli eventuali casi di millantata adesione.

— Se un'organizzazione a) si ritira dal regime, b) non ricertifica l'adesione ai relativi principi o c) è estromessa dallo scudo per, in particolare, «reiterate inosservanze dei principi», verifica ufficiale continuativa per controllare che l'organizzazione abbia eliminato, dalle pertinenti pubblicazioni della sua politica della privacy, qualsiasi riferimento allo scudo che lasci intendere che l'organizzazione continua ad aderirvi attivamente e a godere dei benefici che ne derivano. Se accerta che i riferimenti non sono stati eliminati, il Dipartimento avverte l'organizzazione del fatto che, se continuerà a millantare la certificazione allo scudo, la questione sarà sottoposta all'ente competente per un'eventuale azione coercitiva. Se l'organizzazione non elimina i riferimenti né si autocertifica conforme allo scudo, il Dipartimento investe ufficialmente della questione la FTC, il DOT o altro ente competente oppure, se opportuno, interviene per garantire il rispetto del marchio di certificazione legato allo scudo per la privacy.

— Ulteriori iniziative per individuare i casi di millantata adesione allo scudo e di uso improprio del relativo marchio, anche tramite ricerche su Internet per verificare se le politiche della privacy dell'organizzazione raffigurino tale marchio o facciano riferimento allo scudo.

— Soluzione in tempi rapidi dei problemi riscontrati in sede di controllo ufficiale dei casi di millantata adesione e di uso improprio del marchio di certificazione, anche tramite avvertimenti alle organizzazioni che millantano l'adesione al programma dello scudo come sopra descritto.

— Adozione delle altre misure correttive del caso, anche portando avanti i ricorsi legali che il Dipartimento è autorizzato a promuovere e sottoponendo la questione alla FTC, al DOT o ad altro ente competente.

— Esame e trattamento in tempi rapidi dei reclami ricevuti circa la millantata adesione al regime.

Il Dipartimento riesamina le politiche della privacy delle organizzazioni alla ricerca di una maggiore efficacia nell'individuazione dei casi di millantata adesione allo scudo e nella loro soluzione. In particolare, il servizio rivede le politiche della privacy delle organizzazioni cui è scaduta l'autocertificazione perché non hanno ricertificato l'adesione ai principi, verificando che esse abbiano eliminato, dalle pertinenti pubblicazioni della loro politica della privacy, qualsiasi riferimento allo scudo che lasci intendere che l'organizzazione continua ad aderirvi attivamente. Grazie al riesame sono individuate le organizzazioni che non hanno eliminato tali riferimenti, le quali sono avvertite, con lettera dell'Ufficio legale del Dipartimento, della possibilità di azioni coercitive in caso di mancata eliminazione dei riferimenti. Il Dipartimento continua a seguire la questione accertandosi che l'organizzazione elimini i riferimenti indebiti oppure ricertifichi l'adesione ai principi. S'impegnerà altresì per individuare i casi di millantata adesione allo scudo da parte di organizzazioni che non hanno mai partecipato al programma, adottando nei loro confronti analoghi provvedimenti correttivi.

Controlli ufficiali periodici della conformità e valutazioni del programma

— Controllo continuativo della conformità effettiva, anche tramite l'invio di questionari particolareggiati alle organizzazioni aderenti, per individuare le questioni che potrebbe essere utile approfondire. È effettuato tale controllo della conformità, in particolare, quando: a) il Dipartimento ha ricevuto reclami specifici e non futili circa l'osservanza dei principi da parte dell'organizzazione, b) l'organizzazione non risponde esaurientemente alle richieste con cui il Dipartimento domanda informazioni sullo scudo oppure c) prove credibili indicano che l'organizzazione non rispetta gli impegni assunti con lo scudo. Ove opportuno, il Dipartimento consulta le competenti autorità di protezione dei dati circa tali controlli della conformità.

— Valutazione periodica della gestione e supervisione del programma dello scudo affinché le attività di controllo risultino atte ad affrontare i nuovi problemi via via che si pongono.

Il Dipartimento ha aumentato le risorse assegnate alla gestione e supervisione del programma dello scudo, tra l'altro raddoppiando il personale, e continuerà a impiegare in tali attività risorse adeguate per garantire un controllo e una gestione efficaci del programma.

Un sito web dello scudo ritagliato su gruppi di destinatari

Il Dipartimento mira il sito web dello scudo concentrandolo su tre gruppi di destinatari: persone fisiche dell'UE, imprese dell'UE e imprese statunitensi. L'inserimento di documentazione mirata direttamente alle persone fisiche e imprese dell'UE favorisce la trasparenza in vari modi. Alle persone fisiche dell'UE illustra chiaramente: 1) i diritti che lo scudo conferisce loro; 2) i meccanismi di ricorso di cui dispongono qualora ritengano che un'organizzazione sia venuta meno all'impegno di attenersi ai principi; 3) in che modo reperire informazioni sull'autocertificazione con cui l'organizzazione si è vincolata allo scudo. Alle imprese dell'UE rende più agevole verificare: 1) se l'organizzazione gode dei benefici dello scudo; 2) il tipo di informazioni contemplate dall'autocertificazione con cui l'organizzazione si è vincolata allo scudo; 3) la politica della privacy che si applica alle informazioni contemplate; 4) il metodo con cui l'organizzazione si accerta di rispettare i principi.

Maggiore collaborazione con le autorità di protezione dei dati

Per aumentare le possibilità di collaborazione con le autorità di protezione dei dati, il Dipartimento nomina al suo interno un referente incaricato dei collegamenti con tali autorità. Se reputa che una data organizzazione non rispetti i principi, anche a seguito del reclamo da parte di una persona dell'UE, l'autorità di protezione dei dati può chiedere al referente istituito presso il Dipartimento di esaminare più a fondo la situazione. Al referente sono segnalate anche le organizzazioni che millantano di partecipare allo scudo pur non essendosi mai autocertificate come aderenti ai principi. Il referente assiste le autorità di protezione dei dati che chiedono informazioni sull'autocertificazione o sulla precedente partecipazione di una data organizzazione al programma e risponde alle loro domande circa l'attuazione di specifici obblighi collegati allo scudo. Ai fini di una maggiore trasparenza nei confronti delle persone e imprese dell'UE, il Dipartimento fornisce inoltre alle autorità di protezione dei dati documentazione sullo scudo da caricare sui loro siti web. Grazie alla sensibilizzazione sullo scudo e sui diritti e responsabilità che comporta, dovrebbe risultare più facile individuare i problemi via via che si pongono, in modo da poterli affrontare in modo adeguato.

Agevolazione della risoluzione dei casi di reclamo per inosservanza dei principi

Il Dipartimento riceve, per il tramite del referente, i reclami sottopostigli da un'autorità di protezione dei dati nei quali si sostiene che una data organizzazione vincolata dallo scudo non ne rispetta i principi. Il Dipartimento si impegna al massimo con l'organizzazione per favorire la soluzione del caso di reclamo. Entro 90 giorni dal ricevimento del reclamo, il Dipartimento aggiorna sulla situazione l'autorità di protezione dei dati. Al fine di agevolare la presentazione dei reclami il Dipartimento redige per le autorità di protezione dei dati un modulo da compilare e trasmettere al referente. Il referente tiene traccia di tutti casi sottoposti al Dipartimento dalle autorità di protezione dei dati; nell'analisi annuale illustrata *infra*, il Dipartimento include un'analisi aggregata dei reclami ricevuti ogni anno.

Adozione di procedure arbitrali e scelta degli arbitri in consultazione con la Commissione

Il Dipartimento assolve gli impegni previsti all'allegato I e pubblica le relative procedure una volta raggiunto un accordo.

Meccanismo di riesame comune del funzionamento dello scudo

Il Dipartimento del Commercio, la FTC e gli altri enti interessati si riuniscono a cadenza annuale con la Commissione, le autorità di protezione dei dati interessate e i pertinenti rappresentanti del gruppo dell'articolo 29; in tali riunioni il Dipartimento espone la situazione aggiornata del programma dello scudo. Nelle riunioni annuali si discutono le questioni correnti collegate al funzionamento, attuazione, controllo ed esecuzione dello scudo, compresi i casi che le autorità di protezione dei dati hanno sottoposto al Dipartimento e i risultati dei controlli ufficiali della conformità; possono essere discusse anche le opportune modifiche della legge. Secondo il caso, il primo riesame annuale e quelli successivi comprendono un dialogo su altri temi, ad esempio il processo decisionale automatizzato, toccando anche gli aspetti relativi alle analogie e alle differenze d'impostazione tra l'UE e gli USA.

Aggiornamenti normativi

Il Dipartimento si adopera in ogni modo ragionevole per informare la Commissione, se pertinenti ai fini dello scudo, degli sviluppi rilevanti della normativa statunitense in materia di tutela dei dati personali e di limitazioni e salvaguardie applicabili all'accesso ai dati personali da parte delle autorità statunitensi e al loro uso successivo.

Eccezione per motivi di sicurezza nazionale

Per quanto riguarda le limitazioni che gravano sull'osservanza dei principi dello scudo per motivi di sicurezza nazionale, Robert Litt, Giureconsulto dell'Ufficio del direttore dell'intelligence nazionale, ha inviato a Justin Antonipillai e a Ted Dean del Dipartimento del Commercio due lettere, di cui Le è stata trasmessa copia. Le lettere espongono in modo approfondito, tra l'altro, le politiche, le garanzie e le limitazioni che si applicano alle attività di intelligence dei segnali condotte dagli Stati Uniti d'America e la trasparenza cui si attiene la comunità dell'intelligence statunitense al riguardo. Considerato che la Commissione sta valutando il regime dello scudo per la privacy, le informazioni contenute in tali lettere permettono di concludere che esso funzionerà in maniera adeguata secondo i principi in esso previsti. Prendiamo atto che, per informare l'analisi annuale del regime dello scudo, la Commissione potrà usare in futuro, tra l'altro, informazioni che la comunità dell'intelligence ha divulgato al pubblico.

Alla luce dei principi dello scudo e delle lettere e documentazione di accompagnamento, compresi gli impegni assunti dal Dipartimento circa la gestione e la supervisione del regime, il Dipartimento confida che la Commissione giungerà alla conclusione che il regime dello scudo UE-USA per la privacy offre una protezione consona ai requisiti del diritto dell'Unione e che sarà possibile quindi proseguire il trasferimento dei dati dall'Unione europea alle organizzazioni aderenti allo scudo.

La prego di accogliere, signora Commissaria,
i sensi della mia più alta stima.

Ken Hyatt

Allegato 2

Modello arbitrale

ALLEGATO I

Il presente allegato I stabilisce le condizioni alle quali l'organizzazione aderente allo scudo è tenuta a sottoporre il reclamo a procedimento arbitrale in virtù del principio su ricorso, controllo e responsabilità. La possibilità di arbitrato vincolante illustrata qui di seguito si applica a talune rivendicazioni accessorie relativamente ai dati contemplati dal regime dello scudo UE-USA per la privacy («scudo» o «regime»). L'obiettivo è mettere a disposizione della persona che opta per questa possibilità un meccanismo celere, indipendente e equo per dirimere il caso di asserita violazione dei principi rimasto irrisolto dopo il ricorso agli altri (eventuali) meccanismi previsti dallo scudo.

A. **Ambito di applicazione**

È messa a disposizione della persona la possibilità di ricorrere all'arbitrato per accertare, quanto alle rivendicazioni accessorie, se l'organizzazione aderente allo scudo abbia violato nei suoi confronti gli obblighi derivanti dai principi e se l'eventuale violazione non sia stata ancora riparata in tutto o in parte. Questa possibilità è prevista soltanto per detti fini: non è, ad esempio, percorribile per le eccezioni ai principi ([1]) o per le denunce vertenti sull'adeguatezza dello scudo.

B. **Forme di riparazione disponibili**

In questo contesto il collegio arbitrale dello scudo (composto da uno o da tre arbitri, secondo quanto concordato dalle parti) ha il potere di imporre un provvedimento equo, specifico alla persona e di carattere non pecuniario (quali accesso, rettifica, cancellazione o restituzione dei dati che la riguardano) a titolo di riparazione per la violazione dei principi limitatamente alla persona in questione. Sono questi i soli poteri del collegio arbitrale in tema di riparazioni. Nel valutare le riparazioni possibili, il collegio arbitrale è tenuto a tenere conto delle altre riparazioni già disposte da altri meccanismi nell'ambito dello scudo. Risarcimento danni, costi, commissioni o altre riparazioni non sono ammessi. Ciascuna parte sopporta le proprie spese di assistenza legale.

C. **Obblighi in fase prearbitrale**

Prima di avviare l'azione arbitrale la persona che opta per questa possibilità è tenuta a: 1) sottoporre la questione della presunta violazione all'organizzazione dandole la possibilità di risolverla nei tempi indicati nella parte III, punto 11, lettera d), punto i), dei principi; 2) rivolgersi al meccanismo di ricorso indipendente previsto dai principi, procedura che è gratuita per la persona; 3) per il tramite dell'autorità di protezione dei dati del proprio paese, sottoporre la questione al Dipartimento del Commercio dandogli la possibilità di adoperarsi per risolverla nei tempi indicati nella lettera dell'Amministrazione del commercio internazionale del Dipartimento del Commercio, procedura che è gratuita per la persona.

L'arbitrato non è una possibilità percorribile se la stessa violazione dei principi denunciata dalla stessa persona 1) è stata già sottoposta a arbitrato vincolante, 2) è stata oggetto di una decisione definitiva scaturita da un procedimento giudiziario in cui la persona era una delle parti oppure 3) è stata in passato oggetto di una transazione tra le parti. Non è percorribile neppure se un'autorità di protezione dei dati dell'UE 1) è competente in base alla parte III, punto 5, o punto 9, dei principi oppure 2) ha il potere di dirimere la presunta violazione direttamente con l'organizzazione. Il fatto che l'autorità di protezione dei dati abbia il potere di risolvere lo stesso caso di reclamo nei confronti di un titolare del trattamento dell'UE non preclude di per sé la soluzione arbitrale nei confronti di un soggetto giuridico diverso che non dipende da detta autorità.

D. **Carattere vincolante delle decisioni**

La decisione della persona di chiedere l'arbitrato vincolante è totalmente volontaria. La decisione arbitrale è vincolante per tutte le parti dell'arbitrato. Optando per l'arbitrato la persona rinuncia alla possibilità di chiedere in altra sede riparazione per l'asserita violazione; tuttavia, se il provvedimento equo di carattere non pecuniario non costituisce una riparazione integrale dell'asserita violazione, il ricorso all'arbitrato non preclude alla persona la possibilità di avviare l'azione di risarcimento danni altrimenti ammessa in sede giudiziaria.

([1]) Parte I, punto 5, dei principi.

E. **Riesame e esecuzione**

Ai sensi della legge federale sull'arbitrato, la persona e l'organizzazione aderente allo scudo possono sottoporre la decisione arbitrale al riesame e all'esecuzione in sede giudiziaria previsti dalla legge statunitense ([1]). L'istanza in tal senso deve essere presentata al giudice distrettuale federale con competenza territoriale sul luogo in cui si trova il centro di attività principale dell'organizzazione aderente allo scudo.

Scopo della possibilità di arbitrato è comporre singole controversie; le decisioni arbitrali non sono intese a costituire un precedente probante o vincolante per i casi che coinvolgono altre parti, compreso per i procedimenti arbitrali futuri, per i giudici dell'UE o degli USA e per i procedimenti dell'FTC.

F. **Collegio arbitrale**

Le parti scelgono gli arbitri dall'elenco di arbitri qui descritto.

In linea con la normativa vigente, il Dipartimento del Commercio degli Stati Uniti e la Commissione europea stilano un elenco di almeno 20 arbitri, scelti sulla base dell'indipendenza, dell'integrità e della competenza, tenuto conto dei criteri esposti qui di seguito.

L'arbitro:

1) rimane nell'elenco, salvo circostanza eccezionale o valido motivo, per un periodo di 3 anni rinnovabile per altri 3;

2) non riceve istruzioni da nessuna delle parti, da nessuna organizzazione aderente allo scudo né dagli Stati Uniti d'America, dall'UE o da uno Stato membro dell'UE, così come da nessun'altra autorità pubblica o autorità di esecuzione, né è associato a nessuno di tali soggetti;

3) è abilitato a esercitare la professione forense negli Stati Uniti d'America ed è esperto di diritto della privacy statunitense con competenze in materia di normativa dell'UE sulla protezione dei dati.

G. **Procedure arbitrali**

In linea con la normativa applicabile, entro 6 mesi dall'adozione della decisione di adeguatezza il Dipartimento del Commercio e la Commissione europea concordano l'adozione di una serie esistente e consolidata di procedure arbitrali statunitensi (quali AAA o JAMS) per disciplinare il procedimento dinanzi al collegio arbitrale dello scudo, ferme restando tutte le considerazioni esposte qui di seguito.

1. Dopo aver obbligatoriamente assolto i citati obblighi della fase prearbitrale, la persona può avviare l'arbitrato vincolante trasmettendo un «avviso» all'organizzazione. L'avviso riporta una sintesi delle misure adottate conformemente alla lettera C per risolvere il caso, una descrizione della presunta violazione e, a scelta della persona, documentazione di supporto e/o l'esposizione delle ragioni di diritto relative alla contestazione.

([1]) Ai sensi della legge federale sull'arbitrato, capo 2, la convenzione arbitrale o il lodo arbitrale scaturito da un rapporto giuridico, contrattuale o no, che è considerato commerciale, compresi l'operazione, il contratto o la convenzione di cui all'articolo 2 della legge federale sull'arbitrato, rientra nella convenzione, del 10 giugno 1958, per il riconoscimento e l'esecuzione delle sentenze arbitrali straniere («convenzione di New York») (21 U.S.T. 2519, T.I.A.S. n. 6997) (Codice degli Stati Uniti d'America, titolo 9, articolo 202). La legge federale sull'arbitrato dispone inoltre che la convenzione o il lodo scaturito da un siffatto rapporto in cui sono coinvolti esclusivamente cittadini statunitensi rientri nella convenzione di New York solo se il rapporto interessa beni ubicati all'estero, prevede l'esecuzione all'estero o presenta altrimenti un ragionevole legame con uno o più Stati esteri (*Ibid.*). A norma del capo 2, ciascuna parte dell'arbitrato può adire il giudice competente ai sensi del capo stesso per ottenere un provvedimento di conferma del lodo nei confronti di un'altra parte arbitrale. Il giudice conferma il lodo salvo se riscontra uno dei motivi di rigetto o di differimento del riconoscimento o dell'esecuzione del lodo indicati nella convenzione di New York (*Ibid.*, articolo 207). Sempre a norma del capo 2, i giudici distrettuali degli Stati Uniti d'America sono competenti dell'azione o del procedimento avviato in virtù della convenzione di New York, a prescindere dall'importo oggetto della controversia (*Ibid.*, articolo 203).
Il capo 2 stabilisce inoltre che il capo 1 si applica alle azioni e ai procedimenti avviati a norma del capo stesso nella misura in cui non via sia conflitto con il capo stesso o con la convenzione di New York quale ratificata dagli Stati Uniti (*Ibid.*, articolo 208). Il capo 1 afferma a sua volta la validità, irrevocabilità e esecutività della disposizione scritta di un contratto vertente su un'operazione che comporta aspetti commerciali la quale preveda di risolvere per via arbitrale la controversia sorta da tale contratto o operazione, così come il rifiuto di eseguire la totalità o parte del contratto o dell'operazione, e parimenti la validità, irrevocabilità e esecutività dell'accordo scritto di sottoporre a arbitrato una preesistente controversia sorta da detto contratto, operazione o rifiuto, fatti salvi i motivi di legge o equity che determinano la revoca dei contratti (*Ibid.*, articolo 2). Sempre a norma del capo 1, ciascuna parte arbitrale può adire il giudice indicato dallo stesso capo 1 per ottenere un provvedimento di conferma del lodo; in tal caso, il giudice deve emanare tale provvedimento, a meno che il lodo sia cassato, modificato o rettificato secondo quanto prescritto negli articoli 10 e 11 della stessa legge federale sull'arbitrato (*Ibid.*, articolo 9).

2. Sono predisposte procedure per evitare che la stessa presunta violazione asserita dalla stessa persona sia trattata due volte o determini due riparazioni.

3. L'FTC può intervenire parallelamente all'arbitrato.

4. All'arbitrato non può partecipare nessun rappresentante degli USA, dell'UE o di uno Stato membro dell'UE, così come di nessun'altra autorità pubblica o autorità di esecuzione; in via eccezionale, a richiesta della persona dell'UE le autorità di protezione dei dati dell'UE possono assisterla solo nella redazione dell'avviso, ma non possono avere accesso alla documentazione esibita né a altro materiale connesso all'arbitrato.

5. Il procedimento arbitrale si svolge negli Stati Uniti d'America; la persona può optare per la partecipazione in video o via telefono, che le è fornita gratuitamente. Non è obbligatorio presenziare di persona.

6. Salvo diversa decisione delle parti, il procedimento arbitrale si svolge in lingua inglese. Su richiesta motivata e tenuto conto del fatto che la persona sia rappresentata da un legale o no, è fornita alla persona, gratuitamente, l'interpretazione nell'udienza arbitrale e la traduzione della documentazione arbitrale, a meno che il collegio ritenga che, nelle circostanze specifiche, ciò comporti costi ingiustificati o sproporzionati.

7. È garantita la riservatezza della documentazione sottoposta agli arbitri, che è usata esclusivamente in relazione all'arbitrato.

8. Se necessario, può essere ammessa l'esibizione di documentazione specifica alla persona; le parti garantiscono la riservatezza della documentazione così esibita, che è usata esclusivamente in relazione all'arbitrato.

9. Salvo diversa decisione delle parti, il procedimento arbitrale dovrebbe concludersi entro 90 giorni dalla consegna dell'avviso all'organizzazione.

H. **Costi**

Gli arbitri devono adottare provvedimenti ragionevoli per ridurre al minimo spese e onorari dei procedimenti arbitrali.

Nel rispetto della legge applicabile, il Dipartimento del Commercio agevola la costituzione di un fondo cui ciascuna organizzazione aderente allo scudo è tenuta a versare una quota annua a copertura delle spese, compresi gli onorari degli arbitri; l'entità della quota è basata in parte sulla dimensione dell'organizzazione ed è limitata da determinati importi massimi («massimali»), in consultazione con la Commissione europea. Il fondo sarà gestito da un terzo, che riferisce periodicamente sul suo funzionamento. In sede di analisi annuale, il Dipartimento del Commercio e la Commissione europea esaminano il funzionamento del fondo, compresa la necessità di adeguare le quote o i massimali, e considerano tra l'altro il numero dei procedimenti arbitrali, con i relativi costi e tempi, muovendo dal presupposto condiviso che il sistema non deve comportare un onere finanziario eccessivo per le organizzazioni aderenti allo scudo. Gli onorari degli avvocati non sono contemplati dalla presente disposizione né da nessun fondo costituito in virtù della presente disposizione.

ALLEGATO II

PRINCIPI DEL REGIME DELLO SCUDO UE-USA PER LA PRIVACY EMANANTI DAL DIPARTIMENTO DEL COMMERCIO DEGLI STATI UNITI D'AMERICA

I. PANORAMICA

1. Per quanto Stati Uniti d'America ed Unione europea condividano il principio di rafforzare la tutela della sfera privata, gli Stati Uniti applicano un metodo diverso da quello adottato dall'Unione europea. Gli Stati Uniti si basano su un approccio settoriale costituito da una combinazione di legislazione, regolamentazione e autoregolamentazione. Date le differenze tra i due sistemi, al fine di dotare le organizzazioni presenti negli Stati Uniti di un meccanismo affidabile per il trasferimento dei dati personali dall'Unione europea agli USA garantendo nel contempo agli interessati dell'UE di continuare a godere delle garanzie e della protezione effettive che la normativa europea prevede relativamente al trattamento dei dati personali trasferiti al di fuori dell'UE, il Dipartimento del Commercio emana i presenti principi del regime dello scudo per la privacy («scudo» o «regime»), compresi i principi supplementari, (collettivamente: «i principi») in virtù del potere conferitogli per legge di favorire, promuovere e sviluppare il commercio internazionale (Codice degli Stati Uniti d'America, titolo 15, articolo 1512). I principi sono stati messi a punto in consultazione con la Commissione europea, con l'industria e con altri portatori di interessi per facilitare gli scambi commerciali fra Stati Uniti ed Unione europea. Sono destinati unicamente alle organizzazioni presenti negli Stati Uniti che ricevono dati personali dall'Unione europea, al fine di permettere loro di conformarsi ai requisiti dello scudo e, quindi, di ottenere i benefici della decisione di adeguatezza della Commissione europea ([1]). I principi lasciano impregiudicata l'applicazione delle disposizioni nazionali di attuazione della direttiva 95/46/CE («direttiva») applicabili al trattamento dei dati personali negli Stati membri. I principi non determinano limiti agli obblighi in materia di privacy altrimenti applicabili in forza del diritto statunitense.

2. Per ricevere dati personali trasferiti dall'UE in virtù dello scudo, l'organizzazione deve autocertificare l'adesione ai principi presso il Dipartimento del Commercio o altra persona (fisica o giuridica) da esso designata («Dipartimento»). Sebbene la decisione di un'organizzazione di aderire in questo modo allo scudo sia prettamente volontaria, l'effettiva conformità ai relativi principi è obbligatoria: le organizzazioni che si autocertificano presso il Dipartimento impegnandosi pubblicamente a rispettare i principi devono conformarsi totalmente ai principi. Per poter aderire allo scudo un'organizzazione deve: a) essere sottoposta all'autorità d'indagine e di controllo della Commissione federale del Commercio (FTC), del Dipartimento dei Trasporti (DOT) o di altro ente competente per legge che assicuri concretamente l'osservanza dei principi *(in futuro potranno essere aggiunti in un allegato altri enti previsti dalla legge statunitense e riconosciuti dall'UE)*; b) impegnarsi pubblicamente a rispettare i principi; c) divulgare al pubblico le sue politiche della privacy in linea con i principi; d) dare loro attuazione integrale. L'inosservanza da parte dell'organizzazione è perseguibile ai sensi dell'articolo 5 della legge sulla Commissione federale del Commercio, che proibisce gli atti sleali e ingannevoli nel commercio o aventi ripercussioni sul commercio (Codice degli Stati Uniti d'America, titolo 15, articolo 45, lettera a)] o ai sensi di altre disposizioni legislative o regolamentari che vietano tali atti.

3. Il Dipartimento tiene e mette a disposizione del pubblico un elenco ufficiale delle organizzazioni statunitensi che si sono autocertificate presso di esso impegnandosi a rispettare i principi dello scudo («elenco degli aderenti allo scudo» o «elenco»). I benefici derivanti dall'adesione allo scudo sono attivati a partire dalla data in cui il Dipartimento inserisce l'organizzazione nell'elenco. Il Dipartimento depenna dall'elenco l'organizzazione che si ritira dal regime volontariamente o che non completa la procedura di ricertificazione annuale presso di esso. L'organizzazione depennata dall'elenco degli aderenti allo scudo non può più beneficiare della decisione di adeguatezza della Commissione europea che le consente di ricevere informazioni personali dall'UE. L'organizzazione deve continuare ad applicare i principi alle informazioni personali ricevute mentre aderiva al regime, fintantoché le conserverà, rinnovando ogni anno presso il Dipartimento l'impegno in tal senso; in caso contrario, l'organizzazione deve restituire o cancellare le informazioni oppure proteggerle «adeguatamente» con altro mezzo autorizzato. Il Dipartimento depenna dall'elenco anche le organizzazioni che hanno commesso reiterate inosservanze dei principi: esse non sono ammesse ai benefici derivanti dallo scudo e devono restituire o cancellare le informazioni personali ricevute in tale ambito.

4. Il Dipartimento tiene e mette a disposizione del pubblico anche un elenco ufficiale delle organizzazioni statunitensi che si erano autocertificate presso di esso ma che sono state depennate dall'elenco. Il Dipartimento diffonde un'avvertenza precisa per specificare che tali organizzazioni non partecipano allo scudo; che il depennamento dall'elenco implica che l'organizzazione non può dichiararsi conforme allo scudo e deve astenersi da dichiarazioni o pratiche che lascino intendere che vi aderisce e che le organizzazioni depennate perdono il beneficio della decisione di adeguatezza della Commissione europea che consentirebbe loro di ricevere informazioni personali dall'UE. L'FTC, il Dipartimento dei Trasporti o altre autorità preposte all'applicazione della legge possono avviare

([1]) Se la decisione della Commissione europea sull'adeguatezza della tutela offerta dallo scudo UE-USA per la privacy si applicherà anche a Islanda, Liechtenstein e Norvegia, la presente documentazione riguarderà anche tali tre paesi oltre all'Unione europea. In tal caso, i riferimenti all'UE e ai suoi Stati membri si intendono quindi comprensivi di Islanda, Liechtenstein e Norvegia.

un'azione coercitiva nei confronti dell'organizzazione che, depennata dall'elenco, continua a millantare l'adesione allo scudo o a lasciare altrimenti intendere che vi partecipa.

5. L'adesione ai principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione, oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando, nelle rispettive politiche in materia di tutela della sfera privata, in quali casi saranno regolarmente applicate le eccezioni ammesse dalla lettera b). Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata.

6. Una volta aderito allo scudo, le organizzazioni sono tenute ad applicarne i principi a tutti i dati personali trasferiti in virtù dello stesso. L'organizzazione che sceglie di estendere i benefici dello scudo alle informazioni personali trasferite dall'UE e riguardanti le risorse umane nel contesto di un rapporto di lavoro lo deve menzionare nell'autocertificazione da trasmettere al Dipartimento ed uniformarsi ai requisiti elencati nel principio supplementare sull'autocertificazione.

7. Alle questioni riguardanti l'interpretazione e il rispetto dei principi e alle relative politiche della privacy delle organizzazioni vincolate dallo scudo si applica la normativa statunitense, eccetto nel caso in cui l'organizzazione si sia impegnata a collaborare con le autorità europee di protezione dei dati. Salvo disposizioni contrarie, tutte le disposizioni dello scudo si applicano laddove pertinenti.

8. Definizioni

   a. Per «dati personali» ed «informazioni personali» s'intendono dati e informazioni, riguardanti singoli individui (identificati od identificabili) cui si applica la direttiva, che un'organizzazione presente negli Stati Uniti riceve dall'Unione europea e registra in qualsiasi forma.

   b. Per «trattamento» dei dati personali s'intende qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione o la diffusione, nonché la cancellazione o la distruzione.

   c. Per «titolare del trattamento» s'intende la persona o l'organizzazione che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

9. La data di efficacia dei principi è la data in cui la Commissione europea approva in via definitiva la decisione di adeguatezza.

II. PRINCIPI

1. **Informativa**

   a. L'organizzazione deve informare le persone:

      i. della sua adesione allo scudo, fornendo un collegamento ipertestuale o l'indirizzo Internet in cui è reperibile l'elenco degli aderenti allo scudo;

      ii. dei tipi di dati personali raccolti e, se del caso, dei soggetti o delle filiali che fanno capo ad essa e che aderiscono anch'essi ai principi;

iii. del suo impegno di attenersi ai principi per tutti i dati personali ricevuti dall'UE in virtù dello scudo;

iv. delle finalità alle quali raccoglie e usa informazioni personali che le riguardano;

v. del modo in cui contattare l'organizzazione per trasmettere richieste di informazioni o reclami, indicando anche i soggetti stabiliti nell'UE che possono eventualmente rispondervi;

vi. del tipo o dell'identità dei terzi cui comunica dati personali indicando le finalità della comunicazione;

vii. del diritto di accedere ai dati personali che le riguardano;

viii. delle opzioni e dei mezzi che mette a loro disposizione per limitare l'uso e la divulgazione dei dati personali che le riguardano;

ix. dell'organo indipendente di composizione delle controversie incaricato di trattare i reclami e di mettere a disposizione della persona, gratuitamente, mezzi di ricorso adeguati, indicando se si tratta: 1) del comitato istituito dalle autorità di protezione dei dati, 2) di un organo alternativo di composizione delle controversie basato nell'UE oppure 3) di un organo alternativo di composizione delle controversie basato negli USA;

x. di essere sottoposta all'autorità d'indagine e di controllo dell'FTC, del Dipartimento dei Trasporti o di altro ente competente per legge autorizzato negli USA;

xi. della possibilità di chiedere, a determinate condizioni, un arbitrato vincolante;

xii. dell'obbligo di comunicare informazioni personali in risposta a legittime richieste delle autorità pubbliche, tra l'altro per motivi di sicurezza nazionale o di applicazione della legge;

xiii. della responsabilità che le incombe in caso di ulteriore trasferimento dei dati a terzi.

b. Queste indicazioni vanno formulate in un linguaggio chiaro e in modo da attirare l'attenzione quando si tratta del primo invito a fornire informazioni personali alle organizzazioni rivolto ad una persona oppure non appena ciò risulti successivamente possibile, ma comunque prima che le organizzazioni utilizzino o rivelino per la prima volta a terzi tali informazioni per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte.

2. **Scelta**

a. L'organizzazione deve offrire alle persone la possibilità di scegliere (facoltà di rifiuto) se le informazioni personali che le riguardano possano essere: i) rivelate a terzi; ovvero ii) utilizzate per finalità sostanzialmente diverse da quelle per cui erano state originariamente raccolte o da quelle successivamente autorizzate dalla persona. Devono essere messi a disposizione delle persone meccanismi chiari, agevolmente riconoscibili e di rapida fruizione per esercitare la scelta.

b. In deroga al paragrafo precedente, non occorre offrire la possibilità di scelta quando le informazioni sono trasmesse ad un terzo che agisce in qualità di procuratore per eseguire uno o più compiti a nome dell'organizzazione ed obbedendo ad istruzioni da essa ricevute. L'organizzazione deve tuttavia concludere in ogni caso un contratto con il procuratore.

c. Per le informazioni sensibili (ossia informazioni personali concernenti condizioni mediche o sanitarie, origine etnica o razziale, opinioni politiche, credenze filosofiche o religiose, appartenenza a sindacati, o la vita sessuale dell'individuo), l'organizzazione deve ottenere il consenso esplicito della persona se le informazioni sono destinate a essere: i) rivelate a terzi; o ii) utilizzate per finalità diverse da quelle per cui erano state originariamente raccolte o da quelle successivamente autorizzate dalla persona con l'esercizio della facoltà di accettazione. L'organizzazione è inoltre tenuta a considerare sensibile qualsiasi informazione personale ricevuta da un terzo che la definisce e la considera tale.

3. **Responsabilità in caso di ulteriore trasferimento**

a. Per trasferire informazioni personali a un terzo che agisce come titolare del trattamento, l'organizzazione deve applicare i principi sull'informativa e sulla scelta. L'organizzazione deve inoltre concludere col terzo titolare del trattamento un contratto in base al quale tali dati possono essere trattati solo per finalità determinate e limitate, conformemente al consenso dato dalla persona, e il destinatario offre lo stesso livello di protezione previsto dai principi, impegnandosi a informare l'organizzazione se constata di non poter più assolvere quest'obbligo. Il contratto prevede che, a seguito di tale constatazione, il terzo titolare del trattamento cessi il trattamento o adotti altra misura ragionevole e adeguata per rimediare alla situazione.

b. Per trasferire informazioni personali a un terzo che agisce come procuratore, l'organizzazione deve: i) trasferire i dati solo per finalità determinate e limitate; ii) accertare che il procuratore sia tenuto a offrire almeno lo stesso livello di tutela della vita privata richiesto dai principi; iii) adottare provvedimenti ragionevoli e adeguati per garantire che, in concreto, il procuratore tratti le informazioni personali che gli sono trasmesse in modo conforme agli obblighi cui i principi vincolano l'organizzazione; iv) imporre al procuratore di informarla se constata di non poter più assolvere l'obbligo di offrire lo stesso livello di tutela previsto dai principi; v) non appena avvertita, anche nel quadro del punto iv), adottare misure ragionevoli e adeguate per far cessare il trattamento non autorizzato e porvi rimedio; vi) a richiesta del Dipartimento, fornirgli un sunto o un estratto rappresentativo delle pertinenti disposizioni sulla tutela della vita privata contenute nel contratto concluso con il procuratore.

4. **Sicurezza**

a. L'organizzazione che crea, detiene, usa o diffonde informazioni personali deve adottare misure ragionevoli e adeguate per tutelarle contro la perdita, l'abuso e l'accesso, la divulgazione, l'alterazione e la distruzione non autorizzati, tenuto conto dei rischi insiti nel trattamento dei dati personali e nella loro natura.

5. **Integrità dei dati e limitazione della finalità**

a. Secondo i principi le informazioni personali devono essere limitate alle informazioni pertinenti ai fini del trattamento ([1]). L'organizzazione non può trattare le informazioni personali in modo incompatibile con le finalità per cui sono state raccolte o con quelle successivamente autorizzate dalla persona. Per quanto necessario al conseguimento di tali finalità, l'organizzazione deve adottare misure ragionevoli per assicurare che i dati personali siano affidabili per l'uso previsto, accurati, completi e aggiornati. L'organizzazione deve rispettare i principi fintantoché conserva le informazioni.

b. Le informazioni possono essere conservate in una forma che identifica la persona o ne permette l'identificazione ([2]) solo per il tempo necessario per conseguire la finalità di un trattamento ai sensi della parte 5, lettera a). Quest'obbligo non osta a che l'organizzazione tratti dati personali per periodi più lunghi, per il periodo e nella misura in cui il trattamento sia ragionevolmente funzionale a scopi quali l'archiviazione nel pubblico interesse, l'attività giornalistica, letteraria e artistica, la ricerca scientifica e storica e l'analisi statistica. In tali casi il trattamento risponde ad altri principi e disposizioni del regime. L'organizzazione dovrebbe adottare misure ragionevoli e adeguate per conformarsi alla presente disposizione.

6. **Accesso**

a. La persona deve poter accedere alle informazioni personali che la riguardano in possesso dell'organizzazione ed altresì poterle correggere, modificare o cancellare se ed in quanto risultino inesatte o siano state trattate in violazione dei principi, salvo il caso specifico in cui l'onere o la spesa che tale accesso comporta siano sproporzionati ai rischi per la privacy della persona oppure siano violati i diritti di terzi.

([1]) A seconda delle circostanze, possono costituire esempi di finalità del trattamento conformi alle regole gli obiettivi ragionevolmente funzionali alle relazioni con la clientela, le considerazioni giuridiche e di conformità, le attività di verifica, la sicurezza e la prevenzione delle frodi, la tutela o difesa dei diritti giuridici dell'organizzazione o altri scopi coerenti con le aspettative della persona ragionevole in considerazione del contesto in cui s'iscrive la raccolta.

([2]) In questo contesto la persona è identificabile se, tenuto conto dei mezzi di identificazione di cui si prospetta ragionevolmente l'uso (in considerazione, tra l'altro, dei costi e del tempo necessario per l'identificazione e della tecnologia disponibile al momento del trattamento) e del formato in cui sono conservati i dati, l'organizzazione o il terzo che ha accesso ai dati potrebbero ragionevolmente identificare la persona.

7. **Ricorso, controllo e responsabilità**

a. Per tutelare efficacemente la riservatezza dei dati personali occorre disporre meccanismi solidi volti a garantire il rispetto dei principi, la possibilità di ricorso per la persona lesa dall'inosservanza dei principi e le conseguenze cui è esposta l'organizzazione che non rispetta i principi. I meccanismi devono comprendere almeno:

i. meccanismi di ricorso indipendenti di pronto impiego, atti a consentire d'istruire e dirimere, applicando i principi e senza costi per la persona, qualsiasi reclamo da questa presentato o qualsiasi controversia insorta, e di accordare un indennizzo laddove questa possibilità sia contemplata dalla legge o da iniziative del settore privato;

ii. procedure di controllo per verificare a posteriori la veridicità degli attestati e delle affermazioni rilasciati dall'organizzazione riguardo alle pratiche seguite in fatto di riservatezza dei dati personali e l'effettivo rispetto degli impegni presi a questo proposito, in particolare nei casi di inosservanza;

iii. obbligo di rimediare ai problemi insorti in seguito all'inosservanza dei principi da parte dell'organizzazione che dichiara di aderirvi, con precisazione delle conseguenze cui l'organizzazione si espone. Le sanzioni devono risultare sufficientemente severe da garantire il rispetto dei principi da parte dell'organizzazione.

b. L'organizzazione e i relativi meccanismi di ricorso indipendenti rispondono prontamente alle richieste del Dipartimento vertenti su informazioni relative allo scudo. L'organizzazione è tenuta a rispondere in tempi rapidi ai reclami sul rispetto dei principi inoltrati da autorità degli Stati membri dell'UE per il tramite del Dipartimento. L'organizzazione che ha scelto di collaborare con le autorità di protezione dei dati, compresa l'organizzazione che tratta dati sulle risorse umane, deve rispondere direttamente a tali autorità in relazione all'istruzione dei reclami e alla risoluzione dei relativi casi.

c. Se la persona ha chiesto un arbitrato vincolante tramite avviso all'organizzazione e nel rispetto delle procedure e condizioni previste nell'allegato I, l'organizzazione è tenuta a sottoporre il reclamo a procedimento arbitrale e a rispettare le condizioni dell'allegato I.

d. In caso di ulteriore trasferimento, l'organizzazione aderente allo scudo è responsabile del trattamento dei dati personali ricevuti nell'ambito dello scudo e inoltrati a un terzo che agisce come suo procuratore. In base ai principi l'organizzazione aderente allo scudo resta responsabile qualora il procuratore tratti le informazioni personali in modo non conforme ai principi, salvo se è in grado di dimostrare la sua estraneità all'evento che ha causato il danno.

e. Quando le è contestata un'inosservanza dei principi tramite un ordine emesso dall'FTC o da un giudice, l'organizzazione rende pubbliche le parti inerenti allo scudo delle relazioni di conformità o di valutazione presentate all'FTC, limitatamente a quanto compatibile con gli obblighi di riservatezza. Il Dipartimento ha istituito un referente cui le autorità di protezione dei dati possono sottoporre le questioni inerenti alla conformità ai principi da parte delle organizzazioni aderenti allo scudo. La FTC tratta in via prioritaria i casi d'inosservanza dei principi ad essa sottoposti dal Dipartimento e dalle autorità degli Stati membri dell'UE e condivide le informazioni su tali casi con l'autorità dello Stato che glieli ha sottoposti, ferme restando le vigenti limitazioni per ragioni di riservatezza.

III. PRINCIPI SUPPLEMENTARI

1. **Dati sensibili**

a. L'organizzazione non è obbligata a ottenere il consenso esplicito della persona (facoltà di accettazione) per i dati sensibili se il trattamento è:

i. nel vitale interesse dell'interessato o di un'altra persona;

ii. necessario per far valere un diritto o presentare una difesa in sede giudiziaria;

iii. necessario a fini di cura sanitaria o diagnosi medica;

iv. eseguito nell'ambito delle attività legittime di una fondazione, di un'associazione o di altra organizzazione non a scopo di lucro con finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri di tale fondazione, associazione o organizzazione oppure le persone che sono in regolare contatto con essa nel perseguimento delle sue finalità e che i dati non siano divulgati a terzi senza il consenso dell'interessato;

v. necessario per adempiere agli obblighi imposti all'organizzazione dalla legislazione sul lavoro; oppure

vi. riferito a dati resi manifestamente pubblici dall'interessato.

2. **Eccezioni giornalistiche**

a. Date le tutele garantite alla libertà di stampa dalla Costituzione degli Stati Uniti e l'esenzione prevista dalla direttiva per il materiale giornalistico, laddove il diritto alla libertà di stampa, sancito dal primo emendamento della stessa Costituzione, interferisca con gli interessi legati alla protezione della sfera privata, l'equilibrio tra gli interessi in causa è disciplinato dal primo emendamento per quanto riguarda le attività di persone od organizzazioni statunitensi.

b. Indipendentemente dal fatto che se ne faccia uso o no, non sottostanno agli obblighi dello scudo le informazioni personali raccolte per pubblicazioni, trasmissioni radiotelevisive od altre forme di comunicazione pubblica di materiale giornalistico né le informazioni rinvenute in materiale già pubblicato e divulgate a partire da archivi di mezzi di informazione.

3. **Responsabilità accessoria**

a. In base ai principi dello scudo, i fornitori di servizi Internet (ISP), i vettori di telecomunicazioni e altre organizzazioni non sono giuridicamente responsabili quando si limitano a trasmettere, indirizzare, commutare o memorizzare in *cache* informazioni per conto di un'altra organizzazione. Al pari della direttiva, lo scudo per la privacy non determina una responsabilità accessoria. L'organizzazione non può essere ritenuta responsabile se ed in quanto agisce puramente da tramite per dati personali trasmessi da terzi e non determina le relative finalità e mezzi del trattamento.

4. **Adeguata verifica e revisione contabile**

a. Le attività dei revisori contabili e delle banche d'investimento possono comportare il trattamento di dati personali senza il consenso dell'interessato o senza che questi ne sia a conoscenza. Questo è consentito dai principi sull'informativa, sulla scelta e sull'accesso nelle situazioni illustrate qui di seguito.

b. Le società ad azionariato pubblico e le società private ad azionariato anche pubblico, comprese le organizzazioni aderenti allo scudo, sono sottoposte periodicamente a revisione contabile. In particolare se vertente sull'accertamento di possibili irregolarità, la revisione contabile può essere messa a repentaglio da una divulgazione prematura delle informazioni. Analogamente, se interessata da una possibile fusione o acquisizione, l'organizzazione aderente allo scudo procede a un'adeguata verifica o vi è sottoposta. Queste procedure comportano spesso la raccolta e il trattamento di dati personali, ad esempio di informazioni sui dirigenti e su altri membri del personale con funzioni fondamentali. Una divulgazione prematura delle informazioni potrebbe ostacolare l'operazione o addirittura violare la regolamentazione sui titoli finanziari. I dipendenti di una banca d'investimento e gli avvocati che procedono all'adeguata verifica o i revisori contabili che verificano i conti possono elaborare informazioni senza che l'interessato ne sia a conoscenza solo se ed in quanto l'elaborazione sia necessaria, e limitatamente al periodo necessario, per soddisfare prescrizioni di legge o esigenze di interesse pubblico e in altre circostanze in cui l'applicazione dei principi pregiudicherebbe i legittimi interessi dell'organizzazione. Rientrano fra gli interessi legittimi il monitoraggio del rispetto, da parte delle organizzazioni, dei loro obblighi giuridici e le legittime attività contabili, nonché la riservatezza richiesta nell'eventualità di acquisizioni, fusioni, joint venture o operazioni analoghe effettuate da dipendenti di una banca d'investimento o da revisori contabili.

5. **Ruolo delle autorità di protezione dei dati**

a. Le organizzazioni assolvono l'impegno di collaborare con le autorità di protezione dei dati dell'Unione europea secondo le modalità esposte qui di seguito. Nel contesto dello scudo le organizzazioni statunitensi che ricevono dati personali dall'UE devono impegnarsi ad impiegare meccanismi atti a garantire che i relativi principi siano effettivamente rispettati. Più specificamente, come stabilito dal principio su ricorso, controllo e responsabilità, l'organizzazione aderente deve prevedere: a) i) la possibilità di ricorso per le persone cui i dati si riferiscono; a) ii) procedure di controllo per verificare a posteriori la veridicità degli attestati e delle affermazioni rilasciati riguardo alle pratiche seguite in fatto di riservatezza dei dati personali; a) iii) l'obbligo di rimediare ai problemi insorti in seguito all'inosservanza dei principi da parte sua. L'organizzazione rispetta la lettera a), punti i) e iii), del principio su ricorso, controllo e responsabilità se soddisfa i requisiti previsti nel presente testo per la collaborazione con le autorità di protezione dei dati.

b. Per affermare l'impegno a collaborare con le autorità di protezione dei dati, nell'autocertificazione inerente allo scudo presentata al Dipartimento del Commercio (*cfr.* principio supplementare sull'autocertificazione) l'organizzazione dichiara che:

   i. decide di soddisfare i requisiti della lettera a), punti i) e iii), del principio su ricorso, controllo e responsabilità impegnandosi a collaborare con le autorità di protezione dei dati;

   ii. collabora con le autorità di protezione dei dati per l'istruzione dei reclami presentati nel quadro dello scudo e la risoluzione dei relativi casi;

   iii. si adegua al parere reso dall'autorità di protezione dei dati se questa ritiene che l'organizzazione debba attuare specifici interventi per uniformarsi ai principi dello scudo, compresi i provvedimenti di riparazione o risarcimento nei confronti della persona lesa dall'inosservanza dei principi, e conferma per iscritto a tale autorità di aver adottato i provvedimenti del caso.

c. Funzionamento dei comitati delle autorità di protezione dei dati

   i. La collaborazione con le autorità di protezione dei dati si concreta in informazioni e pareri secondo le seguenti modalità.

      1. Le autorità di protezione dei dati esprimono i pareri per il tramite di un comitato informale che le raggruppa, istituito a livello europeo, in modo da contribuire, tra l'altro, ad assicurare una linea armonizzata e coerente.

      2. Il comitato fornisce alle organizzazioni statunitensi interessate un parere nei casi irrisolti di reclamo presentato da una persona circa il trattamento cui sono state sottoposte informazioni personali trasferite dall'UE nell'ambito del regime dello scudo. Il parere mira a garantire che i principi dello scudo siano applicati correttamente e prevede le riparazioni che le autorità di protezione dei dati reputano adeguate per la o le persone interessate.

      3. Il comitato si pronuncia se interpellato dall'organizzazione interessata e/o se la persona gli presenta direttamente un reclamo nei confronti di un'organizzazione che si è impegnata a collaborare con le autorità di protezione dei dati per le finalità dello scudo, sempre incoraggiando e se necessario aiutando le persone a ricorrere in primo luogo al meccanismo interno di trattamento dei reclami offerto dall'organizzazione.

      4. Il parere è espresso soltanto dopo che le due parti delle controversia hanno avuto ragionevoli possibilità di formulare commenti e addurre qualsiasi elemento di prova desiderino. Il comitato si adopera per esprimere il parere quanto più rapidamente possibile, compatibilmente con l'esigenza di garantire l'equità del procedimento. Di norma il comitato mira ad esprimere il parere entro un termine di 60 giorni dalla data in cui riceve il reclamo o è interpellato, e se possibile anche più rapidamente.

      5. Se lo reputa opportuno, il comitato rende pubblici i risultati dell'esame del reclamo presentatogli.

      6. Il fatto che il comitato renda un parere non determina la responsabilità giuridica del comitato stesso né delle singole autorità di protezione dei dati.

   ii. Come già rilevato, l'organizzazione che sceglie quest'opzione per la composizione delle controversie deve impegnarsi ad uniformarsi al parere delle autorità di protezione dei dati. Se l'organizzazione non si adegua al parere entro 25 giorni dalla data in cui è espresso, senza fornire soddisfacenti giustificazioni del ritardo, il comitato comunica l'intenzione di presentare il caso alla Commissione federale del Commercio, al Dipartimento dei Trasporti o ad altri enti statunitensi, federali o statali che la legge abilita a avviare azioni coercitive, allo scopo di garantire il rispetto della legge nei casi di millanteria o inganno oppure di concludere che si è verificata una grave violazione dell'accordo di collaborazione, il quale è quindi da considerarsi nullo e privo di effetti. In quest'ultimo caso il comitato informa il Dipartimento del Commercio affinché modifichi di conseguenza l'elenco degli aderenti allo scudo. La mancanza all'impegno di collaborare con le autorità di protezione dei dati o l'inosservanza dei principi dello scudo sono perseguibili in quanto pratica ingannevole a norma dell'articolo 5 della legge sull'FTC o di altra analoga disposizione di legge.

d. L'organizzazione che vuole far rientrare nel regime dello scudo i dati sulle risorse umane trasferiti dall'UE nell'ambito di un rapporto di lavoro deve impegnarsi a collaborare con le autorità di protezione dei dati per quanto riguarda tali dati (*cfr.* principio supplementare sui dati sulle risorse umane).

e. All'organizzazione che opta per detta possibilità è richiesto di pagare una quota annua calcolata per coprire i costi d'esercizio del comitato; può altresì essere tenuta a sostenere le eventuali spese di traduzione incorse dal comitato per l'esame del caso o del reclamo sottopostogli contro l'organizzazione. La quota annua non supera l'importo di 500 dollari (USD); alle imprese più piccole è addebitata una quota inferiore.

6. **Autocertificazione**

a. I benefici derivanti dallo scudo valgono dalla data in cui il Dipartimento inserisce l'organizzazione nell'elenco degli aderenti allo scudo una volta accertata la completezza dell'autocertificazione da essa presentata.

b. Per autocertificarsi come aderente allo scudo, l'organizzazione deve presentare al Dipartimento un'autocertificazione firmata per suo conto da un dipendente abilitato, indicandovi come minimo le informazioni seguenti:

i. nome dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numeri di telefono e di fax;

ii. descrizione delle attività svolte dall'organizzazione in rapporto alle informazioni personali provenienti dall'UE;

iii. descrizione della politica della privacy seguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro:

1. se dispone di un sito web pubblico, il relativo indirizzo Internet al quale è consultabile la politica della privacy seguita; in alternativa, se non dispone di un sito web pubblico, il luogo in cui il pubblico può prendere visione della politica della privacy seguita;

2. la data effettiva di attuazione della politica;

3. l'ufficio referente per il trattamento dei reclami, le richieste di accesso e qualsiasi altra questione che può porsi in relazione allo scudo;

4. lo specifico organo competente per legge a conoscere delle azioni intentate contro l'organizzazione per possibili pratiche sleali o ingannevoli e violazioni di leggi o regolamenti che disciplinano la tutela della vita privata (ferma restando l'elencazione nei principi o in un futuro allegato ai principi);

5. la denominazione del o dei programmi sulla privacy cui l'organizzazione aderisce;

6. il metodo di verifica (ad esempio, verifica interna o verifica a opera di terzi) (*cfr.* principio supplementare sulla verifica);

7. il meccanismo di ricorso indipendente disponibile per l'istruzione dei casi irrisolti di reclamo.

c. L'organizzazione che lo desidera può far rientrare nel regime dello scudo le informazioni sulle risorse umane trasferite dall'UE per usi nel contesto di un rapporto di lavoro, se un organo stabilito per legge, elencato nei principi o in un loro futuro allegato, è competente a conoscere dei ricorsi contro l'organizzazione causati dal trattamento delle informazioni sulle risorse umane. L'organizzazione deve dichiarare l'intenzione in tal senso nell'autocertificazione, impegnandosi a collaborare con la o le autorità dell'UE interessate conformemente, secondo i casi, al principio supplementare sui dati sulle risorse umane o a quello sul ruolo delle autorità di protezione dei dati, e a conformarsi ai pareri resi da tali autorità. L'organizzazione deve trasmettere al Dipartimento copia della politica della privacy seguita relativamente alle risorse umane e comunicare il luogo in cui i dipendenti interessati possono prenderne visione.

d. Il Dipartimento tiene l'elenco delle organizzazioni aderenti allo scudo che hanno presentato autocertificazioni complete, assicurando così la disponibilità dei vantaggi offerti dal regime, e lo aggiorna in base alle autocertificazioni ripresentate ogni anno e alle notificazioni ricevute in applicazione del principio supplementare su composizione delle controversie e controllo dell'applicazione. L'autocertificazione deve essere ripresentata con cadenza almeno annuale; in caso contrario, l'organizzazione è depennata dall'elenco e non può più godere dei vantaggi derivanti dall'adesione allo scudo. Sia l'elenco sia le autocertificazioni presentate dalle organizzazioni sono resi pubblici. Ciascuna organizzazione che il Dipartimento inserisce nell'elenco degli aderenti allo scudo deve indicare che aderisce ai principi del regime nella dichiarazione pubblica sulla politica della privacy seguita.

Se consultabile in rete, la politica della privacy dell'organizzazione deve contenere un collegamento ipertestuale al sito web del Dipartimento dedicato allo scudo e un collegamento ipertestuale al sito web o al modulo di presentazione del reclamo del meccanismo di ricorso indipendente disponibile per l'istruzione dei casi irrisolti di reclamo.

e. I principi dello scudo per la privacy si applicano immediatamente alla data di certificazione. In considerazione del fatto che i principi hanno ripercussioni sulle relazioni commerciali con i terzi, l'organizzazione che si autocertifica ai fini dello scudo nei primi due mesi successivi alla data di efficacia del regime allinea tali relazioni con il principio sulla responsabilità in caso di ulteriore trasferimento non appena possibile, e comunque entro nove mesi dalla data dell'autocertificazione ai fini dello scudo. Nel frattempo, l'organizzazione che trasferisce dati a un terzo: i) applica i principi sull'informativa e sulla scelta; ii) se i dati personali sono trasferiti a un terzo che agisce come procuratore, accerta che questi sia tenuto a offrire almeno lo stesso livello di tutela della vita privata richiesto dai principi.

f. L'organizzazione deve attenersi ai principi dello scudo per tutti i dati personali ricevuti dall'UE in virtù del regime. Per i dati personali ricevuti nel periodo in cui l'organizzazione gode dei vantaggi dello scudo, l'impegno a rispettare i relativi principi non decade col tempo: l'obbligo di applicarli vige fintantoché l'organizzazione conserva, usa o divulga i dati in questione, anche nel caso in cui abbia successivamente abbandonato il regime per qualsivoglia motivo. L'organizzazione che, pur abbandonando lo scudo, desidera conservare tali dati deve confermare ogni anno al Dipartimento l'impegno di continuare ad applicare loro i principi oppure di proteggerli «adeguatamente» con altro mezzo autorizzato (ad esempio, un contratto che rispecchi totalmente le condizioni delle pertinenti clausole contrattuali tipo adottate dalla Commissione europea); in caso contrario, l'organizzazione deve restituire o cancellare le informazioni. L'organizzazione che abbandona lo scudo elimina dalla sua politica della privacy qualsiasi riferimento allo scudo che lasci intendere che continua ad aderirvi attivamente e a godere dei benefici che ne derivano.

g. L'organizzazione che cessa di esistere come persona giuridica distinta in seguito a fusione o acquisizione deve notificarlo in anticipo al Dipartimento. La notifica dovrebbe indicare se il soggetto acquirente o il soggetto risultante dalla fusione: 1) continuerà ad essere vincolato ai principi dello scudo in base alla legge applicabile alla fusione o acquisizione, oppure 2) deciderà di autocertificarsi come aderente ai principi dello scudo oppure di istituire altre garanzie, ad esempio un accordo scritto che sancisce l'adesione ai principi. Se non si applica né il punto i) né il punto ii), i dati personali acquisiti nell'ambito dello scudo devono essere cancellati immediatamente.

h. L'organizzazione che, per qualsivoglia motivo, abbandona lo scudo deve eliminare qualsiasi dichiarazione che lasci intendere che continua a parteciparvi o a godere dei relativi benefici. Se usato, dev'essere eliminato anche il marchio di certificazione dello scudo per la privacy. La FTC o altro ente pubblico competente possono perseguire l'organizzazione per qualsiasi dichiarazione pubblica con cui millanti l'adesione ai principi dello scudo. L'adesione millantata nei confronti del Dipartimento può essere perseguibile in forza della legge sulle false dichiarazioni (Codice degli Stati Uniti d'America, titolo 18, articolo 1001).

7. **Verifica**

a. L'organizzazione deve prevedere procedure di controllo per verificare a posteriori la veridicità degli attestati e delle affermazioni rilasciati riguardo alle pratiche seguite in fatto di riservatezza dei dati personali e l'effettivo rispetto degli impegni presi a questo proposito conformemente ai principi dello scudo.

b. Per soddisfare i requisiti del principio su ricorso, controllo e responsabilità, l'organizzazione deve verificare gli attestati e le affermazioni mediante un'autovalutazione autonoma o una verifica esterna della compatibilità.

c. Nell'impostazione basata sull'autovalutazione, la verifica deve accertare che la politica della privacy pubblicata, seguita dall'organizzazione per le informazioni personali ricevute dall'UE, sia accurata, completa, posta in evidenza, attuata integralmente e accessibile. Deve accertare inoltre che la politica sia conforme ai principi dello scudo; che le persone siano informate del meccanismo interno di trattamento dei reclami e dei meccanismi indipendenti attraverso cui possono sporgere reclamo; che siano predisposte procedure per formare i dipendenti all'applicazione della politica e per sanzionarli qualora se ne discostino; che siano predisposte procedure interne

per svolgere periodicamente un esame obiettivo del soddisfacimento dei citati requisiti. Almeno una volta l'anno un dipendente abilitato o altro rappresentante autorizzato dell'organizzazione deve firmare una dichiarazione attestante l'autovalutazione, la quale dev'essere messa a disposizione sia delle persone che ne fanno richiesta sia nell'ambito delle indagini o dei reclami per mancato soddisfacimento dei requisiti.

d. Se l'organizzazione ha optato per la verifica esterna della compatibilità, la verifica deve accertare che la politica della privacy seguita dall'organizzazione per le informazioni personali ricevute dall'UE sia conforme ai principi dello scudo, che sia effettivamente applicata e che le persone siano informate dei meccanismi di cui dispongono per sporgere reclamo. Tra i metodi impiegati per la verifica possono rientrare, tra gli altri e secondo i casi, l'audit, le indagini a campione, l'uso di «esche» o l'impiego di strumenti tecnologici. Almeno una volta l'anno l'esaminatore, oppure un dipendente abilitato o altro rappresentante autorizzato dell'organizzazione, deve firmare una dichiarazione attestante il completamento con esito positivo della verifica esterna della compatibilità, la quale dev'essere messa a disposizione sia delle persone che ne fanno richiesta sia nell'ambito delle indagini o dei reclami per mancato soddisfacimento dei requisiti.

e. L'organizzazione deve tenere traccia dell'attuazione delle pratiche seguite in fatto di rispetto della sfera privata nell'ambito dello scudo e, nell'ambito delle indagini o dei reclami per mancato soddisfacimento dei requisiti, metterle a disposizione, a richiesta, dell'organo indipendente competente dell'istruzione di tali casi o dell'ente competente in materia di pratiche sleali e ingannevoli. L'organizzazione deve rispondere prontamente alle richieste d'informazioni o di altro tipo emananti dal Dipartimento riguardo all'osservanza dei principi.

8. **Accesso**

a. Principio dell'accesso in pratica

i. In base ai principi dello scudo il diritto di accesso è fondamentale per la tutela della privacy, in particolare perché consente alla persona di verificare l'esattezza dei dati che la riguardano. Il principio dell'accesso implica che la persona ha diritto di:

1. sapere dall'organizzazione se sta trattando o no dati personali che la riguardano ([1]);

2. sapere di quali dati si tratta in modo da poterne verificare l'accuratezza e accertare la liceità del trattamento;

3. ottenere la correzione, la modifica o la cancellazione dei dati inesatti o trattati in violazione dei principi.

ii. La persona non è tenuta a motivare la domanda di accesso ai dati che la riguardano. Nel rispondere alla domanda di accesso l'organizzazione dovrebbe tenere presente innanzitutto il o i motivi che ne sono all'origine. Ad esempio, se la domanda di accesso è vaga o generica, l'organizzazione può avviare un dialogo con la persona per comprendere meglio la motivazione della domanda e individuare le informazioni che possono rispondervi. L'organizzazione potrebbe indagare per scoprire con quale o quali suoi comparti la persona abbia interagito o su quale tipo di informazioni o di uso verta la domanda di accesso.

iii. Considerata l'importanza fondamentale dell'accesso, l'organizzazione dovrebbe sempre adoperarsi in buona fede per consentirlo. Quando occorre, ad esempio, tutelare determinate informazioni che possono essere separate agevolmente da altre informazioni personali oggetto di una domanda di accesso, l'organizzazione dovrebbe fornire le informazioni di natura non riservata eliminando quelle soggette a tutela. Se decide, in una data circostanza, di limitare l'accesso, l'organizzazione dovrebbe motivare la decisione al richiedente indicandogli un referente contattabile per ulteriori informazioni.

b. Onere o costo della concessione dell'accesso

i. Il diritto di accesso ai dati personali può essere limitato in circostanze eccezionali in cui l'accesso violerebbe i diritti legittimi di persone diverse dall'interessato o quando, nello specifico caso, l'onere o il costo della concessione dell'accesso risulterebbero sproporzionati rispetto ai rischi per la privacy della persona. L'onere e il costo sono fattori importanti dei quali tenere conto, ma non sono determinanti nel decidere se la concessione dell'accesso sia ragionevole o no.

([1]) L'organizzazione dovrebbe rispondere alla persona che chiede spiegazioni sulle finalità del trattamento, sulle categorie di dati personali interessati e sui destinatari o categorie di destinatari cui i dati personali sono comunicati.

ii. Se, ad esempio, le informazioni personali sono usate per decisioni che producono effetti rilevanti per l'interessato (come il rifiuto o la concessione di benefici importanti quali un'assicurazione, un prestito ipotecario o un lavoro), conformemente alle altre disposizioni dei presenti principi supplementari l'organizzazione deve concedere l'accesso anche se risulta relativamente difficile o costoso. L'organizzazione dovrebbe comunque fornire l'accesso se le informazioni personali richieste, pur non essendo sensibili né usate per decisioni che producono effetti rilevanti per l'interessato, sono disponibili agevolmente e implicano un basso costo di comunicazione.

c. Informazioni commerciali riservate

i. Le informazioni commerciali riservate sono informazioni che l'organizzazione tutela contro la divulgazione per non agevolare la concorrenza sul mercato. L'organizzazione può negare o limitare l'accesso se ed in quanto l'accesso integrale porterebbe a rivelare sue informazioni commerciali riservate, quali profili di marketing o classificazioni, ovvero informazioni commerciali riservate di un terzo vincolato per contratto alla riservatezza.

ii. Quando è possibile separare agevolmente le informazioni commerciali di natura riservata dalle altre informazioni personali oggetto di una domanda di accesso, l'organizzazione dovrebbe fornire le informazioni di natura non riservata eliminando quelle commerciali riservate.

d. Struttura della banca dati

i. L'accesso può assumere la forma di comunicazione alla persona delle informazioni personali d'interesse da parte dell'organizzazione e non implica che la persona acceda alla banca dati dell'organizzazione.

ii. L'accesso dev'essere concesso solo se ed in quanto l'organizzazione conserva informazioni personali. Il principio dell'accesso non determina di per sé l'obbligo di conservare, aggiornare, riorganizzare o ristrutturare archivi di informazioni personali.

e. Limitazioni dell'accesso

i. L'organizzazione deve sempre adoperarsi in buona fede per consentire alla persona di accedere ai dati personali che la riguardano: le situazioni in cui può limitare l'accesso sono circoscritte e devono essere giustificate da motivi specifici. Così come previsto dalla direttiva, l'organizzazione può limitare l'accesso alle informazioni se la divulgazione rischia di interferire con la tutela d'interessi pubblici superiori, quali la sicurezza nazionale, la difesa o la sicurezza pubblica. Inoltre, l'accesso può essere negato se le informazioni personali sono trattate esclusivamente a scopo di ricerca o per finalità statistiche. L'accesso è inoltre rifiutato o limitato quando determinerebbe:

1. un'interferenza nell'esecuzione o applicazione della legge ovvero in diritti sostanziali di natura privata, compresi la prevenzione, l'indagine o l'accertamento di reati ovvero il diritto a un giudice imparziale;

2. la violazione di diritti legittimi o di interessi rilevanti di altri;

3. la violazione del segreto professionale dell'avvocato o di altro obbligo professionale;

4. un pregiudizio all'indagine di sicurezza o alla vertenza aziendale nei confronti di un dipendente ovvero in relazione alla programmazione dell'avvicendamento del personale e alla riorganizzazione societaria; oppure

5. un pregiudizio alla riservatezza necessaria per l'espletamento delle funzioni di controllo, ispezione o regolamentazione previste dalla sana gestione ovvero a trattative in corso o future che coinvolgono l'organizzazione.

ii. L'organizzazione che adduce un'eccezione ha l'onere di dimostrarne la necessità e di motivare la limitazione dell'accesso; dovrebbe altresì indicare alla persona un referente cui rivolgersi per ulteriori informazioni.

f. Diritto di sapere e addebito dei costi di concessione dell'accesso

i. La persona ha diritto di sapere dall'organizzazione se questa detiene o no dati personali che la riguardano, così come ha il diritto che tali dati le siano comunicati. L'organizzazione può addebitare costi che non siano sproporzionati.

ii. L'addebito può essere giustificato, ad esempio, quando le domande di accesso sono palesemente eccessive, in particolare perché reiterate.

iii. L'accesso non può essere rifiutato adducendone il costo se la persona si offre di sostenere le spese.

g. Domande di accesso reiterate o vessatorie

L'organizzazione può fissare un limite ragionevole al numero di volte in cui una stessa persona può vedere soddisfatte le sue domande di accesso in un dato lasso di tempo. Nel fissare il limite l'organizzazione dovrebbe prendere in considerazione fattori quali la frequenza d'aggiornamento dei dati, le finalità del loro impiego e la loro natura.

h. Domande di accesso fraudolente

L'organizzazione non è tenuta a concedere l'accesso se non le sono trasmesse informazioni sufficienti a confermare l'identità del richiedente.

i. Tempo di risposta

L'organizzazione dovrebbe rispondere alla domanda di accesso entro tempi ragionevoli, in modo ragionevole e in una forma che risulti agevolmente comprensibile alla persona. L'organizzazione che informa periodicamente gli interessati può soddisfare con la comunicazione periodica la domanda di accesso, a condizione che questo non determini un ritardo eccessivo.

9. **Dati sulle risorse umane**

a. Copertura dello scudo per la privacy

i. Se l'organizzazione presente nell'UE trasferisce negli Stati Uniti informazioni personali sui propri dipendenti (presenti o passati), raccolte nell'ambito del rapporto di lavoro, alla società controllante, a una società controllata o a un prestatore di servizi non collegato aderenti allo scudo, il trasferimento gode dei relativi benefici. In tali casi, le informazioni sono raccolte e trattate prima del trasferimento a norma della legge nazionale dello Stato membro dell'UE in cui sono state raccolte, e devono essere rispettate le condizioni o restrizioni applicabili al loro trasferimento in forza di detta legge.

ii. I principi dello scudo trovano applicazione solo per il trasferimento di dati identificati o identificabili individualmente o per l'accesso agli stessi. Non si pongono questioni di privacy per le relazioni statistiche basate su dati aggregati sull'occupazione e prive di dati personali né per l'uso di dati resi anonimi.

b. Applicazione dei principi sull'informativa e sulla scelta

i. L'organizzazione statunitense che ha ricevuto dall'UE informazioni sui dipendenti nell'ambito dello scudo può divulgarle a terzi o usarle per finalità differenti solo in conformità ai principi sull'informativa e sulla scelta. Se, ad esempio, l'intenzione è quella di usare a fini non occupazionali (comunicazioni commerciali ecc.) informazioni personali raccolte nell'ambito di un rapporto di lavoro, l'organizzazione statunitense deve necessariamente ottenere il consenso preliminare della persona, a meno che questa non abbia già autorizzato l'uso delle informazioni per tali scopi. L'uso delle informazioni non può essere incompatibile con le finalità per cui sono state raccolte o con quelle successivamente autorizzate dalla persona. Le scelte fatte a questo proposito non devono essere usate per limitare le opportunità occupazionali o adottare provvedimenti punitivi nei confronti del dipendente.

ii. È possibile che determinate condizioni di applicazione generale ai trasferimenti in provenienza da alcuni Stati membri dell'UE vietino usi diversi delle informazioni anche dopo il loro trasferimento al di fuori dell'UE: tali condizioni devono essere rispettate.

iii. I datori di lavoro dovrebbero fare il possibile, nei limiti del ragionevole, per rispettare le preferenze dei dipendenti in fatto di tutela della sfera privata, ad esempio limitando l'accesso ai dati personali, rendendo anonimi taluni dati o attribuendo codici o pseudonimi se i nominativi esatti non sono necessari per la finalità gestionale in questione.

iv. In quanto e fino a che ciò risulti necessario per non ledere la capacità dell'organizzazione di procedere a promozioni e nomine o prendere decisioni analoghe relative al personale, l'organizzazione non è tenuta a soddisfare i requisiti di informativa e di scelta.

c. Applicazione del principio sull'accesso

Il principio supplementare sull'accesso fornisce indicazioni sui motivi che possono giustificare il rifiuto o la restrizione dell'accesso richiesto in tema di risorse umane. Nell'Unione europea il datore di lavoro deve ovviamente rispettare la normativa locale e garantire al dipendente l'accesso alle informazioni secondo le modalità prescritte dalla legge dello Stato in cui si trova, a prescindere dal luogo di trattamento e di conservazione dei dati. Lo scudo impone all'organizzazione che tratta tali dati negli Stati Uniti d'America di collaborare, fornendo l'accesso direttamente o tramite il datore di lavoro dell'UE.

d. Applicazione

i. Se e in quanto le informazioni sono usate soltanto nel contesto del rapporto di lavoro, l'organizzazione presente nell'UE mantiene la responsabilità primaria nei confronti dei dipendenti. Ne consegue che il dipendente europeo che, denunciata una violazione dei suoi diritti alla riservatezza, non è soddisfatto dell'esito delle procedure interne di esame, di reclamo e di ricorso (o di qualsiasi vertenza avviata nell'ambito del contratto concluso con un sindacato) deve rivolgersi all'autorità statale o nazionale competente della protezione dei dati o dei diritti dei lavoratori nella giurisdizione in cui lavora. Rientra nel caso di specie anche la situazione in cui il presunto uso improprio dei dati personali fa capo all'organizzazione statunitense che ha ricevuto le informazioni dal datore di lavoro, e che può pertanto configurarsi come presunta violazione dei principi dello scudo. È questo il sistema più efficace per orientarsi tra i vari diritti e obblighi, che spesso si accavallano, derivanti dal diritto del lavoro e dai contratti di lavoro locali e dalla normativa sulla protezione dei dati.

ii. Se vuole che lo scudo si applichi ai dati UE sulle risorse umane trasferiti dall'Unione europea nel contesto di un rapporto di lavoro, l'organizzazione statunitense aderente allo scudo che li usa deve pertanto impegnarsi a collaborare con le autorità competenti dell'UE nelle indagini e ad attenersi al parere da esse formulato al riguardo.

e. Applicazione del principio sulla responsabilità in caso di ulteriore trasferimento

Per le esigenze operative occasionali di natura occupazionale cui l'organizzazione aderente allo scudo deve far fronte riguardo ai dati personali trasferiti nell'ambito del regime (ad esempio, la prenotazione di un volo o di una stanza d'albergo o ancora la copertura assicurativa), i dati personali che riguardano un numero esiguo di dipendenti possono essere trasmessi al titolare del trattamento senza applicare il principio sull'accesso e senza concludere un contratto col terzo titolare del trattamento, come invece imporrebbe il principio sulla responsabilità in caso di ulteriore trasferimento, a condizione che l'organizzazione abbia rispettato i principi sull'informativa e sulla scelta.

10. **Contratti obbligatori per l'ulteriore trasferimento**

a. Contratti sul trattamento dei dati

i. Quando i dati personali sono trasferiti dall'UE agli USA a fini esclusivi di trattamento è necessario un contratto, anche se il responsabile del trattamento aderisce allo scudo.

ii. Nell'Unione europea il titolare del trattamento è sempre tenuto a concludere un contratto per il trasferimento a fini esclusivi di trattamento, indipendentemente dal fatto che la relativa operazione sia effettuata all'interno o all'esterno dell'UE o che il responsabile del trattamento aderisca allo scudo. L'obiettivo del contratto è assicurare che il responsabile del trattamento:

1. agisca soltanto su istruzione del titolare del trattamento;

2. preveda misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, e sia in grado di stabilire se è consentito l'ulteriore trasferimento;

3. tenuto conto della natura del trattamento, assista il titolare del trattamento al fine di rispondere alla persona che esercita i propri diritti in virtù dello scudo.

iii. Poiché gli aderenti allo scudo forniscono una protezione adeguata, il contratto concluso con uno di essi a fini esclusivi di trattamento non è subordinato a autorizzazione preliminare (ovvero l'autorizzazione è concessa automaticamente dagli Stati membri dell'UE) com'è invece il caso per il contratto stipulato con il destinatario che non aderisce al regime o che non fornisce altrimenti una protezione adeguata.

b. Trasferimenti all'interno di un gruppo di società o soggetti collegati in virtù di un rapporto di controllo

In base al principio sulla responsabilità in caso di ulteriore trasferimento, la conclusione di un contratto non sempre è necessaria per le informazioni personali trasferite tra due titolari del trattamento all'interno di un gruppo di società o soggetti collegati in virtù di un rapporto di controllo. All'interno di tale gruppo il titolare del trattamento può operare il trasferimento basandosi su altri strumenti dell'UE, quali le norme vincolanti d'impresa dell'UE o altri strumenti infragruppo (ad esempio, i programmi di conformità e controllo), garantendo così la continuità della protezione delle informazioni personali prevista dai principi. In tale trasferimento l'organizzazione aderente allo scudo rimane responsabile dell'osservanza dei relativi principi.

c. Trasferimenti fra titolari del trattamento

Per i trasferimenti fra titolari del trattamento il destinatario non deve necessariamente essere un'organizzazione aderente allo scudo o disporre di un meccanismo di ricorso indipendente. L'organizzazione aderente allo scudo deve concludere con il terzo titolare del trattamento che riceve i dati un contratto che preveda lo stesso livello di protezione fornito dallo scudo, senza imporgli di aderire allo scudo o di disporre di un meccanismo di ricorso indipendente, a condizione che il terzo metta a disposizione un meccanismo equivalente.

11. **Composizione delle controversie e controllo dell'applicazione**

a. Il principio su ricorso, controllo e responsabilità stabilisce gli obblighi in materia di controllo dell'applicazione dello scudo. Le modalità di soddisfacimento del requisito imposto dalla lettera a), punto ii), di tale principio sono esposte nel principio supplementare sulla verifica, mentre la lettera a), punti i) e iii), del medesimo, che implicano entrambi meccanismi di ricorso indipendenti, costituisce l'oggetto del presente principio supplementare. I meccanismi possono assumere forme diverse, ma devono sempre soddisfare le prescrizioni del principio su ricorso, controllo e responsabilità. L'organizzazione adempie agli obblighi che le incombono in questo contesto in uno dei modi seguenti: i) applicando programmi per la privacy elaborati dal settore privato nei quali sono integrati i principi dello scudo e che contemplano meccanismi di attuazione efficaci, del tipo descritto nel principio su ricorso, controllo e responsabilità; ii) uniformandosi alle disposizioni normative o regolamentari, emanate dalle autorità di controllo, che disciplinano il trattamento dei reclami e la composizione delle controversie; iii) impegnandosi a collaborare con le autorità di protezione dei dati ubicate nell'Unione europea o con loro rappresentanti autorizzati.

b. L'elenco è fornito a titolo puramente esemplificativo e non è limitativo. Il settore privato può mettere a punto altri meccanismi di controllo dell'applicazione, a condizione che siano conformi al principio su ricorso, controllo e responsabilità e ai principi supplementari. Le prescrizioni del principio su ricorso, controllo e responsabilità vanno a sommarsi al requisito che impone l'azionabilità delle iniziative di autoregolamentazione in virtù

dell'articolo 5 della legge sulla Commissione federale del Commercio, il quale proibisce gli atti sleali e ingannevoli, o di altra legge o regolamento che vieti tali atti.

c. Per contribuire al rispetto degli impegni assunti con l'adesione allo scudo e sostenere la gestione del programma, l'organizzazione e il relativo meccanismo di ricorso indipendente devono fornire al Dipartimento, quando le chiede, le informazioni relative allo scudo. L'organizzazione deve inoltre rispondere celermente ai reclami vertenti sulla sua conformità ai principi che le autorità di protezione dei dati hanno presentato tramite il Dipartimento. La risposta dovrebbe stabilire se il reclamo è fondato e, in caso affermativo, in che modo l'organizzazione intende porvi rimedio. Il Dipartimento tutela la riservatezza delle informazioni ricevute conformemente alla legge degli Stati Uniti d'America.

d. Meccanismi di ricorso

i. Il consumatore dovrebbe essere incoraggiato a sporgere reclamo all'organizzazione prima di rivolgersi al meccanismo di ricorso indipendente. L'organizzazione deve rispondere al consumatore entro 45 giorni dal ricevimento del reclamo. L'indipendenza del meccanismo di ricorso è un dato di fatto dimostrabile in vari modi, ad esempio da aspetti quali l'imparzialità, la trasparenza della composizione e del finanziamento e una comprovata esperienza. Come prescritto dal principio su ricorso, controllo e responsabilità, la persona deve poter contare su un mezzo di ricorso disponibile agevolmente e gratuito. L'organo di composizione delle controversie dovrebbe esaminare ciascun reclamo presentato, a meno che non sia futile o infondato. Questo non osta a che l'organizzazione che gestisce il meccanismo di ricorso stabilisca criteri d'ammissibilità, che devono però essere trasparenti e giustificati (ad esempio, esclusione dei reclami che esulano dal campo d'applicazione del programma o sono all'esame di altro consesso) e non dovrebbero andare a scapito dell'impegno di esaminare i ricorsi legittimi. Il meccanismo di ricorso dovrebbe inoltre fornire alle persone che sporgono reclamo informazioni complete e disponibili agevolmente sul funzionamento della procedura di composizione delle controversie, comprese informazioni sulle pratiche della privacy seguite dal meccanismo, conformemente ai principi dello scudo. Per semplificare il processo di risoluzione dei casi di reclamo, il meccanismo dovrebbe altresì collaborare allo sviluppo di strumenti quali i moduli di reclamo.

ii. Il meccanismo di ricorso indipendente deve riportare sul proprio sito web pubblico informazioni relative ai principi dello scudo e ai servizi che presta in tale ambito. Le informazioni devono comprendere: 1) informazioni sugli obblighi che i principi dello scudo impongono ai meccanismi di ricorso indipendenti oppure un collegamento ipertestuale agli stessi; 2) un collegamento ipertestuale al sito web del Dipartimento dedicato allo scudo; 3) l'indicazione che i servizi di composizione delle controversie prestati dal meccanismo sono gratuiti per la persona; 4) la spiegazione del modo in cui presentare un reclamo in virtù dello scudo; 5) i tempi di trattamento dei reclami presentati in virtù dello scudo; 6) la descrizione della gamma delle possibili riparazioni.

iii. Il meccanismo di ricorso indipendente deve pubblicare ogni anno una relazione che presenti, in forma aggregata, i dati statistici relativi ai servizi di composizione delle controversie prestati. La relazione annuale deve indicare: 1) il numero complessivo dei reclami in virtù dello scudo ricevuti nell'anno di riferimento; 2) il tipo di reclami ricevuti; 3) gli elementi qualitativi collegati alla composizione delle controversie, ad esempio il tempo di trattamento dei reclami; 4) l'esito dei reclami ricevuti, in particolare il numero e il tipo delle riparazioni o delle sanzioni decretate.

iv. Come illustrato nell'allegato I, è messa a disposizione della persona la possibilità di ricorrere all'arbitrato per accertare, quanto alle rivendicazioni accessorie, se l'organizzazione aderente allo scudo abbia violato nei suoi confronti gli obblighi derivanti dai principi e se l'eventuale violazione non sia stata ancora riparata in tutto o in parte. Questa possibilità è prevista soltanto per detti fini: non è, ad esempio, percorribile per le eccezioni ai principi ([1]) o per le denunce vertenti sull'adeguatezza dello scudo. In questo contesto il collegio arbitrale dello scudo (composto da uno o da tre arbitri, secondo quanto concordato dalle parti) ha il potere di imporre un provvedimento equo, specifico alla persona e di carattere non pecuniario (quali accesso, rettifica, cancellazione o restituzione dei dati che la riguardano) a titolo di riparazione per la violazione dei principi limitatamente alla persona in questione. Ai sensi della legge federale sull'arbitrato, la persona e l'organizzazione aderente allo scudo possono sottoporre la decisione arbitrale al riesame e all'esecuzione in sede giudiziaria previsti dalla legge statunitense.

([1]) Parte I, punto 5, dei principi.

e. Riparazioni e sanzioni

La riparazione ottenuta tramite l'organo di composizione delle controversie dovrebbe determinare l'intervento dell'organizzazione per correggere o eliminare, nei limiti del possibile, gli effetti dell'inosservanza, per assicurare la conformità ai principi di qualsiasi trattamento futuro e, se del caso, per cessare il trattamento de dati personali della persona che ha sporto reclamo. Le sanzioni devono essere sufficientemente severe da garantire che l'organizzazione si attenga ai principi. Una gamma di sanzioni di grado variabile consente all'organo di composizione delle controversie di reagire in maniera adeguata alla gravità dell'inosservanza. Le sanzioni dovrebbero includere la pubblicazione della constatazione di non conformità e, in determinate situazioni, l'obbligo di cancellare i dati ([1]). Tra le sanzioni potrebbero annoverarsi la sospensione o la revoca del marchio, il risarcimento alla persona per le perdite subite a causa dell'inosservanza e provvedimenti d'ingiunzione. Se l'organizzazione aderente allo scudo non si attiene alla decisione pronunciata, l'organo di composizione delle controversie e l'organo di autoregolamentazione del settore privato devono darne notifica all'ente pubblico competente o al giudice, secondo i casi, nonché al Dipartimento.

f. Attività dell'FTC

L'FTC si è impegnata a esaminare in via prioritaria i casi di presunta inosservanza dei principi che i) un organo di autoregolamentazione nel settore della privacy e altro organo indipendente di composizione delle controversie, ii) uno Stato membro dell'UE o iii) il Dipartimento le sottopongono perché stabilisca se c'è stata violazione dell'articolo 5 della legge sull'FTC che proibisce gli atti e le pratiche sleali e ingannevoli nel commercio. Se ha elementi per concludere che violazione vi è stata, l'FTC può risolvere la questione ottenendo un provvedimento amministrativo inibitorio delle pratiche contestate oppure depositando presso un giudice distrettuale federale una denuncia che, se va a buon fine, potrebbe scaturire in un provvedimento analogo emesso da un giudice federale. Si configura violazione anche quando l'organizzazione millanta l'adesione ai principi dello scudo o la partecipazione allo scudo pur non figurando più nell'elenco degli aderenti o non essendosi mai autocertificata come tale presso il Dipartimento. La FTC può ottenere l'imposizione di un'ammenda per violazione del provvedimento inibitorio amministrativo, mentre può denunciare in sede civile o penale l'«oltraggio alla corte» in caso di violazione del provvedimento del giudice federale. La FTC informa il Dipartimento di qualsiasi iniziativa in questo senso. Il Dipartimento incoraggia gli altri enti pubblici ad informarlo dell'esito definitivo dei casi loro deferiti o delle altre decisioni in tema di rispetto dei principi dello scudo.

g. Inosservanze reiterate

i. L'organizzazione per cui si riscontrano reiterate inosservanze dei principi perde i benefici derivanti dallo scudo: il Dipartimento la depenna dall'elenco degli aderenti e l'organizzazione deve restituire o cancellare le informazioni personali ricevute nell'ambito del regime.

ii. La fattispecie dell'inosservanza reiterata si configura quando l'organizzazione che si è autocertificata presso il Dipartimento rifiuta di uniformarsi alla decisione definitiva dell'ente pubblico, dell'organo di autoregolamentazione o dell'organo indipendente di composizione delle controversie competenti della privacy ovvero quando tale ente o organo constata che l'organizzazione viola i principi con tale frequenza da togliere qualsiasi credibilità alla sua dichiarazione formale di rispetto. In queste circostanze l'organizzazione è tenuta a darne immediata notifica al Dipartimento. La mancata notifica può essere perseguibile in forza della legge sulle false dichiarazioni (Codice degli Stati Uniti d'America, titolo 18, articolo 1001). Il ritiro dal programma di autoregolamentazione del settore privato o dall'organo indipendente di composizione delle controversie competenti della privacy non esime l'organizzazione dall'obbligo di conformarsi ai principi, e si configurerebbe come inosservanza reiterata.

iii. Quando riceve la notifica di un caso di inosservanza reiterata, sia essa trasmessa dall'organizzazione stessa oppure dall'ente pubblico, dall'organo di autoregolamentazione o dall'organo indipendente di composizione delle controversie competenti della privacy, il Dipartimento depenna l'organizzazione dall'elenco degli aderenti allo scudo, ma non prima di averle concesso un preavviso di 30 giorni e la possibilità di replica.

([1]) L'organo di composizione delle controversie dispone di discrezionalità quanto alle circostanze in cui ricorrere a tali sanzioni. La sensibilità dei dati costituisce uno degli elementi da prendere in considerazione per decidere se richiederne la cancellazione, così come il fatto che l'organizzazione abbia raccolto, usato o divulgato informazioni in flagrante violazione dei principi dello scudo.

L'elenco degli aderenti allo scudo tenuto dal Dipartimento indica di conseguenza quali organizzazioni godano dei benefici del regime e quali li abbiano perduti.

iv. L'organizzazione che si candida a partecipare a un organo di autoregolamentazione al fine di essere riammessa allo scudo è tenuta a presentargli tutte le informazioni relative alla precedente adesione al regime.

12. **Scelta — Tempi di esercizio della facoltà di rifiuto**

a. In generale il principio sulla scelta mira a garantire che le informazioni personali siano usate e divulgate in termini compatibili con le aspettative e le scelte dell'interessato. La persona dovrebbe pertanto poter esercitare in qualsiasi momento la facoltà di rifiuto in rapporto all'uso delle informazioni personali che la riguardano a fini di marketing diretto, subordinatamente al rispetto di limiti ragionevoli stabiliti dall'organizzazione, concernenti ad esempio il tempo necessario per dare seguito alla decisione di rifiuto. L'organizzazione può richiedere inoltre le informazioni necessarie a confermare l'identità della persona che esercita tale facoltà. Negli Stati Uniti può esercitare tale facoltà tramite un programma centrale di rifiuto, ad esempio il *Mail Preference Service* della *Direct Marketing Association*. L'organizzazione che aderisce a tale servizio dovrebbe pubblicizzarne l'esistenza presso i consumatori che non desiderano ricevere informazioni commerciali. Dovrebbe essere in ogni caso offerto alla persona un meccanismo disponibile agevolmente e a costi accessibili per esercitare questa facoltà.

b. L'organizzazione può altresì usare le informazioni per talune attività di marketing diretto quando non è possibile, in pratica, dare preliminarmente alla persona la possibilità di rifiuto, a condizione che contestualmente (e, su richiesta, in qualsiasi momento) le offra prontamente la possibilità (senza costo per la persona) di rifiutare ulteriori comunicazioni di marketing diretto, e che successivamente rispetti tale rifiuto.

13. **Informazioni sui viaggiatori**

a. In varie situazioni diverse possono essere trasferiti a organizzazioni ubicate al di fuori dell'UE dati ricavati da prenotazioni aeree e altro tipo di informazioni di viaggio, quali informazioni sul programma di fedeltà nel trasporto aereo o sulla prenotazione alberghiera, e dati sulle richieste speciali, come le particolari esigenze alimentari dovute a precetti religiosi o la richiesta di assistenza. A norma dell'articolo 26 della direttiva, i dati personali possono essere trasferiti verso «un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2» a condizione che i) il trasferimento sia necessario per la prestazione dei servizi chiesti dal consumatore o per il soddisfacimento dei termini di un accordo o che ii) il consumatore abbia manifestato in maniera inequivocabile il proprio consenso al trasferimento. L'organizzazione statunitense aderente allo scudo garantisce un'adeguata tutela dei dati personali e può quindi ricevere trasferimenti di dati dall'UE senza dover soddisfare dette o altre condizioni stabilite dall'articolo 26 della direttiva. Poiché il regime dello scudo prevede norme specifiche al riguardo, le informazioni sensibili (la cui raccolta può risultare necessaria, ad esempio, in rapporto ai clienti bisognosi di assistenza) possono essere trasferite agli aderenti allo scudo. L'organizzazione trasferente deve tuttavia uniformarsi sempre alla normativa vigente nello Stato membro dell'UE in cui opera, che può peraltro prescrivere condizioni particolari riguardo ai dati sensibili.

14. **Medicinali e prodotti farmaceutici**

a. Applicazione della normativa dello Stato membro dell'UE o dei principi dello scudo

La normativa dello Stato membro dell'UE si applica alla raccolta dei dati personali e al relativo trattamento prima del trasferimento negli Stati Uniti d'America. I principi dello scudo si applicano una volta trasferiti i dati negli Stati Uniti. I dati usati per la ricerca farmaceutica e per altri fini dovrebbero essere resi anonimi laddove appropriato.

b. Ricerca scientifica futura

i. I dati personali acquisiti per studi specifici della ricerca medica o farmaceutica svolgono spesso un ruolo prezioso nella ricerca scientifica futura. Se i dati personali raccolti per una determinata ricerca sono trasferiti a un'organizzazione statunitense nell'ambito dello scudo, l'organizzazione può usarli in una nuova attività di ricerca purché in occasione del primo studio sia stata data un'adeguata informativa e la possibilità di scelta. Nell'informativa dovrebbero figurare informazioni su tutti gli usi specifici futuri dei dati, quali seguito periodico, studio collegato o commercializzazione.

ii. È impossibile specificare tutti gli usi futuri dei dati, perché una nuova comprensione dei dati originari, le scoperte e i progressi della medicina e l'evoluzione della normativa e della sanità pubblica potrebbero determinare un nuovo uso a fini di ricerca. Se del caso, l'informativa dovrebbe quindi indicare chiaramente che i dati personali potranno essere usati in futuro per attività imprecisate di ricerca medica e farmaceutica. Se l'uso non è compatibile con le finalità generali di ricerca per cui i dati personali erano stati originariamente raccolti o per cui l'interessato ha successivamente dato il consenso, è necessario ottenere un nuovo consenso.

c. Ritiro da sperimentazione clinica

Il partecipante a una sperimentazione clinica può decidere di ritirarsi in qualsiasi momento, così come in qualsiasi momento gli può essere chiesto di ritirarsi. È tuttavia possibile trattare ancora, insieme agli altri, i dati personali che lo riguardano raccolti prima del ritiro, purché questa possibilità gli sia stata segnalata nell'informativa ricevuta quando ha accettato di partecipare alla sperimentazione.

d. Trasferimento per motivi di regolamentazione e di vigilanza

L'azienda produttrice di farmaci o di dispositivi medici può trasmettere all'ente regolatore statunitense, a fini di regolamentazione e di vigilanza, i dati personali relativi a sperimentazioni cliniche condotte nell'UE. Questo tipo di trasferimento è ammesso anche verso altre parti rispetto ai regolatori, quali centri della medesima impresa o altri ricercatori, nel rispetto dei principi sull'informativa e sulla scelta.

e. Studi in cieco

i. In molte sperimentazioni cliniche, per garantire l'obiettività i partecipanti e spesso anche gli sperimentatori non possono accedere alle informazioni sul tipo di trattamento assegnato a ciascun partecipante, perché l'accesso inficerebbe la validità della ricerca e dei relativi risultati. Non deve essere permesso al partecipante a una sperimentazione clinica in cieco di accedere ai dati sul trattamento assegnatogli, a condizione che questa limitazione gli sia stata indicata al momento dell'adesione alla sperimentazione e che la divulgazione di tali informazioni comprometta l'integrità della ricerca.

ii. Il consenso a partecipare alla sperimentazione a queste condizioni costituisce una ragionevole rinuncia al diritto di accesso. Dopo la conclusione della sperimentazione e l'analisi dei risultati il partecipante che lo richiede dovrebbe poter accedere ai dati che lo riguardano, rivolgendosi in primo luogo al medico o altro operatore sanitario da cui ha ricevuto il trattamento durante la sperimentazione oppure, in secondo luogo, all'organizzazione promotrice della ricerca.

f. Controllo della sicurezza e efficacia dei prodotti

Nella misura in cui l'osservanza dei principi dello scudo interferisca nell'osservanza degli obblighi normativi, l'azienda produttrice di farmaci o di dispositivi medici non è tenuta, relativamente agli aspetti di informativa, scelta, responsabilità in caso di ulteriore trasferimento e accesso, a applicarli nelle attività di controllo della sicurezza e efficacia dei prodotti, comprese la segnalazione degli eventi sfavorevoli e la tracciabilità dei pazienti/soggetti che usano determinati medicinali o dispositivi medici. Questo vale sia per la relazione presentata, ad

esempio, dall'operatore sanitario all'azienda produttrice di farmaci o di dispositivi medici sia per la relazione presentata da tale azienda a un ente pubblico, quale la *Food and Drug Administration* (Agenzia statunitense per gli alimenti e i medicinali).

g. Dati codificati

Per non rivelare l'identità dei singoli partecipanti lo sperimentatore principale assegna invariabilmente ai dati della ricerca una codifica unica fin dall'inizio. La chiave di codifica non è comunicata all'azienda farmaceutica promotrice della ricerca. Il ricercatore è l'unico a esserne in possesso, in modo da poter identificare il partecipante in circostanze particolari (ad esempio quando è necessario un supplemento d'assistenza medica). Il trasferimento dall'UE agli Stati Uniti dei dati così codificati non costituisce un trasferimento di dati personali per cui valgono i principi dello scudo.

15. **Documenti pubblici e informazioni di pubblico dominio**

a. L'organizzazione deve applicare ai dati personali ricavati da fonti di pubblico dominio i principi dello scudo sulla sicurezza, sull'integrità dei dati e la limitazione della finalità e su ricorso, controllo e responsabilità. Tali principi valgono anche per i dati personali ricavati da documenti pubblici, ossia dai dati detenuti da amministrazioni o enti pubblici di qualsiasi livello consultabili liberamente da chiunque.

b. Non è necessario applicare i principi sull'informativa, sulla scelta o sulla responsabilità in caso di ulteriore trasferimento delle informazioni dei documenti pubblici che non sono associate a elementi non pubblici, fermo restando il rispetto delle condizioni cui la giurisdizione competente subordina la consultazione. Parimenti, di norma non è necessario applicare i principi sull'informativa, sulla scelta o sulla responsabilità in caso di ulteriore trasferimento alle informazioni di pubblico dominio, a meno che il trasferente europeo indichi che le informazioni sono soggette a restrizioni che comportano per l'organizzazione l'obbligo di applicare tali principi per le finalità previste. L'organizzazione non è responsabile dell'uso di siffatte informazioni da parte di chi le ha ricavate da fonti pubblicate.

c. Qualora risulti che l'organizzazione ha deliberatamente divulgato informazioni personali in violazione dei principi per trarre beneficio da dette eccezioni, o consentire a terzi di trarne beneficio, l'organizzazione cessa di essere ammessa ai benefici dello scudo.

d. Non è necessario applicare il principio sull'accesso alle informazioni dei documenti pubblici che non sono associate ad altre informazioni personali, eccettuati i pochi dati usati per indicizzare o organizzare tali documenti; devono tuttavia essere rispettate le condizioni cui la giurisdizione competente subordina la consultazione. Quando invece informazioni ricavate da documenti pubblici sono associate a elementi non pubblici (salvo nel caso specifico illustrato in precedenza), l'organizzazione è tenuta a fornire l'accesso a tutte le informazioni, a meno che non rientrino in altre eccezioni consentite.

e. Come nel caso delle informazioni ricavate da documenti pubblici, non è necessario fornire l'accesso alle informazioni che sono già di pubblico dominio e che non sono associate a elementi non pubblici. Nel rispondere alla domanda di accesso l'organizzazione che si dedica professionalmente alla vendita di informazioni di pubblico dominio può farsi riconoscere il compenso richiesto abitualmente. In alternativa la persona può chiedere l'accesso alle informazioni che la riguardano all'organizzazione che ha compilato i dati in origine.

16. **Domande di accesso delle autorità pubbliche**

a. Ai fini della trasparenza sulle legittime domande di accesso a informazioni personali presentate dalle autorità pubbliche, l'organizzazione aderente allo scudo può pubblicare di propria iniziativa rapporti periodici sulla trasparenza, indicandovi il numero delle domande di accesso a informazioni personali ricevute dalle autorità pubbliche per motivi di applicazione della legge o di sicurezza nazionale, nella misura in cui tale pubblicazione sia ammessa dalla legge applicabile.

b. Insieme alle informazioni emananti dalla comunità dell'intelligence e a altri dati, le informazioni comunicate dalle organizzazioni aderenti allo scudo in detti rapporti possono essere usate per informare l'analisi annuale comune del funzionamento dello scudo conformemente ai principi.

c. Il fatto di non aver adempiuto all'avviso previsto dal principio sull'informativa, lettera a), punto xii), non osta né compromette la capacità dell'organizzazione di rispondere a una domanda legittima.

Allegato I

Modello arbitrale

Il presente allegato I stabilisce le condizioni alle quali l'organizzazione aderente allo scudo è tenuta a sottoporre il reclamo a procedimento arbitrale in virtù del principio su ricorso, controllo e responsabilità. La possibilità di arbitrato vincolante illustrata qui di seguito si applica a talune rivendicazioni accessorie relativamente ai dati contemplati dal regime dello scudo UE-USA per la privacy («scudo» o «regime»). L'obiettivo è mettere a disposizione della persona che opta per questa possibilità un meccanismo celere, indipendente e equo per dirimere il caso di asserita violazione dei principi rimasto irrisolto dopo il ricorso agli altri (eventuali) meccanismi previsti dallo scudo.

A. **Ambito di applicazione**

È messa a disposizione della persona la possibilità di ricorrere all'arbitrato per accertare, quanto alle rivendicazioni accessorie, se l'organizzazione aderente allo scudo abbia violato nei suoi confronti gli obblighi derivanti dai principi e se l'eventuale violazione non sia stata ancora riparata in tutto o in parte. Questa possibilità è prevista soltanto per detti fini: non è, ad esempio, percorribile per le eccezioni ai principi ([1]) o per le denunce vertenti sull'adeguatezza dello scudo.

B. **Forme di riparazione disponibili**

In questo contesto il collegio arbitrale dello scudo (composto da uno o da tre arbitri, secondo quanto concordato dalle parti) ha il potere di imporre un provvedimento equo, specifico alla persona e di carattere non pecuniario (quali accesso, rettifica, cancellazione o restituzione dei dati che la riguardano) a titolo di riparazione per la violazione dei principi limitatamente alla persona in questione. Sono questi i soli poteri del collegio arbitrale in tema di riparazioni. Nel valutare le riparazioni possibili, il collegio arbitrale è tenuto a tenere conto delle altre riparazioni già disposte da altri meccanismi nell'ambito dello scudo. Risarcimento danni, costi, commissioni o altre riparazioni non sono ammessi. Ciascuna parte sopporta le proprie spese di assistenza legale.

C. **Obblighi in fase prearbitrale**

Prima di avviare l'azione arbitrale la persona che opta per questa possibilità è tenuta a: 1) sottoporre la questione della presunta violazione all'organizzazione dandole la possibilità di risolverla nei tempi indicati nella parte III, punto 11, lettera d), punto i), dei principi; 2) rivolgersi al meccanismo di ricorso indipendente previsto dai principi, procedura che è gratuita per la persona; 3) per il tramite dell'autorità di protezione dei dati del proprio paese, sottoporre la questione al Dipartimento del Commercio dandogli la possibilità di adoperarsi per risolverla nei tempi indicati nella lettera dell'Amministrazione del commercio internazionale del Dipartimento del Commercio, procedura che è gratuita per la persona.

L'arbitrato non è una possibilità percorribile se la stessa violazione dei principi denunciata dalla stessa persona 1) è stata già sottoposta a arbitrato vincolante, 2) è stata oggetto di una decisione definitiva scaturita da un procedimento giudiziario in cui la persona era una delle parti oppure 3) è stata in passato oggetto di una transazione tra le parti. Non è percorribile neppure se un'autorità di protezione dei dati dell'UE 1) è competente in base alla parte III, punto 5, o punto 9, dei principi oppure 2) ha il potere di dirimere la presunta violazione direttamente con l'organizzazione. Il fatto che l'autorità di protezione dei dati abbia il potere di risolvere lo stesso caso di reclamo nei confronti di un titolare del trattamento dell'UE non preclude di per sé la soluzione arbitrale nei confronti di un soggetto giuridico diverso che non dipende da detta autorità.

D. **Carattere vincolante delle decisioni**

La decisione della persona di chiedere l'arbitrato vincolante è totalmente volontaria. La decisione arbitrale è vincolante per tutte le parti dell'arbitrato. Optando per l'arbitrato la persona rinuncia alla possibilità di chiedere in altra sede riparazione per l'asserita violazione; tuttavia, se il provvedimento equo di carattere non pecuniario non costituisce una riparazione integrale dell'asserita violazione, il ricorso all'arbitrato non preclude alla persona la possibilità di avviare l'azione di risarcimento danni altrimenti ammessa in sede giudiziaria.

([1]) Parte I, punto 5, dei principi.

E. **Riesame e esecuzione**

Ai sensi della legge federale sull'arbitrato ([1]), la persona e l'organizzazione aderente allo scudo possono sottoporre la decisione arbitrale al riesame e all'esecuzione in sede giudiziaria previsti dalla legge statunitense. L'istanza in tal senso deve essere presentata al giudice distrettuale federale con competenza territoriale sul luogo in cui si trova il centro di attività principale dell'organizzazione aderente allo scudo.

Scopo della possibilità di arbitrato è comporre singole controversie; le decisioni arbitrali non sono intese a costituire un precedente probante o vincolante per i casi che coinvolgono altre parti, compreso per i procedimenti arbitrali futuri, per i giudici dell'UE o degli USA e per i procedimenti dell'FTC.

F. **Collegio arbitrale**

Le parti scelgono gli arbitri dall'elenco di arbitri qui descritto.

In linea con la normativa vigente, il Dipartimento del Commercio degli Stati Uniti e la Commissione europea stilano un elenco di almeno 20 arbitri, scelti sulla base dell'indipendenza, dell'integrità e della competenza, tenuto conto dei criteri esposti qui di seguito.

L'arbitro:

1) rimane nell'elenco, salvo circostanza eccezionale o valido motivo, per un periodo di 3 anni rinnovabile per altri 3;

2) non riceve istruzioni da nessuna delle parti, da nessuna organizzazione aderente allo scudo né dagli Stati Uniti d'America, dall'UE o da uno Stato membro dell'UE, così come da nessun'altra autorità pubblica o autorità di esecuzione, né è associato a nessuno di tali soggetti;

3) è abilitato a esercitare la professione forense negli Stati Uniti d'America ed è esperto di diritto della privacy statunitense con competenze in materia di normativa dell'UE sulla protezione dei dati.

G. **Procedure arbitrali**

In linea con la normativa applicabile, entro 6 mesi dall'adozione della decisione di adeguatezza il Dipartimento del Commercio e la Commissione europea concordano l'adozione di una serie esistente e consolidata di procedure arbitrali statunitensi (quali AAA o JAMS) per disciplinare il procedimento dinanzi al collegio arbitrale dello scudo, ferme restando tutte le considerazioni esposte qui di seguito.

1. Dopo aver obbligatoriamente assolto i citati obblighi della fase prearbitrale, la persona può avviare l'arbitrato vincolante trasmettendo un «avviso» all'organizzazione. L'avviso riporta una sintesi delle misure adottate conformemente alla lettera C per risolvere il caso, una descrizione della presunta violazione e, a scelta della persona, documentazione di supporto e/o l'esposizione delle ragioni di diritto relative alla contestazione.

([1]) Ai sensi della legge federale sull'arbitrato, capo 2, la convenzione arbitrale o il lodo arbitrale scaturito da un rapporto giuridico, contrattuale o no, che è considerato commerciale, compresi l'operazione, il contratto o la convenzione di cui all'articolo 2 della legge federale sull'arbitrato, rientra nella convenzione, del 10 giugno 1958, per il riconoscimento e l'esecuzione delle sentenze arbitrali straniere («convenzione di New York») (21 U.S.T. 2519, T.I.A.S. n. 6997) (Codice degli Stati Uniti d'America, titolo 9, articolo 202). La legge federale sull'arbitrato dispone inoltre che la convenzione o il lodo scaturito da un siffatto rapporto in cui sono coinvolti esclusivamente cittadini statunitensi rientri nella convenzione di New York solo se il rapporto interessa beni ubicati all'estero, prevede l'esecuzione all'estero o presenta altrimenti un ragionevole legame con uno o più Stati esteri (*Ibid.*). A norma del capo 2, ciascuna parte dell'arbitrato può adire il giudice competente ai sensi del capo stesso per ottenere un provvedimento di conferma del lodo nei confronti di un'altra parte arbitrale. Il giudice conferma il lodo salvo se riscontra uno dei motivi di rigetto o di differimento del riconoscimento o dell'esecuzione del lodo indicati nella convenzione di New York (*Ibid.*, articolo 207). Sempre a norma del capo 2, i giudici distrettuali degli Stati Uniti d'America sono competenti dell'azione o del procedimento avviato in virtù della convenzione di New York, a prescindere dall'importo oggetto della controversia (*Ibid.*, articolo 203).
Il capo 2 stabilisce inoltre che il capo 1 si applica alle azioni e ai procedimenti avviati a norma del capo stesso nella misura in cui non via sia conflitto con il capo stesso o con la convenzione di New York quale ratificata dagli Stati Uniti (*Ibid.*, articolo 208). Il capo 1 afferma a sua volta la validità, irrevocabilità e esecutività della disposizione scritta di un contratto vertente su un'operazione che comporta aspetti commerciali la quale preveda di risolvere per via arbitrale la controversia sorta da tale contratto o operazione, così come il rifiuto di eseguire la totalità o parte del contratto o dell'operazione, e parimenti la validità, irrevocabilità e esecutività dell'accordo scritto di sottoporre a arbitrato una preesistente controversia sorta da detto contratto, operazione o rifiuto, fatti salvi i motivi di legge o equity che determinano la revoca dei contratti (*Ibid.*, articolo 2). Sempre a norma del capo 1, ciascuna parte arbitrale può adire il giudice indicato dallo stesso capo 1 per ottenere un provvedimento di conferma del lodo; in tal caso, il giudice deve emanare tale provvedimento, a meno che il lodo sia cassato, modificato o rettificato secondo quanto prescritto negli articoli 10 e 11 della stessa legge federale sull'arbitrato (*Ibid.*, articolo 9).

2. Sono predisposte procedure per evitare che la stessa presunta violazione asserita dalla stessa persona sia trattata due volte o determini due riparazioni.

3. L'FTC può intervenire parallelamente all'arbitrato.

4. All'arbitrato non può partecipare nessun rappresentante degli USA, dell'UE o di uno Stato membro dell'UE, così come di nessun'altra autorità pubblica o autorità di esecuzione; in via eccezionale, a richiesta della persona dell'UE le autorità di protezione dei dati dell'UE possono assisterla solo nella redazione dell'avviso, ma non possono avere accesso alla documentazione esibita né a altro materiale connesso all'arbitrato.

5. Il procedimento arbitrale si svolge negli Stati Uniti d'America; la persona può optare per la partecipazione in video o via telefono, che le è fornita gratuitamente. Non è obbligatorio presenziare di persona.

6. Salvo diversa decisione delle parti, il procedimento arbitrale si svolge in lingua inglese. Su richiesta motivata e tenuto conto del fatto che la persona sia rappresentata da un legale o no, è fornita alla persona, gratuitamente, l'interpretazione nell'udienza arbitrale e la traduzione della documentazione arbitrale, a meno che il collegio ritenga che, nelle circostanze specifiche, ciò comporti costi ingiustificati o sproporzionati.

7. È garantita la riservatezza della documentazione sottoposta agli arbitri, che è usata esclusivamente in relazione all'arbitrato.

8. Se necessario, può essere ammessa l'esibizione di documentazione specifica alla persona; le parti garantiscono la riservatezza della documentazione così esibita, che è usata esclusivamente in relazione all'arbitrato.

9. Salvo diversa decisione delle parti, il procedimento arbitrale dovrebbe concludersi entro 90 giorni dalla consegna dell'avviso all'organizzazione.

H. **Costi**

Gli arbitri devono adottare provvedimenti ragionevoli per ridurre al minimo spese e onorari dei procedimenti arbitrali.

Nel rispetto della legge applicabile, il Dipartimento del Commercio agevola la costituzione di un fondo cui ciascuna organizzazione aderente allo scudo è tenuta a versare una quota annua a copertura delle spese, compresi gli onorari degli arbitri; l'entità della quota è basata in parte sulla dimensione dell'organizzazione ed è limitata da determinati importi massimi («massimali»), in consultazione con la Commissione europea. Il fondo sarà gestito da un terzo, che riferisce periodicamente sul suo funzionamento. In sede di analisi annuale, il Dipartimento del Commercio e la Commissione europea esaminano il funzionamento del fondo, compresa la necessità di adeguare le quote o i massimali, e considerano tra l'altro il numero dei procedimenti arbitrali, con i relativi costi e tempi, muovendo dal presupposto condiviso che il sistema non deve comportare un onere finanziario eccessivo per le organizzazioni aderenti allo scudo. Gli onorari degli avvocati non sono contemplati dalla presente disposizione né da nessun fondo costituito in virtù della presente disposizione.

ALLEGATO III

Lettera del segretario di Stato statunitense John Kerry

7 luglio 2016

Gentile Commissaria Jourová,

mi rallegro dell'intesa raggiunta tra Unione europea e Stati Uniti d'America sullo scudo per la privacy, che includerà un meccanismo di mediazione attraverso il quale le autorità dell'UE potranno presentare, per conto delle persone dell'UE, richieste vertenti sulle pratiche di intelligence dei segnali seguite dagli Stati Uniti.

Il 17 gennaio 2014 il presidente Barack Obama ha annunciato importanti riforme nel settore dell'intelligence, esposte nella direttiva presidenziale 28 (PPD-28). A norma della PPD-28, ho nominato Catherine A. Novelli, Sottosegretaria di Stato e Prima coordinatrice della diplomazia internazionale per le tecnologie dell'informazione, referente per i governi stranieri che si pongono interrogativi sulle attività di intelligence dei segnali condotte dagli Stati Uniti d'America. Muovendo da tale ruolo ho istituito per lo scudo per la privacy un meccanismo di mediazione nei termini illustrati nell'allegato A, che sono stati aggiornati dopo la mia lettera del 22 febbraio 2016. Ho investito la Sottosegretaria Novelli della funzione di mediatrice. La Sottosegretaria Novelli è indipendente dalla comunità dell'intelligence statunitense e riferisce direttamente a me.

Ho dato istruzione al personale del Dipartimento di destinare le risorse necessarie all'attuazione di questo nuovo meccanismo di mediazione, che confido sarà uno strumento efficace per rispondere alle preoccupazioni delle persone dell'UE.

La prego di accogliere, signora Commissaria,
i sensi della mia più alta stima.

John F. Kerry

Allegato A

Meccanismo di mediazione dello scudo UE-USA per la privacy in materia di intelligence dei segnali

In considerazione dell'importanza del regime dello scudo UE-USA per la privacy («scudo» o «regime»), il presente memorandum stabilisce l'iter di attuazione di un nuovo meccanismo sull'intelligence dei segnali in conformità alla direttiva presidenziale 28 (PPD-28) ([1]).

Il 17 gennaio 2014 il presidente Obama ha annunciato importanti riforme nel settore dell'intelligence in un discorso in cui ha sottolineato come l'impegno degli USA in questo senso contribuisca a proteggere non solo gli Stati Uniti, ma anche i suoi amici e alleati. Quest'impegno sarà fruttuoso solo se i comuni cittadini degli altri paesi potranno contare sul fatto che gli Stati Uniti rispettano anche la loro vita privata. Contestualmente il presidente Obama ha annunciato l'emanazione di una nuova direttiva presidenziale, la PPD-28, per precisare che cosa gli USA fanno, e che cosa invece non fanno, nelle attività di sorveglianza all'estero.

L'articolo 4, lettera d), della PPD-28 incarica il segretario di Stato di nominare un Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione («Primo coordinatore» o «Prima coordinatrice») che funga da referente per i governi stranieri che si pongono interrogativi sulle attività di intelligence dei segnali condotte dagli Stati Uniti d'America. A partire da gennaio 2015 la Sottosegretaria Catherine Novelli riveste la carica di Prima coordinatrice.

Il presente memorandum illustra il nuovo meccanismo cui la Prima coordinatrice si atterrà, secondo modalità consolidate conformi alla legge e alla politica degli Stati Uniti d'America, per facilitare il trattamento delle domande di accesso motivate dalla sicurezza nazionale ai dati trasmessi dall'Unione europea agli Stati Uniti nell'ambito dello scudo, delle clausole contrattuali tipo, delle norme vincolanti d'impresa, delle «deroghe» ([2]) o delle «eventuali deroghe future» ([3]), così come la risposta a tali domande.

1. **Meccanismo di mediazione dello scudo** — La Prima coordinatrice svolge la funzione di Mediatore e, in base alle necessità nomina altri funzionari del Dipartimento di Stato per assisterla nell'esecuzione dei compiti descritti nel presente memorandum (qui di seguito la Prima coordinatrice e i vari funzionari incaricati di tali compiti sono denominati «Mediatore dello scudo» o «Mediatore»). Il Mediatore dello scudo opera in stretta collaborazione con i funzionari di altri ministeri e enti cui la legge e la politica degli Stati Uniti conferiscono competenze di trattamento delle domande. Il Mediatore è indipendente dalla comunità dell'intelligence statunitense e riferisce direttamente al segretario di Stato, il quale assicura che svolga la sua funzione con obiettività e senza indebite ingerenze che possano influire sulla risposta apportata.

2. **Coordinamento efficace** — Per rispondere adeguatamente alla richiesta proveniente dall'organo di trattamento e trasmissione dei reclami delle persone dell'UE, il Mediatore dello scudo può contare sulla collaborazione e il coordinamento efficaci con gli organi di vigilanza indicati qui di seguito. Se la domanda verte sulla compatibilità della

([1]) Se la decisione della Commissione europea sull'adeguatezza della tutela offerta dallo scudo UE-USA per la privacy si applicherà anche a Islanda, Liechtenstein e Norvegia, la presente documentazione riguarderà anche tali tre paesi oltre all'Unione europea. In tal caso, i riferimenti all'UE e ai suoi Stati membri si intendono quindi comprensivi di Islanda, Liechtenstein e Norvegia.

([2]) In questo contesto per «deroghe» s'intendono uno o più trasferimenti commerciali effettuati se si verifica una delle condizioni seguenti: a) l'interessato ha manifestato in maniera inequivocabile il proprio consenso al trasferimento previsto; b) il trasferimento è necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero per l'esecuzione di misure precontrattuali prese a richiesta dell'interessato; c) il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un terzo a favore dell'interessato; d) il trasferimento è necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, ovvero per accertare, esercitare o difendere un diritto in via giudiziale; e) il trasferimento è necessario per la salvaguardia di interessi vitali dell'interessato; f) il trasferimento è effettuato a partire da un registro che, a norma delle leggi o dei regolamenti vigenti, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, purché sussistano i requisiti per la consultazione previsti dalla normativa.

([3]) In questo contesto per «eventuali deroghe future» s'intendono uno o più trasferimenti commerciali effettuati se si verifica una delle condizioni seguenti, purché la condizione costituisca un legittimo presupposto per il trasferimento di dati personali dall'UE agli USA: a) l'interessato ha esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi cui si espone con siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; c) se non si applica nessuna delle altre deroghe o eventuali deroghe future e se il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato, il titolare del trattamento ha valutato tutte le circostanze relative al trasferimento e, sulla base di tale valutazione, ha addotto garanzie adeguate relativamente alla protezione dei dati personali.

sorveglianza con la legge statunitense, il Mediatore può collaborare con uno degli organi indipendenti di vigilanza che hanno poteri investigativi.

a. Il Mediatore opera in stretta collaborazione con altri enti dell'amministrazione statunitense, compresi i competenti organi indipendenti di vigilanza, affinché le domande complete siano trattate e risolte conformemente alle leggi e politiche applicabili. In particolare, il Mediatore ha facoltà di operare in stretto coordinamento con l'Ufficio del direttore dell'intelligence nazionale, il Dipartimento della Giustizia e, secondo i casi, altri dipartimenti e enti statunitensi attivi nel settore della sicurezza nazionale degli Stati Uniti, così come con gli ispettori generali, gli addetti alla legge sulla libertà d'informazione e i funzionari che si occupano delle libertà civili e del rispetto della vita privata.

b. Il governo degli Stati Uniti ricorre ai meccanismi di coordinamento e supervisione in materia di sicurezza nazionale esistenti nei diversi dipartimenti e enti per agevolare il Mediatore nel compito di rispondere, conformemente alla parte 4, lettera e), alle domande complete di cui alla parte 3, lettera b).

c. Il Mediatore può rinviare le questioni relative alle domande all'Autorità per la tutela della vita privata e delle libertà civili degli USA perché le esamini.

3. **Presentazione delle domande**

a. La domanda è dapprima presentata all'autorità di vigilanza dello Stato membro competente della vigilanza sui servizi di sicurezza nazionale e/o del trattamento dei dati personali da parte delle autorità pubbliche. La domanda è inoltrata al Mediatore da un organo centralizzato a livello dell'UE (di seguito, collettivamente, «organo di trattamento e trasmissione dei reclami presentati da persone dell'UE» o «organo di reclamo»).

b. L'organo di trattamento e trasmissione dei reclami presentati da persone dell'UE accerta che la domanda sia completa:

i) verificando l'identità della persona e il fatto che agisca per proprio conto e non in rappresentanza di un governo o di un'organizzazione intergovernativa;

ii) verificando che la domanda sia redatta per iscritto e includa almeno le seguenti indicazioni:

— tutte le informazioni che ne costituiscono il fondamento,

— la natura delle informazioni o della riparazione richieste,

— eventualmente, l'ente o gli enti dell'amministrazione degli Stati Uniti che si ritiene siano implicati,

— le altre misure attuate per ottenere le informazioni o la riparazione richieste e la risposta ricevuta in tale contesto;

iii) verificando che la domanda verta su dati che si può ragionevolmente presumere siano stati trasferiti dall'UE agli USA nell'ambito dello scudo, delle clausole contrattuali tipo, delle norme vincolanti d'impresa, delle deroghe o delle eventuali deroghe future;

iv) accertando *prima facie* che la domanda non sia futile, vessatoria o in malafede.

c. Per essere completa e essere quindi trattata dal Mediatore dello scudo conformemente al presente memorandum, la domanda non deve necessariamente dimostrare che il governo degli Stati Uniti d'America abbia effettivamente avuto accesso ai dati che riguardano il richiedente attraverso attività di intelligence dei segnali.

4. **Impegno a comunicare con l'organo trasmittente di trattamento dei reclami presentati da persone dell'UE**

a. Il Mediatore dello scudo accusa ricevuta della domanda all'organo trasmittente di trattamento dei reclami presentati da persone dell'UE («organo trasmittente»).

b. Il Mediatore effettua una prima verifica per controllare che la domanda sia completa secondo quanto previsto alla parte 3, lettera b). Se rileva lacune o ha dubbi circa la completezza della domanda, il Mediatore si adopera per risolvere la questione assieme all'organo trasmittente.

c. Se per facilitare un trattamento adeguato della domanda occorrono altre informazioni o l'intervento specifico della persona che l'ha presentata in origine, il Mediatore ne informa l'organo trasmittente.

d. Il Mediatore dello scudo segue l'iter della domanda e aggiorna di conseguenza l'organo trasmittente.

e. Se la domanda risulta completa conformemente alla parte 3 del presente memorandum, il Mediatore comunica tempestivamente una risposta adeguata all'organo trasmittente, fermo restando l'obbligo permanente di proteggere le informazioni secondo quanto disposto dalle leggi e politiche vigenti. Il Mediatore risponde all'organo trasmittente confermando i) che il reclamo è stato esaminato adeguatamente e ii) che sono stati rispettati le leggi, i regolamenti, i decreti e le direttive presidenziali e le politiche degli enti che negli Stati Uniti disciplinano le limitazioni e le garanzie esposte nella lettera dell'Ufficio del direttore dell'intelligence nazionale (ODNI) oppure, se non sono stati rispettati, che l'inosservanza è stata nel frattempo sanata. Il Mediatore non conferma né nega che la persona sia stata sottoposta a sorveglianza né indica la specifica misura correttiva applicata. Come illustrato in maggiore dettaglio nella parte 5, le domande vertenti sulla legge sulla libertà d'informazione sono trattate a norma della legge e dei regolamenti applicabili.

f. Il Mediatore comunica direttamente con l'organo di trattamento e trasmissione dei reclami presentati da persone dell'UE, cui compete di comunicare a sua volta con la persona che ha presentato la domanda. Le comunicazioni dirette che s'iscrivono in uno dei processi descritti qui di seguito si svolgono secondo le procedure vigenti.

g. Gli impegni assunti con il presente memorandum non si applicano al generico reclamo in cui si asserisce che lo scudo UE-USA per la privacy non è conforme ai requisiti dell'Unione europea in materia di protezione dei dati. Nell'assumere gli impegni previsti dal presente memorandum la Commissione europea e il governo degli Stati Uniti d'America concordano che, data la portata degli stessi, possono porsi problemi di limitatezza delle risorse, compreso per le domande vertenti sulla legge sulla libertà di informazione. Qualora l'esecuzione delle funzioni del Mediatore dello scudo richieda più risorse di quelle ragionevolmente prevedibili e impedisca l'assolvimento degli impegni assunti, il governo degli Stati Uniti discute con la Commissione europea gli eventuali adattamenti necessari per risolvere la situazione.

5. **Richiesta di informazioni** — È possibile presentare domanda di accesso ai documenti del governo degli Stati Uniti a norma della legge sulla libertà di informazione, che ne disciplina anche il trattamento.

a. Detta legge, che consente a chiunque, indipendentemente dalla cittadinanza, di chiedere l'accesso ai documenti esistenti degli enti federali, è codificata nel Codice degli Stati Uniti, titolo 5, articolo 552. La legge e le informazioni supplementari al riguardo sono consultabili agli indirizzi www.FOIA.gov e http://www.justice.gov/oip/foia-resources. In ogni ente è presente un addetto alla legge sulla libertà di informazione e ogni ente indica, sul proprio sito web pubblico, le modalità con cui presentargli una richiesta nell'ambito di tale legge. Vigono tra gli enti procedure di consultazione in caso di richiesta presentata nell'ambito della legge che implica documenti detenuti da un ente diverso.

b. A titolo di esempio:

i) l'Ufficio del direttore dell'intelligence nazionale (ODNI) ha creato il portale ODNI dedicato alla legge sulla libertà di informazione all'indirizzo http://www.dni.gov/index.php/about-this-site/foia. Il portale informa circa la presentazione della domanda, la verifica dello stato di una domanda già presentata e l'accesso alle informazioni emanate e pubblicate dall'ODNI in base alla legge sulla libertà di informazione. Il portale comprende collegamenti ipertestuali alle corrispondenti pagine di altri servizi della comunità dell'intelligence, all'indirizzo http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) l'Ufficio per la politica informativa del Dipartimento della Giustizia fornisce informazioni complete circa la legge sulla libertà di informazione all'indirizzo http://www.justice.gov/oip. Si tratta non soltanto di informazioni sulle modalità con cui presentare al Dipartimento della Giustizia una domanda nell'ambito di tale legge, ma anche di orientamenti, rivolti al governo degli Stati Uniti, sull'interpretazione e l'applicazione degli obblighi in essa previsti.

c. Ai sensi della legge sulla libertà di informazione l'accesso ai documenti del governo è soggetto a determinate esenzioni stabilite espressamente, tra cui limitazioni dell'accesso alle informazioni classificate sulla sicurezza nazionale, alle informazioni personali di terzi e alle informazioni relative a indagini giudiziarie; queste esenzioni sono comparabili alle limitazioni imposte da ciascuno Stato membro dell'UE tramite la rispettiva legge sull'accesso alle informazioni. Le limitazioni si applicano nello stesso modo sia agli americani sia agli stranieri.

d. Avverso la decisione riguardante l'accesso a documenti richiesto nell'ambito della legge sulla libertà di informazione è possibile un ricorso amministrativo e, quindi, un ricorso dinanzi a un giudice federale. Il giudice è tenuto a stabilire nuovamente se l'accesso ai documenti sia negato legittimamente (Codice degli Stati Uniti d'America, titolo 5, articolo 552(a)(4)(B)] e può obbligare il governo a consentirlo. In alcuni casi il giudice ha ribaltato la decisione con cui governo aveva stabilito che l'acceso dovesse essere negato perché si trattava di informazioni classificate. Il risarcimento pecuniario non è possibile, ma il giudice può disporre il rimborso delle spese legali.

6. **Richiesta di ulteriore intervento** — La domanda vertente su una presunta violazione della legge o irregolarità di altro tipo è deferita al competente ente pubblico statunitense, compresi gli organi indipendenti di vigilanza, cui è conferito il potere di esaminare la domanda e risolvere la questione della mancata conformità nelle linee illustrate qui di seguito.

a. Gli ispettori generali sono indipendenti per legge, godono di ampi poteri di indagine, verifica e esame dei programmi, anche in materia di frode e abuso o violazione della legge, e hanno facoltà di raccomandare misure correttive.

i) La legge del 1978 sugli ispettori generali, e successive modifiche, ha istituito gli ispettori generali federali configurandoli come unità indipendenti e obiettive inserite nella maggior parte degli enti e incaricandoli di combattere gli sprechi, le frodi e gli abusi nei programmi e nelle operazioni del rispettivo ente. A tal fine ciascun ispettore generale è responsabile dell'esecuzione delle verifiche e indagini riguardanti i programmi e le operazioni dell'ente. Svolge inoltre una funzione di indirizzo e di coordinamento per le attività volte a promuovere economia, efficienza ed efficacia e a prevenire e accertare frodi e abusi nei programmi e nelle operazioni dell'ente, e raccomanda le politiche in tal senso.

ii) Ciascun servizio della comunità dell'intelligence dispone di un proprio Ufficio dell'ispettore generale, incaricato tra l'altro di vigilare sulle attività di intelligence esterna. Sono stati pubblicati vari rapporti degli ispettori generali dedicati a programmi di intelligence.

iii) A titolo di esempio:

— l'Ufficio dell'ispettore generale della comunità dell'intelligence («Ufficio») è stato istituito in applicazione dell'articolo 405 della legge autorizzativa dell'intelligence per l'esercizio finanziario 2010. Per tutta la comunità dell'intelligence l'Ufficio è responsabile delle verifiche, indagini, ispezioni e valutazioni atte a individuare e risolvere i rischi sistemici, le vulnerabilità e le carenze trasversali ai compiti degli enti che la compongono, in modo da produrre un effetto positivo generale in termini di economie e efficienza. Relativamente ai programmi e alle attività dell'ODNI e/o della comunità dell'intelligence, l'Ufficio è autorizzato a esaminare i reclami e le informazioni vertenti su presunte violazioni della legge, dei regolamenti o di altre disposizioni e su sprechi, frodi, abusi di potere e pericoli rilevanti o specifici per la salute e la sicurezza pubbliche. L'Ufficio indica le modalità con cui contattarlo direttamente per presentargli un rapporto all'indirizzo http://www.dni.gov/index.php/about-this-site/contact-the-ig,

— l'Ufficio dell'ispettore generale presso il Dipartimento della Giustizia degli USA («Ufficio») è un ente indipendente istituito per legge con il compito di individuare e scoraggiare sprechi, frodi, abusi e irregolarità nei programmi e tra il personale di tale Dipartimento e di promuovere l'economia e l'efficienza in detti programmi. L'Ufficio indaga sulle presunte violazioni di diritto civile e penale da parte dei dipendenti del Dipartimento della Giustizia, del quale verifica e ispeziona anche i programmi. È competente di tutte le denunce di irregolarità sporte nei confronti di dipendenti del Dipartimento della Giustizia, inclusi il *Federal Bureau of Investigation* (FBI), la *Drug Enforcement Administration* (DEA), il *Federal Bureau of Prisons* (Amministrazione penitenziaria federale), l'*U.S. Marshals Service* (USMS), il *Bureau of Alcohol, Tobacco, Firearms, and Explosives* (ATF), gli uffici dei procuratori e i dipendenti inseriti in altre divisioni o uffici del Dipartimento. (Esiste un'unica eccezione: la presunta irregolarità compiuta da un procuratore del Dipartimento o da un dipendente con funzioni di applicazione della legge e relativa

all'esercizio del potere di tale procuratore di indagare, contestare in giudizio o prestare consulenza legale ricade nella responsabilità dell'Ufficio per la responsabilità professionale interno al Dipartimento.) L'articolo 1001 del *Patriot Act* statunitense, adottato con legge del 26 ottobre 2001, incarica inoltre l'ispettore generale di valutare le informazioni e ricevere i reclami vertenti su un presunto abuso dei diritti e libertà civili ad opera dei dipendenti del Dipartimento della Giustizia. L'Ufficio ha un sito web pubblico (https://www.oig.justice.gov) che mette a disposizione una «linea rossa» per la presentazione dei reclami (https://www.oig.justice.gov/hotline/index.htm).

b. Anche gli uffici e i servizi per la tutela della vita privata e le libertà civili del governo degli Stati Uniti hanno responsabilità in materia. A titolo di esempio:

i) l'articolo 803 della legge del 2007 sull'attuazione delle raccomandazioni della Commissione sui fatti dell'11 settembre, codificata nel Codice degli Stati Uniti d'America, titolo 42, articolo 2000-ee1, istituisce la figura di addetto alla tutela della vita privata e alle libertà civili presso alcuni dipartimenti e enti (tra cui il Dipartimento di Stato, il Dipartimento della Giustizia e l'ODNI). A norma dell'articolo 803, tali addetti svolgono la funzione di consigliere principale per assicurare, tra l'altro, che il dipartimento, l'ente o il soggetto predisponga procedure adeguate per trattare le denunce di persone che lo accusano di aver commesso nei loro confronti una violazione della privacy o delle libertà civili;

ii) l'Ufficio per la tutela della vita privata e le libertà civili dell'ODNI («Ufficio») è guidato dal responsabile della tutela delle libertà civili, funzione istituita dalla legge sulla sicurezza nazionale del 1948 e successive modifiche. Rientrano tra i compiti dell'Ufficio la verifica della presenza di tutele adeguate della vita privata e delle libertà civili nelle politiche e procedure seguite dai soggetti appartenenti alla comunità dell'intelligence e la valutazione e l'esame delle denunce di presunto abuso o violazione delle libertà civili e della privacy nei programmi e nelle attività dell'ODNI. L'Ufficio mette a disposizione del pubblico informazioni sul proprio sito web (www.dni.gov/clpo), comprese le istruzioni su come sporgere reclamo. Se riceve un reclamo vertente sul rispetto della privacy o delle libertà civili nei programmi e nelle attività della comunità dell'intelligence, l'Ufficio coordina con gli altri soggetti di quella comunità l'ulteriore trattamento da riservargli in tale ambito. Si rilevi che anche l'Agenzia per la sicurezza nazionale (NSA) dispone di un Ufficio per la tutela della vita privata e le libertà civili, che informa delle responsabilità che gli incombono sul proprio sito web (https://www.nsa.gov/civil_liberties/). Se dalle informazioni risulta che un dato ente non rispetta i requisiti in materia di privacy (ad esempio, un obbligo imposto dall'articolo 4 della PPD-28), esistono meccanismi di conformità che permettono di esaminare e risolvere il problema. Gli enti sono tenuti a segnalare questi casi all'ODNI ai sensi della PPD-28;

iii) l'Ufficio per la tutela della vita privata e le libertà civili presso il Dipartimento della Giustizia («Ufficio») svolge un ruolo di supporto nell'espletamento dei compiti e delle responsabilità del responsabile della tutela della vita privata e delle libertà civili del Dipartimento. Compito principale dell'Ufficio è tutelare la privacy e le libertà civili del popolo americano attraverso la valutazione, la supervisione e il coordinamento delle operazioni del Dipartimento che interessano la vita privata. L'Ufficio: presta consulenza legale e indirizzo ai servizi del Dipartimento; provvede a che il Dipartimento sia conforme in tema di tutela della vita privata, anche sotto il profilo della conformità alla legge sulla privacy del 1974, alle disposizioni in materia della legge del 2002 sull'e-government e della legge sulla gestione a livello federale della sicurezza delle informazioni e alle circolari amministrative emanate in applicazione di tali leggi; mette a punto e impartisce nel Dipartimento la formazione sulla privacy; assiste il responsabile della tutela della vita privata e delle libertà civili nell'elaborazione della politica del Dipartimento in materia di privacy; prepara le relazioni sulla privacy destinate al presidente e al Congresso e esamina le pratiche di gestione delle informazioni seguite dal Dipartimento per assicurarne la conformità alla tutela della vita privata e delle libertà civili. L'Ufficio illustra le sue competenze al pubblico all'indirizzo http://www.justice.gov/opcl;

iv) a norma del Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee e ss, l'Autorità per la tutela della vita privata e delle libertà civili («Autorità») tiene costantemente sotto controllo: i) le politiche e le procedure (con la relativa attuazione) seguite dai dipartimenti, dagli enti e dai soggetti dell'esecutivo per proteggere gli Stati Uniti dal terrorismo, al fine di verificare che rispettino la privacy e le libertà civili; ii) le altre iniziative dell'esecutivo in tal senso, per stabilire se garantiscano una tutela adeguata della vita privata e delle libertà civili e siano conformi alle leggi, ai regolamenti e alle politiche applicabili in materia. L'Autorità riceve e esamina segnalazioni e altre informazioni dagli addetti alla tutela della vita privata e dagli addetti alle libertà civili, a cui rivolge, se del caso, raccomandazioni riguardo alle attività svolte. L'articolo 803 della legge del 2007 sull'attuazione delle raccomandazioni della Commissione sui fatti dell'11 settembre, codificata nel Codice degli Stati Uniti d'America, titolo 42, articolo 2000-ee1, incarica gli addetti alla tutela della vita privata e alle libertà civili di otto soggetti federali (tra cui il segretario della difesa, il segretario per la sicurezza interna, il Direttore dell'intelligence nazionale e il Direttore della Central Intelligence Agency (CIA)], e di qualsiasi altro

soggetto indicato dall'Autorità, di presentare a questa relazioni periodiche in cui siano indicati anche il numero, la natura e il trattamento riservato ai reclami per presunta violazione ricevuti dal rispettivo ente. La legge costitutiva dell'Autorità la incarica di ricevere dette relazioni e, se del caso, di rivolgere agli addetti alla tutela della vita privata e alle libertà civili raccomandazioni riguardo alle attività che svolgono.

ALLEGATO IV

Lettera della presidente della Commissione federale del Commercio Edith Ramirez

7 luglio 2016

VIA EMAIL

Věra Jourová
Commissaria per la Giustizia, i consumatori e la parità di genere
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissaria Jourová,

la Commissione federale del Commercio (FTC) si pregia di illustrarLe le modalità di esecuzione del nuovo regime dello scudo UE-USA per la privacy («scudo» o «regime»). È nostra convinzione che il regime svolgerà un ruolo fondamentale per favorire operazioni commerciali attente alla tutela della vita privata in un mondo sempre più interconnesso. Permetterà alle imprese di effettuare operazioni importanti nell'economia globale, consentendo nel contempo ai consumatori dell'UE di salvaguardare tutele rilevanti in materia di privacy. Da tempo impegnata a tutelare la vita privata attraverso le frontiere, l'FTC attribuirà un'elevata priorità all'applicazione del nuovo regime. Illustriamo qui di seguito la solida tradizione che l'FTC vanta in generale in materia di applicazione delle regole della privacy, anche relativamente al programma originario dell'approdo sicuro e all'impostazione seguita per l'applicazione del nuovo regime.

L'FTC si è impegnata a dare esecuzione al programma dell'approdo sicuro per la prima volta nel 2000, quando l'allora presidente Robert Pitofsky trasmise alla Commissione europea una lettera in cui l'FTC s'impegnava a far rispettare attivamente e rigorosamente i principi di tale programma. L'FTC non è mai venuta meno all'impegno assunto, come dimostrano le quasi 40 azioni coercitive avviate, le numerose indagini supplementari e la cooperazione intrattenuta con le autorità europee di protezione dei dati.

Dopo che, nel novembre 2013, la Commissione europea aveva espresso perplessità circa l'amministrazione e l'applicazione del programma dell'approdo sicuro, l'FTC e il Dipartimento del Commercio degli Stati Uniti avviarono consultazioni con essa per sondare le possibilità di rafforzamento del programma. Il 6 ottobre 2015, a consultazioni aperte, con la sentenza nella causa *Schrems* la Corte di giustizia dell'Unione europea ha, tra l'altro, invalidato la decisione con cui la Commissione europea aveva decretato l'adeguatezza del programma dell'approdo sicuro. A seguito di questa decisione l'FTC ha continuato la collaborazione stretta con il Dipartimento del Commercio e la Commissione europea, nel tentativo di rafforzare le tutele garantite alle persone dell'UE in termini di privacy. Lo scudo per la privacy è il risultato di queste consultazioni. Così come per l'approdo sicuro, l'FTC s'impegna a dare attivamente e rigorosamente applicazione al nuovo regime. La presente lettera sancisce quest'impegno.

L'FTC s'impegna in particolare su quattro aspetti fondamentali: 1) attribuzione di priorità ai casi e indagini; 2) soluzione dei casi di millantata appartenenza allo scudo; 3) controllo continuato sui provvedimenti coercitivi; 4) potenziamento dei rapporti e della cooperazione esecutiva con le autorità di protezione dei dati dell'UE. Seguono informazioni particolareggiate su ciascuno di detti impegni, cui si aggiungono un inquadramento del contesto in cui s'iscrive il ruolo dell'FTC per la tutela della privacy dei consumatori e l'applicazione dell'approdo sicuro e una descrizione del più vasto panorama della privacy negli USA ([1]).

I. CONTESTO GENERALE

A. **Attività dell'FTC per la politica e l'applicazione in materia di privacy**

L'FTC gode di ampi poteri di applicazione nella sfera civile al fine di promuovere la tutela dei consumatori e la concorrenza in ambito commerciale. In virtù del mandato di tutela dei consumatori conferitole, l'FTC dà applicazione

([1]) Ulteriori informazioni sulle leggi federali e statali statunitensi in materia di privacy sono riportate nell'allegato A; una sintesi delle recenti azioni coercitive avviate dall'FTC in materia di privacy e sicurezza figura è disponibile sul sito web dell'FTC all'indirizzo https://www.ftc.gov/reports/privacy-data-security-update-2015.

a una vasta gamma di leggi intese alla tutela della vita privata e alla sicurezza dei dati che riguardano i consumatori. Tra queste la principale è la legge sull'FTC stessa, che proibisce gli atti o pratiche sleali e ingannevoli nel commercio o inerenti al commercio ([1]). È ingannevole la rappresentazione, omissione o pratica quando è rilevante e rischia di fuorviare il consumatore che tiene un comportamento ragionevole in considerazione delle circostanze ([2]). È sleale l'atto o la pratica che causa o rischia di causare un danno rilevante che il consumatore non può ragionevolmente evitare o che non è compensato da un beneficio superiore per i consumatori o per la concorrenza ([3]). L'FTC ha inoltre la responsabilità di controllare il rispetto di leggi specifiche riguardo alla protezione delle informazioni sulla salute e sul credito e altre materie finanziarie e alla protezione delle informazioni *online* relative a minori. Per ciascuna di tali leggi ha emanato i regolamenti di esecuzione.

A norma della legge sull'FTC, questa è competente delle materie che rientrano nel commercio o che hanno ripercussioni sul commercio: non ha quindi competenza in tema di rispetto della normativa penale o di questioni di sicurezza nazionale e neppure riguardo alla maggior parte delle altre iniziative governative. Vigono inoltre eccezioni alla sua competenza in materia di attività commerciali, ad esempio nei confronti di banche, compagnie aeree, assicurazioni e prestatori di servizi di telecomunicazione nell'esercizio di attività di vettore pubblico. L'FTC non ha competenza neppure riguardo alla maggior parte delle organizzazioni non a scopo di lucro, tranne che per i soggetti che si presentano come associazioni di beneficenza o altrimenti senza scopo di lucro ma che in realtà esercitano un'attività lucrativa. Non ha competenza nemmeno sulle organizzazioni senza scopo di lucro che operano per dare profitto ai loro membri con scopo di lucro, anche sotto forma di rilevanti benefici economici ([4]). In alcuni casi l'FTC ha una competenza concorrente assieme ad altri enti di applicazione della legge.

L'FTC ha intessuto stretti rapporti di lavoro con le autorità federali e statali, con le quali collabora assiduamente per coordinare le indagini o rinviare loro le domande quando occorra.

Il controllo dell'applicazione è il perno dell'impostazione seguita dall'FTC in materia di tutela della vita privata: ad oggi l'FTC ha sostenuto oltre 500 casi di tutela della vita privata e della sicurezza delle informazioni riguardanti i consumatori, trattando di informazioni sia *offline* sia *online* e intervenendo con azioni coercitive presso imprese sia grandi sia piccole per presunti motivi che spaziavano dalla divulgazione irregolare di dati sensibili relativi ai consumatori alla protezione carente delle informazioni personali dei consumatori, dalla tracciatura ingannevole dei consumatori online allo spamming nei loro confronti, dall'installazione di software spia o altro malware sui computer dei consumatori alla violazione dell'opposizione alle telefonate commerciali e di altre regole sulla pubblicità telefonica, fino alla raccolta e alla condivisone irregolari di informazioni relative ai consumatori sui dispositivi mobili Le azioni coercitive dell'FTC, nel mondo tanto fisico quanto digitale, trasmettono alle imprese un messaggio importante sulla necessità di tutelare la vita privata dei consumatori.

L'FTC ha portato avanti numerose iniziative politiche volte a migliorare la tutela della vita privata dei consumatori, le quali vanno a informare la sua attività di controllo dell'applicazione. Ha ospitato seminari e pubblicato relazioni in cui ha raccomandato le migliori pratiche da adottare per perfezionare la privacy nell'ecosistema mobile, per aumentare la trasparenza nel settore dell'intermediazione nella trasmissione dati, per ottimizzare i vantaggi dei megadati attenuandone nel contempo i rischi, specie per i consumatori a basso reddito e non serviti a sufficienza, e per porre in evidenza le implicazioni che, tra gli altri aspetti, il riconoscimento facciale e l'Internet delle cose hanno in termini di privacy e sicurezza.

Per potenziare l'effetto delle sue iniziative di applicazione della legge e di evoluzione delle politiche, l'FTC è attiva nell'educazione dei consumatori e delle imprese, impiegando una varietà di mezzi (pubblicazioni, risorse online, seminari, *social media*) per mettere a disposizione materiale educativo su una vasta gamma di temi, ad esempio le applicazioni mobili, la privacy dei minori e la sicurezza dei dati. Da ultimo l'FTC ha avviato l'iniziativa *Start With Security* (la sicurezza innanzitutto), nella quale sono proposti alle imprese i nuovi orientamenti scaturiti dagli insegnamenti ricavati dai casi di sicurezza dei dati da essa trattati, e ha organizzato una serie di seminari in tutti gli USA. Da tempo l'FTC è inoltre leader nell'educazione dei consumatori alla sicurezza informatica di base: l'anno scorso le pagine del sito *OnGuard Online* e dell'equivalente in lingua spagnola *Alerta en Línea* hanno contato oltre 5 milioni di visitatori.

B. **Tutele giuridiche degli USA a beneficio dei consumatori dell'UE**

Il regime dello scudo s'innesterà sul più ampio panorama statunitense della privacy, che offre ai consumatori dell'UE vari tipi di tutele.

([1]) Codice degli Stati Uniti d'America, titolo 15, articolo 45(a).

([2]) Cfr. Dichiarazione dell'FTC sugli atti e pratiche ingannevoli, acclusa a Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), consultabile all'indirizzo https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

([3]) Codice degli Stati Uniti d'America, titolo 15, articolo 45(n). Cfr. Dichiarazione dell'FTC sugli atti e pratiche sleali, *acclusa a Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *consultazione all'indirizzo* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

([4]) Cfr. California Dental Ass'n cfr. FTC, 526 U.S. 756 (1999).

Il divieto di atti o pratiche sleali o ingannevoli imposto dalla legge sull'FTC non si limita a proteggere i consumatori statunitensi dalle imprese statunitensi; comprende infatti le pratiche 1) che causano o presentano probabilità di causare danni ragionevolmente prevedibili negli USA o 2) che implicano un comportamento rilevante tenuto negli Stati Uniti. Inoltre, l'FTC può attivare nei confronti dei consumatori stranieri tutte le misure correttive, restituzione compresa, di cui dispongono i consumatori statunitensi.

L'attività di controllo dell'applicazione svolta dall'FTC reca di fatto benefici rilevanti ai consumatori sia statunitensi sia stranieri. Ad esempio, i casi aperti in applicazione dell'articolo 5 della legge sull'FTC hanno tutelato la privacy di consumatori stranieri al pari di quella dei consumatori statunitensi. Nella causa avviata contro Accusearch, intermediario nel settore delle informazioni, l'FTC ha sostenuto che, cedendo a terzi dati telefonici riservati senza che il consumatore ne fosse al corrente o vi avesse acconsentito, la società aveva condotto una pratica sleale in violazione dell'articolo 5 della legge sull'FTC. Le informazioni cedute da Accusearch riguardavano consumatori sia statunitensi sia stranieri ([1]). Il giudice ha emanato un provvedimento inibitorio nei confronti di Accusearch proibendole, tra l'altro, di commercializzare o cedere le informazioni personali dei consumatori senza il loro consenso scritto, a meno che siano ricavate legittimamente da fonti di disponibilità pubblica, e ha disposto la restituzione di quasi 200 000 USD ([2]).

Un altro esempio è la transazione che l'FTC ha concluso con TRUSTe, grazie alla quale i consumatori, compresi quelli dell'Unione europea, possono fare affidamento sul modo in cui un'organizzazione di autoregolamentazione di dimensione mondiale rappresenta il proprio metodo di verifica e certificazione dei servizi online statunitensi e stranieri ([3]). Si rilevi che l'azione intentata dall'FTC contro TRUSTe ha avuto anche l'effetto di rafforzare più in generale il sistema di autoregolamentazione in materia di privacy, decretando la responsabilità giuridica dei soggetti investiti di un ruolo importante nei programmi di autoregolamentazione, compresi i regimi transnazionali sulla privacy.

L'FTC è parimenti responsabile del controllo dell'applicazione di altre leggi specifiche che prevedono tutele valide anche per i consumatori al di fuori degli Stati Uniti, come ad esempio la legge sulla tutela della vita privata dei minori online (COPPA). Fra le altre disposizioni la COPPA impone agli operatori che gestiscono siti web e servizi in rete rivolti ai minori, ovvero siti generici che rilevano scientemente informazioni personali di minori di età inferiore a 13 anni, di prevedere un'avvertenza rivolta ai genitori e di ottenere da questi un consenso verificabile. I siti web e i servizi in rete basati negli USA che sono soggetti alla COPPA e rilevano informazioni personali da minori stranieri sono tenuti a conformarsi a tale legge. Anche i siti web e i servizi in rete basati all'estero devono conformarsi alla COPPA se si rivolgono a minori che si trovano negli USA o se rilevano scientemente informazioni personali di minori che si trovano negli USA. Al di là delle leggi federali statunitensi di cui l'FTC controlla l'applicazione, ulteriori benefici possono derivare per i consumatori dell'UE da altre leggi federali e statali in materia di protezione dei consumatori e di tutela della vita privata.

C. **Applicazione dell'approdo sicuro**

Nell'ambito del programma di controllo dell'applicazione in materia di privacy e sicurezza l'FTC ha provveduto a tutelare i consumatori dell'UE anche tramite azioni coercitive per violazione dei principi dell'approdo sicuro. Le azioni coercitive avviate dall'FTC in tale ambito sono 39: 36 per millantata certificazione al regime e 3 (contro Google, Facebook e Myspace) per presunte violazioni dei principi dell'approdo sicuro in materia di riservatezza ([4]). Questi casi dimostrano l'azionabilità delle certificazioni e le ripercussioni dell'inosservanza. In ottemperanza alle ordinanze consensuali di durata ventennale adottate, Google, Facebook e Myspace sono tenute a attuare dei programmi di privacy completi, costruiti in modo da affrontare ragionevolmente i rischi per la tutela della vita privata che si pongono nello sviluppo e nella gestione dei prodotti e servizi esistenti e nuovi e da tutelare la vita privata e la riservatezza delle informazioni personali. I prescritti programmi di privacy completi devono individuare i rischi rilevanti prevedibili e controllarli. Le imprese sono tenute inoltre a sottoporre tali programmi alla valutazione continua e indipendente dell'FTC. Le ordinanze vietano alle imprese di dare una rappresentazione non veritiera delle pratiche seguite in materia di privacy e di millantare l'adesione a programmi di privacy o di sicurezza, divieto che si applica anche agli atti e pratiche delle imprese nell'ambito del

([1]) Cfr. Commissariato per la protezione della vita privata del Canada, Reclamo nell'ambito del PIPEDA nei confronti di Accusearch, Inc., attiva come Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Il Commissariato canadese ha presentato una nota in veste di *amicus curiae* nell'appello contro l'azione dell'FTC e ha condotto indagini autonome sul caso, giungendo alla conclusione che le pratiche di Accusearch violavano anche la legge canadese.

([2]) Cfr. *FTC/Accusearch, Inc.*, n. 06CV015D (D. Wyo. 20 dicembre 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Cfr. *In the Matter of True Ultimate Standards Everywhere, Inc.*, n. C-4512 (F.T.C. 12 marzo 2015) (decisione e ordinanza), consultabile all'indirizzo https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Cfr. *In the Matter of Google, Inc.*, n. C-4336 (F.T.C. 13 ottobre 2011) (decisione e ordinanza), *consultabile all'indirizzo* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matt*; *In the Matter of Facebook, Inc.*, n. C-4365 (F.T.C. 27 luglio 2012) (decisione e ordinanza), *consultabile all'indirizzo* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, n. C-4369 (F.T.C. 30 agosto 2012) (decisione e ordinanza), consultabile all'indirizzo https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

nuovo regime dello scudo. L'FTC può far rispettare le ordinanze chiedendo sanzioni civili e infatti nel 2012 Google ha pagato la cifra senza precedenti di 22,5 milioni di dollari per chiudere la questione della presunta violazione dell'ordinanza. Dette ordinanze dell'FTC contribuiscono quindi a tutelare oltre un miliardo di consumatori nel mondo, di cui centinaia di milioni residenti in Europa.

L'FTC ha aperto casi anche per millantata adesione al programma dell'approdo sicuro. L'FTC prende sul serio questo tipo di millanterie. Nel procedimento *FTC/Karnani* del 2011, ad esempio, l'FTC ha avviato un'azione contro un commerciante via Internet statunitense adducendo a motivo il fatto che il commerciante e la sua impresa lasciavano intendere ai consumatori del Regno Unito che l'impresa fosse basata in quel paese, fra l'altro usando le estensioni.uk e facendo riferimento alla valuta e al sistema postale del Regno Unito ([1]). Ricevuti i prodotti i consumatori scoprivano però che dovevano pagare dazi d'importazione non preventivati, che le garanzie non valevano nel Regno Unito e che il rimborso era subordinato a spese. L'FTC accusò i convenuti anche di aver ingannato i consumatori circa l'adesione al programma dell'approdo sicuro. I consumatori vittime di queste pratiche si trovavano tutti nel Regno Unito.

In molti casi le altre azioni coercitive nell'ambito dell'approdo sicuro hanno riguardato organizzazioni che, pur avendo aderito al programma, non avevano poi rinnovato annualmente la certificazione ma continuavano a presentarsi come aderenti. Come illustrato qui di seguito, l'FTC si impegna parimenti a affrontare i casi di millantata adesione allo scudo per la privacy. Quest'attività strategica di controllo dell'applicazione verrà a integrare l'impegno intensificato del Dipartimento del Commercio per verificare la conformità ai requisiti del programma in materia di certificazione e ricertificazione, il controllo che esercita sulla conformità effettiva, anche tramite i questionari inviati agli aderenti al regime, e il potenziato impegno per individuare i casi di millantata adesione allo scudo e di abuso del relativo marchio di certificazione ([2]).

II. ATTRIBUZIONE DI PRIORITÀ AI CASI E INDAGINI

Come per il programma dell'approdo sicuro, anche nell'ambito dello scudo l'FTC s'impegna a dare priorità ai casi sottoposti dagli Stati membri dell'UE. Priorità sarà attribuita anche ai casi sottoposti dagli organi di autoregolamentazione e dagli altri organi indipendenti di composizione delle controversie e vertenti sull'inosservanza delle direttive di autoregolamentazione inerenti al regime dello scudo.

L'FTC sta predisponendo una procedura standard per agevolare gli Stati membri dell'UE nella presentazione dei casi nell'ambito dello scudo e sta elaborando orientamenti che indichino il tipo di informazioni che le saranno più utili ai fini dell'esame del caso sottopostole. In questo contesto l'FTC nominerà un referente interno dedicato agli Stati membri dell'UE. È estremamente utile che l'autorità richiedente abbia già svolto un esame preliminare della presunta violazione e possa collaborare alle indagini dell'FTC.

Quando investita di un caso da uno Stato membro dell'UE o da un organo di autoregolamentazione l'FTC può affrontare le questioni sottopostele intervenendo su vari fronti, ad esempio verificando le politiche della privacy seguite dall'impresa, ottenendo ulteriori informazioni dall'impresa o da terzi, dando riscontri al soggetto richiedente, valutando se esista uno schema di violazione o se la violazione interessi un numero consistente di consumatori, stabilendo se il caso verte su materie rientranti nella sfera di competenza del Dipartimento del Commercio, valutando l'utilità di un'azione educativa sui consumatori e sulle imprese e, se del caso, avviando un procedimento coercitivo.

L'FTC s'impegna a condividere le informazioni sui casi sottopostile (anche riguardo all'evoluzione del caso) con le autorità di applicazione della legge richiedenti, ferme restando le leggi e le limitazioni in tema di riservatezza. Per quanto possibile in considerazione del numero e del tipo dei casi ricevuti, l'FTC comunica anche la sua valutazione del caso, comprensiva della descrizione delle questioni rilevanti sollevate e delle iniziative adottate per far fronte alle violazioni delle norme di sua competenza. Per conferire maggiore efficacia alle iniziative volte a contrastare le condotte illecite, l'FTC dà inoltre riscontro all'autorità richiedente circa il tipo di casi ricevuti. Se l'autorità richiedente chiede informazioni

([1]) Cfr. *FTC/Karnani*, n. 2:09-cv-05276 (C.D. Cal. 20 maggio 2011) (ordinanza definitiva pronunciata), consultabile all'indirizzo https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; cfr. *anche* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, http://www.ftc.gov/blog/2011/06/around-world-shady-ways (9 giugno 2011).

([2]) Lettera di Ken Hyatt, Sottosegretario al Commercio ad interim, incaricato del commercio internazionale, Amministrazione del commercio internazionale, a Věra Jourová, Commissaria per la Giustizia, i consumatori e la parità di genere.

sull'evoluzione del caso sottoposto per poter portare avanti il proprio procedimento coercitivo, l'FTC risponde, tenuto conto del numero di casi all'esame e fatti salvi gli obblighi giuridici di riservatezza e di altro tipo.

L'FTC collabora da vicino con le autorità di protezione dei dati dell'UE per assisterle nelle attività di applicazione della legge. Se del caso, la collaborazione si esplica in condivisione delle informazioni e assistenza alle indagini a norma della legge statunitense sull'Internet sicura (SAFE WEB), che autorizza l'FTC a collaborare con le omologhe straniere nei casi di applicazione di leggi estere che vietano pratiche sostanzialmente analoghe a quelle vietate dalle leggi che l'FTC è tenuta a far applicare ([1]). Nel quadro di quest'assistenza l'FTC può, fatti salvi gli obblighi imposti dalla legge sull'Internet sicura, comunicare informazioni ottenute nel corso della propria indagine, emettere provvedimenti cogenti a nome dell'autorità di protezione dei dati dell'UE che sta svolgendo la propria indagine e raccogliere la deposizione orale di testimoni o convenuti in relazione al procedimento coercitivo avviato da tale autorità. L'FTC esercita regolarmente questo potere per assistere le autorità di tutto il mondo nei casi inerenti alla tutela della vita privata e alla protezione dei consumatori ([2]).

Oltre a dare priorità ai casi sottopostile nell'ambito dello scudo dagli Stati membri dell'UE o da organi di autoregolamentazione nel settore della privacy ([3]), l'FTC s'impegna, se del caso, a indagare di propria iniziativa sulle possibili violazioni dello scudo, attivando una serie di strumenti.

Da oltre un decennio l'FTC attua un solido programma di indagini sulle questioni della privacy e della sicurezza che interessano soggetti commerciali. In tale ambito ha verificato sistematicamente se il soggetto si dichiarasse aderente all'approdo sicuro. In caso affermativo, se dall'indagine risultava una manifesta violazione dei relativi principi, l'FTC ha incluso accuse di violazioni dell'approdo sicuro nell'azione coercitiva avviata. Quest'impostazione proattiva sarà mantenuta anche per il nuovo regime. È importante sottolineare che l'FTC conduce molte più indagini di quante sfocino poi in azioni coercitive pubbliche: molte indagini sono infatti chiuse perché il personale dell'FTC non ravvisa una violazione manifesta della legge; trattandosi di indagini riservate e non pubbliche, spesso la notizia della chiusura del caso non è divulgata.

Le quasi 40 azioni coercitive avviate dall'FTC nell'ambito del programma dell'approdo sicuro sottolineano l'impegno a far rispettare in via proattiva i programmi transnazionali di tutela della privacy. L'FTC vaglierà le possibili violazioni del regime dello scudo nel quadro delle indagini in materia di privacy e di sicurezza che conduce regolarmente.

III. SOLUZIONE DEI CASI DI MILLANTATA APPARTENENZA ALLO SCUDO

Come accennato prima, l'FTC prevede di intervenire nei confronti dei soggetti che millantano l'adesione allo scudo, esaminando in via prioritaria i casi sottoposti dal Dipartimento del Commercio relativamente a organizzazioni che ha riscontrato millantare l'adesione al regime dello scudo o usare senza autorizzazione il relativo marchio di certificazione.

Si rileva altresì che, se la politica della privacy dell'organizzazione afferma la conformità ai principi dello scudo, il fatto che l'organizzazione non si registri o non rinnovi la registrazione presso il Dipartimento del Commercio non dovrebbe di per sé esimerla dall'essere vincolata al controllo dell'FTC quanto all'applicazione degli impegni assunti in tale ambito.

([1]) Per decidere se esercitare i poteri conferitile dalla legge sull'Internet sicura l'FTC valuta tra l'altro: a) se l'ente richiedente abbia accettato di fornirle o le fornirà assistenza su base di reciprocità; b) se il soddisfacimento della richiesta rechi pregiudizio all'interesse pubblico degli Stati Uniti d'America; c) se l'indagine o il procedimento coercitivo avviato dall'ente richiedente verta su atti o pratiche che causano o presentano probabilità di causare danni a un numero consistente di persone (Codice degli Stati Uniti d'America, titolo 15, articolo 46(j) (3)]. Questo potere non vale per l'applicazione della normativa sulla concorrenza.

([2]) Negli esercizi finanziari 2012-2015, ad esempio, l'FTC ha esercitato il potere conferitole dalla legge sull'Internet sicura per comunicare informazioni in risposta a quasi 60 richieste di enti stranieri e ha emanato quasi 60 domande d'indagine civile (equivalenti alle citazioni amministrative) nel quadro della prestazione di assistenza in 25 indagini straniere.

([3]) Sebbene non si occupi di risolvere i singoli casi di reclamo del singolo consumatore né svolga opera di mediazione al riguardo, l'FTC dichiara che darà priorità ai casi sottopostile dalle autorità di protezione dei dati dell'UE. L'FTC usa inoltre i reclami inseriti nella propria banca dati *Consumer Sentinel*, cui accedono molte altre autorità di applicazione della legge, per rilevare le tendenze, stabilire le priorità di applicazione e individuare i potenziali obiettivi da sottoporre a indagine. Per la presentazione di un reclamo all'FTC, le persone dell'UE dispongono dello stesso sistema di reclamo offerto ai cittadini statunitensi — cfr. www.ftc.gov/complaint. Per il singolo reclamo nell'ambito dello scudo, la persona dell'UE potrebbe tuttavia trovare più utile presentarlo all'autorità di protezione dei dati del proprio Stato membro o a un organo alternativo di composizione delle controversie.

IV. CONTROLLO SUI PROVVEDIMENTI COERCITIVI

L'FTC s'impegna a controllare l'attuazione dei provvedimenti coercitivi per assicurare la conformità allo scudo.

Questa conformità sarà garantita inserendo una gamma adeguata di ingiunzioni nei futuri provvedimenti dell'FTC adottati nell'ambito dello scudo, tra cui il divieto di millanterie riguardo allo scudo e a altro programma sulla privacy sul quale si fonda l'azione dell'FTC.

I casi in cui l'FTC ha dato applicazione al programma originario dell'approdo sicuro sono illuminanti. In ciascuno dei 36 casi di millantata certificazione, il provvedimento diffida il convenuto dal millantare l'adesione all'approdo sicuro o ad altro programma in materia di privacy o di sicurezza e gli impone di trasmettere all'FTC relazioni di conformità. Nei casi vertenti su violazioni dei principi dell'approdo sicuro l'impresa è stata obbligata a attuare un programma di privacy completo, da sottoporre ogni anno, per vent'anni, alla valutazione di un terzo indipendente, e a trasmetterla all'FTC.

Violare il provvedimento amministrativo disposto dall'FTC può comportare una sanzione civile fino a 16 000 USD per singola violazione oppure, in caso di violazione reiterata, di 16 000 USD al giorno ([1]): in caso di pratiche lesive di un numero consistente di consumatori, la sanzione può quindi essere dell'ordine di milioni di dollari. Anche l'ordinanza consensuale comporta obblighi di conformità e di presentazione di relazioni. Il destinatario dell'ordinanza deve conservare per un dato numero di anni la documentazione che ne dimostra la conformità. L'ordinanza deve essere divulgata anche al personale incaricato di assicurarne il rispetto.

Come per qualsiasi altro provvedimento, l'FTC controlla sistematicamente la conformità dei provvedimenti emanati nell'ambito dell'approdo sicuro. Per l'FTC l'effettiva applicazione dei provvedimenti emanati in materia di privacy e di sicurezza dei dati è molto importante e implica, se necessario, un suo intervento al riguardo. Si è già accennato, ad esempio, al fatto che Google ha pagato una sanzione civile di 22,5 milioni di dollari per chiudere la questione della presunta violazione dell'ordinanza emessa dall'FTC nei suoi confronti. Si rilevi che i provvedimenti dell'FTC continueranno a tutelare i consumatori che, in tutto il mondo, interagiscono con l'impresa e non soltanto quelli che hanno presentato il reclamo.

L'FTC mantiene in rete un elenco delle imprese colpite da un suo provvedimento in relazione all'applicazione sia del programma dell'approdo sicuro sia del nuovo regime dello scudo ([2]). I principi dello scudo richiedono ora all'impresa colpita da un provvedimento per inosservanza degli stessi emesso dall'FTC o da un giudice di rendere pubbliche le parti inerenti allo scudo delle relazioni di conformità o di valutazione presentate all'FTC, limitatamente a quanto compatibile con le leggi e i regolamenti sulla riservatezza.

V. RAPPORTI E COOPERAZIONE ESECUTIVA CON LE AUTORITÀ DI PROTEZIONE DEI DATI DELL'UE

Nel riconoscere il ruolo importante che le autorità di protezione dei dati dell'UE svolgono per la conformità allo scudo, l'FTC incoraggia a intensificare la consultazione e la cooperazione esecutiva con esse. Oltre a consultare l'autorità di protezione dei dati richiedente sulle questioni relative al singolo caso, l'FTC s'impegna a riunirsi periodicamente con i pertinenti rappresentanti del gruppo dell'articolo 29 per discutere in generale sul modo di migliorare la cooperazione esecutiva nell'ambito del regime. Parteciperà anche, assieme al Dipartimento del Commercio, alla Commissione europea e ai rappresentanti del gruppo dell'articolo 29, alla valutazione annuale del regime per discutere della relativa attuazione.

L'FTC incoraggia lo sviluppo di strumenti atti a potenziare la cooperazione esecutiva con le autorità di protezione dei dati dell'UE così come con altre omologhe nel mondo. In particolare, l'anno scorso l'FTC ha lanciato, assieme a autorità omologhe dell'Unione europea e del mondo, un sistema di avviso interno alla rete globale di applicazione della legge in materia di privacy (*Global Privacy Enforcement Network* — GPEN) per condividere informazioni sulle indagini e promuovere il coordinamento nell'esecuzione. Questo sistema di avviso della GPEN potrebbe dimostrarsi particolarmente utile nell'ambito dello scudo: l'FTC e le autorità di protezione dei dati dell'UE potrebbero usarlo per il coordinamento delle indagini avviate nel quadro del regime o in altri ambiti relativi alla privacy, anche come punto di partenza per lo scambio d'informazioni, al fine di offrire ai consumatori una tutela della privacy coordinata e più efficace. L'FTC attende

([1]) Codice degli Stati Uniti d'America, titolo 15, articolo 45(m). Codice dei regolamenti federali, titolo 16, articolo 1.98.
([2]) Cfr. FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&fieldconsumerprotectiontopicstid=251.

con interesse di proseguire con le autorità dell'UE partecipanti i lavori volti a diffondere maggiormente il sistema di avviso della GPEN e a sviluppare altri strumenti che permettano di migliorare la cooperazione esecutiva nei casi vertenti sulla privacy, compresi quelli inseriti nello scudo.

L'FTC si pregia di affermare il proprio impegno a dare esecuzione al regime dello scudo per la privacy e attende con interesse di continuare a lavorare assieme alle omologhe dell'UE per tutelare la vita privata dei consumatori su entrambe le sponde dell'Atlantico.

La prego di accogliere, signora Commissaria,
i sensi della mia più alta stima.

Edith Ramirez

Presidente

Allegato A

Contesto in cui s'innesta lo scudo UE-USA per la privacy: panorama della privacy e della sicurezza negli Stati Uniti d'America

Le tutele offerte dal regime dello scudo UE-USA per la privacy («scudo» o «regime») esistono nel contesto delle più ampie tutele del rispetto della vita privata garantite dal sistema giuridico statunitense nel suo complesso. In primo luogo, la Commissione federale del Commercio (FTC) prevede, per le pratiche commerciali statunitensi, un programma solido di tutela della vita privata e di sicurezza dei dati che protegge i consumatori di tutto il mondo In secondo luogo, da quando il programma originario UE-USA dell'approdo sicuro fu adottato nel 2000, il panorama statunitense della tutela della privacy e della sicurezza dei consumatori è mutato notevolmente: sono state emanate numerose leggi federali e dei singoli Stati sulla privacy e sulla sicurezza e sono aumentate considerevolmente le azioni proposte in giustizia, da soggetti pubblici e privati, riguardo al rispetto dei diritti alla privacy. L'ampia gamma di tutele giuridiche della privacy e della sicurezza dei consumatori applicabili alle pratiche commerciali di gestione dei dati che vigono negli Stati Uniti vengono a completare le tutele offerte alle persone dell'UE dal nuovo regime.

I. PROGRAMMA GENERALE DELL'FTC PER IL CONTROLLO DELL'APPLICAZIONE IN MATERIA DI PRIVACY E SICUREZZA

L'FTC è il principale ente di protezione dei consumatori negli USA per quanto riguarda la privacy nel settore commerciale. Ha il potere di perseguire gli atti o pratiche sleali o ingannevoli che violano la privacy del consumatore e di far rispettare alcune leggi maggiormente mirate alla tutela di determinate informazioni finanziarie e sanitarie, delle informazioni sui minori e di quelle usate per decidere dell'ammissibilità del consumatore a determinati benefici.

L'FTC vanta un'esperienza senza eguali nel rispetto della privacy dei consumatori. Le azioni coercitive da essa adottate hanno riguardato pratiche illecite condotte sia online sia offline. Ha, ad esempio, attaccato con azioni coercitive società molto note quali Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC e Snapchat, così come imprese meno conosciute. Ha avviato azioni giudiziarie contro imprese accusate di aver inondato di messaggi indesiderati i consumatori, di aver installato software spia sui loro computer, di non averne protetto le informazioni personali, di averne tracciato i percorsi online in modo ingannevole, di aver violato la privacy di minori, di aver raccolto illecitamente informazioni relative ai consumatori sui dispositivi mobili e di non aver protetto adeguatamente i disposizioni collegati a Internet usati per archiviare le informazioni personali. Solitamente i provvedimenti scaturiti da tali azioni hanno disposto un controllo continuato da parte dell'FTC per un periodo di vent'anni, hanno vietato ulteriori violazioni della legge e hanno comminato alle imprese una sanzione pecuniaria ingente in caso di violazione del provvedimento ([1]). Si rilevi che il provvedimento dell'FTC non tutela soltanto la persona che ha presentato reclamo, bensì tutti i consumatori che entreranno in relazione con l'impresa in futuro. In ambito transnazionale l'FTC è competente a tutelare i consumatori di tutto il mondo dalle pratiche condotte negli Stati Uniti ([2]).

Ad oggi l'FTC ha aperto oltre 130 casi di spamming e di software spia, oltre 120 casi di violazione dell'opposizione alle telefonate commerciali nella pubblicità telefonica, oltre 100 azioni nel quadro della legge sull'informativa corretta nel credito, quasi 60 casi vertenti sulla sicurezza dei dati, oltre 50 casi generici sulla tutela della vita privata, oltre 30 casi di violazione della legge Gramm-Leach-Bliley e oltre 20 azioni per il rispetto della legge sulla tutela della vita privata dei minori online (COPPA) ([3]). Ha inoltre emanato e pubblicato lettere di avvertimento ([4]).

([1]) Il soggetto che non si conforma a un provvedimento dell'FTC incorre in una sanzione civile fino a 16 000 USD per singola violazione oppure, in caso di violazione reiterata, di 16 000 USD al giorno. Cfr. Codice degli Stati Uniti d'America, titolo 15, articolo 45(1); Codice dei regolamenti federali, titolo 16, articolo 1.98(c).

([2]) Il Congresso ha confermato espressamente il potere dell'FTC di chiedere per via giudiziaria misure correttive, restituzione compresa, per gli atti o pratiche inerenti al commercio con l'estero 1) che causano o presentano probabilità di causare danni ragionevolmente prevedibili negli USA o 2) che implicano un comportamento rilevante tenuto negli Stati Uniti. Cfr. Codice degli Stati Uniti d'America, titolo 15, articolo 45(a)(4).

([3]) In alcuni casi sulla privacy e la sicurezza dei dati portati avanti dall'FTC l'impresa è accusata di aver condotto pratiche sia sleali sia ingannevoli; talvolta questi casi implicano la presunta violazione di varie leggi, quali la legge sull'informativa corretta nel credito, la legge Gramm-Leach-Bliley e la COPPA.

([4]) Cfr., *ad esempio*, Comunicato stampa della Commissione federale del Commercio, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (22 dicembre 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Comunicato stampa della Commissione federale del Commercio, FTC Warns Data Broker Operations of Possible Privacy Violations (7 maggio 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Comunicato stampa della Commissione federale del Commercio, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (3 aprile 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

In linea con questa tradizione di controllo rigoroso dell'applicazione della privacy, l'FTC ha anche vagliato le potenziali violazioni del programma dell'approdo sicuro. Da quando questo fu adottato, l'FTC ha aperto di propria iniziativa numerose indagini per verificare la conformità all'approdo sicuro e ha avviato 39 cause contro imprese statunitensi per violazione del programma. L'FTC manterrà quest'impostazione proattiva attribuendo priorità al controllo dell'applicazione del nuovo regime.

II. TUTELE DELLA PRIVACY DEL CONSUMATORE A LIVELLO FEDERALE E DI STATI FEDERATI

Il riepilogo delle modalità di esecuzione dei principi dell'approdo sicuro, allegato alla decisione della Commissione europea sull'adeguatezza di tale programma, sintetizza le numerose leggi federali e dei singoli Stati federati sulla privacy vigenti negli USA nel 2000, anno di adozione dell'approdo sicuro ([1]). La raccolta e l'uso di informazioni personali nel commercio erano all'epoca disciplinati, oltre che dall'articolo 5 della legge sull'FTC, da molte leggi federali: legge sulle comunicazioni via cavo, legge di tutela della privacy del conducente, legge sulla privacy nelle comunicazioni elettroniche, legge sul trasferimento elettronico di fondi, legge sull'informativa corretta nel credito, legge Gramm-Leach-Bliley, legge sul diritto alla privacy finanziaria, legge sulla tutela del consumatore telefonico e legge sulla tutela della privacy in video. Anche molti Stati federati avevano adottato analoghe disposizioni di legge in questi settori.

Dal 2000 numerosi sviluppi avvenuti a livello federale e federato hanno aumentato le tutele offerte alla privacy dei consumatori ([2]). A livello federale, ad esempio, nel 2013 l'FTC ha modificato la norma relativa alla COPPA, in modo da aggiungervi altre tutele delle informazioni personali che riguardano i minori. Ha altresì emanato due norme (sulla privacy e sulle garanzie) in applicazione della legge Gramm- Leach-Bliley, in base alle quali gli istituti finanziari ([3]) devono comunicare le pratiche seguite per la condivisione delle informazioni e attuare un programma generale di sicurezza delle informazioni volto a tutelare le informazioni che riguardano i consumatori ([4]). Analogamente, la legge sulle operazioni di credito corrette e accurate (FACTA), adottata nel 2003, integra le leggi sul credito vigenti da lunga data negli USA imponendo obblighi riguardo alla dissimulazione, condivisione e eliminazione di taluni dati finanziari sensibili. L'FTC ha emanato varie norme ai sensi della FACTA, tra l'altro in materia di diritto del consumatore di ricevere gratuitamente un rapporto di credito annuale, obblighi di eliminazione in condizioni sicure delle informazioni sul consumatore, diritto del consumatore di rifiutare di ricevere determinate offerte di credito o assicurazione, diritto del consumatore di rifiutare che l'impresa usi le informazioni fornite da una controllata per commercializzare prodotti e servizi e obblighi degli istituti finanziari e dei creditori di attuare programmi di rilevamento e prevenzione delle usurpazioni d'identità ([5]). Nel 2013 sono state inoltre rivedute le norme emanate ai sensi della legge sulla portabilità e responsabilità dell'assicurazione sanitaria, inserendovi ulteriori garanzie a tutela della privacy e della sicurezza delle informazioni personali sulla salute ([6]). Sono entrate in vigore anche norme che tutelano il consumatore dalle chiamate indesiderate di pubblicità telefonica, dalle chiamate automatizzate a fini pubblicitari e dai messaggi di posta elettronica indesiderati. Inoltre, il Congresso ha adottato leggi che obbligano determinate società che rilevano informazioni sulla salute di informare il consumatore in caso di violazione della sicurezza ([7]).

Anche gli Stati federati si sono dimostrati molto attivi nell'adozione di leggi sulla privacy e la sicurezza. Dal 2000, 47 Stati federati più il Distretto della Columbia, Guam, Portorico e le Isole Vergini hanno emanato leggi che impongono alle

([1]) Cfr. Dipartimento del Commercio dei USA, Riepilogo delle modalità di esecuzione dei principi di approdo sicuro, https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Per una sintesi più completa delle tutele giuridiche vigenti negli USA, cfr. Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

([3]) La legge Gramm-Leach-Bliley dà una definizione molto ampia di «istituto finanziario» includendovi tutte le imprese che svolgono un'«attività significativa» di fornitura di prodotti o servizi finanziari, ad esempio attività di: cambio di assegni, prestito in anticipo sul reddito, mediazione ipotecaria, prestito extrabancario, stima del patrimonio personale o immobiliare, compilazione professionale delle denunce dei redditi.

([4]) Ai sensi della legge sulla tutela finanziaria dei consumatori del 2010 (CFPA), titolo X di Pub. L. 111-203, 124 Stat. 1955 (21 luglio 2010) (detta anche «legge Dodd-Frank sulla riforma di Wall Street e la protezione dei consumatori»), il potere dell'FTC di emanare norme ai sensi della legge Gramm-Leach-Bliley è passato in gran parte all'Ufficio per la protezione finanziaria dei consumatori (CFPB). L'FTC mantiene il potere di coercizione ai sensi della legge Gramm-Leach- Bliley, il potere di emanare norme riguardo alle garanzie e un potere normativo limitato riguardo alla privacy relativamente ai concessionari di autoveicoli.

([5]) Ai sensi della CFPA, l'FTC condivide la funzione coercitiva con il CFPB, cui è invece trasferito gran parte del potere normativo (ad eccezione delle norme sui programmi relativi all'usurpazione di identità («*Red Flags*») e di quelle sull'eliminazione dei dati).

([6]) Cfr. Codice dei regolamenti federali, titolo 45, parti 160, 162, 164.

([7]) Cfr., *ad esempio*, legge sul rilancio degli investimenti e la ripresa in America del 2009, Pub. L. n. 111-5, 123 Stat. 115 (2009) e regolamenti associati, Codice dei regolamenti federali, titolo 45, articoli 164.404-164.414; Codice dei regolamenti federali, titolo 16, parte 318.

imprese d'informare l'interessato in caso di violazioni della sicurezza delle informazioni personali ([1]). In almeno 32 Stati più Portorico vigono leggi sull'eliminazione dei dati, che impongono obblighi relativamente alla distruzione o all'eliminazione delle informazioni personali ([2]). Vari Stati hanno adottato anche leggi sulla sicurezza dei dati in generale. Inoltre, la California ha adottato varie leggi in materia di privacy, fra cui una che obbliga le imprese a predisporre politiche della privacy e a divulgare le pratiche seguite riguardo alla non tracciabilità ([3]), una detta «*Shine the Light*» (fare luce) che impone maggiore trasparenza agli intermediari di dati ([4]) e una che obbliga a mettere a disposizione un tasto «cancella» che permette ai minori di chiedere la cancellazione di talune informazioni dai *social media* ([5]). Applicando dette leggi e esercitando altri poteri, il governo federale e singoli Stati federati hanno inflitto ammende ingenti alle imprese che non hanno protetto adeguatamente la privacy e la sicurezza delle informazioni personali relative ai consumatori ([6]).

Anche i contenziosi aperti da privati hanno determinato sentenze favorevoli e transazioni che hanno migliorato per i consumatori la tutela della privacy e la sicurezza dei dati. Ad esempio, nel 2015 Target ha accettato una transazione che ha comportato il pagamento di 10 milioni di dollari a clienti che sostenevano che le informazioni personali che li riguardavano fossero state compromesse a causa di una violazione diffusa della sicurezza dei dati. Nel 2013 AOL ha accettato di pagare 5 milioni di dollari nella transazione che ha chiuso una *class action* basata sulla presunta anonimizzazione inadeguata in un caso di divulgazione delle interrogazioni effettuate da centinaia di migliaia di suoi membri. Un giudice federale ha omologato un pagamento di 9 milioni di dollari da parte di Netflix per presunta conservazione dei dati storici relativi ai noleggi in violazione della legge sulla tutela della privacy in video del 1988. In California i giudici federali hanno omologato due transazioni distinte concluse da Facebook, una per 20 milioni di dollari e l'altra per 9,5 milioni di dollari, vertenti sulle pratiche seguite dalla società per la raccolta, l'uso e la condivisione delle informazioni personali dei suoi utenti. Nel 2008, sempre in California, un giudice dello Stato ha omologato una transazione di 20 milioni di dollari con LensCrafters per divulgazione illecita delle informazioni mediche dei consumatori.

Dalla presente sintesi emerge in sostanza che gli Stati Uniti d'America offrono una tutela giuridica considerevole della privacy e sicurezza dei consumatori. Il nuovo regime dello scudo, che offre garanzie sostanziali alle persone dell'UE, s'innesterà su questo più ampio substrato, in cui la tutela della privacy dei consumatori e della sicurezza dei dati resta una priorità importante.

([1]) Cfr., *ad esempio*, Conferenza nazionale degli organi legislativi degli Stati federati (NCSL), *State Security Breach Notification Laws* (4 gennaio 2016), consultabile all'indirizzo http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12 gennaio 2016), *consultabile all'indirizzo* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Codice delle imprese e professioni della California, articoli 22575-22579.

([4]) Codice civile della California, articoli 1798.80-1798.84.

([5]) Codice delle imprese e professioni della California, articoli 22580-22582.

([6]) Cfr. Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 febbraio 2014), *consultabile all'indirizzo* http://www.computerworld.com/s/article/9246393/Jay ClineU.S.takesthegoldindolingoutprivacyfines?taxonomyId=17&pageNumber=1.

ALLEGATO V

Lettera del segretario ai Trasporti degli Stati Uniti Anthony Foxx

19 febbraio 2016

Commissaria Vera Jourová
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Oggetto: Regime dello scudo UE-USA per la privacy

Gentile Commissaria Jourová,

il Dipartimento dei Trasporti degli Stati Uniti d'America («Dipartimento» o «DOT») si pregia di illustrare il proprio ruolo nell'applicazione del regime dello scudo UE-USA per la privacy («scudo» o «regime»). In un mondo sempre più interconnesso il regime ha un'importanza fondamentale ai fini della tutela dei dati personali comunicati nelle operazioni commerciali. Permette alle imprese di effettuare operazioni importanti nell'economia globale, consentendo nel contempo ai consumatori dell'UE di salvaguardare tutele rilevanti in materia di privacy.

In origine il Dipartimento si era impegnato a dare esecuzione al regime dell'approdo sicuro con una lettera inviata alla Commissione europea oltre 15 anni fa. In essa il Dipartimento s'impegnava a far rispettare attivamente e rigorosamente i principi del programma, impegno che continua a rispettare e che è sancito dalla presente lettera.

In particolare il DOT rinnova l'impegno assunto sui seguenti aspetti fondamentali: 1) attribuzione di priorità all'esame delle presunte violazioni dello scudo; 2) adeguato intervento coercitivo nei confronti del soggetto che millanta la certificazione allo scudo; 3) controllo dell'esecuzione e pubblicazione dei provvedimenti coercitivi inerenti a violazioni dello scudo. Seguono informazioni particolareggiate su ciascuno di detti impegni, cui si aggiunge, per il necessario inquadramento della questione, una descrizione del contesto in cui s'iscrive il ruolo svolto dal Dipartimento nella tutela della vita privata dei consumatori e nell'applicazione del regime dello scudo.

I. CONTESTO GENERALE

A. **Poteri del DOT in materia di privacy**

Il Dipartimento è fortemente impegnato a tutelare la riservatezza dei dati che i consumatori comunicano alle compagnie aeree e ai rivenditori che fanno servizio di biglietteria. Il potere del DOT d'intervenire in questa materia trova la base giuridica nel Codice degli Stati Uniti d'America, titolo 49, articolo 41712, che vieta al vettore o al rivenditore che fa servizio di biglietteria, nell'attività di vendita di trasporto aereo, qualsiasi pratica sleale o ingannevole ovvero qualsiasi metodo sleale di concorrenza che causi o possa causare un danno al consumatore. L'articolo 41712 è modellato sull'articolo 5 della legge sulla Commissione federale del Commercio (FTC) (Codice degli Stati Uniti d'America, titolo 49, articolo 45). Nella nostra interpretazione la disposizione sulle pratiche sleali o ingannevoli vieta alla compagnia aerea o al rivenditore che fa servizio di biglietteria 1) di violare i termini della propria politica della privacy; o 2) di rilevare o divulgare informazioni con modalità contrarie all'ordine pubblico, immorali o atte a causare al consumatore un danno rilevante non compensato da un beneficio superiore. Nella nostra interpretazione l'articolo 41712 vieta inoltre alla compagnia aerea o al rivenditore che fa servizio di biglietteria 1) di violare le norme emanate dal Dipartimento in cui determinate pratiche in materia di privacy sono indicate come sleali o ingannevoli o 2) di violare la legge sulla tutela della vita privata dei minori online (COPPA) o le norme dell'FTC che la attuano. A norma della legge federale, il DOT ha competenza esclusiva sulla disciplina delle pratiche in materia di privacy seguite dalle compagnie aeree e competenza concorrente con l'FTC per le stesse pratiche seguite dal rivenditore che fa servizio di biglietteria nell'attività di vendita di trasporto aereo.

Una volta che il vettore o il rivenditore di trasporto aereo ha assunto pubblicamente l'impegno di rispettare i principi dello scudo, il Dipartimento può quindi esercitare i poteri conferitigli dal paragrafo 41712 per farglieli rispettare. Pertanto, se la compagnia aerea o il rivenditore cui il passeggero comunica informazioni si è impegnato a rispettare i principi dello scudo, il venire meno a quest'impegno costituisce una violazione dell'articolo 41712.

B. **Pratiche di applicazione**

L'Ufficio per l'applicazione della legge e i procedimenti nel trasposto aereo del DOT («Ufficio») indaga sui casi e avvia azioni al riguardo a norma del Codice degli Stati Uniti d'America, titolo 49, articolo 41712. Nell'applicazione del divieto delle pratiche sleali e ingannevoli, disposto per legge dall'articolo 41712, opera principalmente tramite il negoziato, la stesura di provvedimenti inibitori e la redazione di provvedimenti di valutazione delle sanzioni civili. Nella maggior parte dei casi l'Ufficio viene a conoscenza delle potenziali violazioni tramite i reclami che riceve da persone, agenzie di viaggio e enti pubblici statunitensi e stranieri. I consumatori possono usare il sito web del DOT per sporgere reclamo nei confronti delle compagnie aeree e dei rivenditori che fanno servizio di biglietteria ([1]).

Se non è conclusa una transazione adeguata e ragionevole, l'Ufficio ha il potere di avviare un procedimento coercitivo che comporta un incidente probatorio dinanzi a un giudice amministrativo del Dipartimento, che è abilitato a emanare provvedimenti inibitori e infliggere sanzioni civili. La violazione dell'articolo 41712 può determinare l'emanazione di un provvedimento inibitorio e l'imposizione di una sanzione civile fino a 27 500 USD per ciascuna violazione.

Il Dipartimento non ha il potere di accordare un risarcimento o una riparazione pecuniaria al singolo reclamante, ma ha quello di approvare la transazione derivante da un'indagine dell'Ufficio che offre un beneficio (denaro contante, buoni ecc.) direttamente al consumatore in vece del pagamento della sanzione pecuniaria altrimenti dovuta al governo degli Stati Uniti. Il caso si è verificato in passato e, in presenza delle necessarie circostanze, potrà verificarsi anche nel contesto dei principi dello scudo. Se la compagnia aerea si rendesse responsabile di violazioni reiterate dell'articolo 41712, si porrebbe anche la questione della sua attitudine alla conformità; in situazioni estreme, questo potrebbe indurre a stabilire che la compagnia non è più idonea a esercitare l'attività e a privarla quindi della facoltà di esercitare l'attività economica.

Finora il DOT ha ricevuto un numero relativamente basso di reclami per presunta violazione della privacy da parte di compagnie aeree o di rivenditori che fanno servizio di biglietteria. Quando il caso si verifica, il reclamo è esaminato secondo i principi illustrati sopra.

C. **Tutele giuridiche del DOT a beneficio dei consumatori dell'UE**

A norma dell'articolo 41712, il divieto di pratiche sleali o ingannevoli nel trasporto aereo o nella vendita di trasporto aereo si applica a tutti i vettori aerei e rivenditori che fanno servizio di biglietteria, siano essi statunitensi o stranieri. Il Dipartimento interviene spesso nei confronti di compagnie aeree statunitensi e straniere per pratiche che interessano consumatori sia statunitensi sia stranieri in quanto applicate nel corso di una prestazione di trasporto verso gli USA o in partenza dagli USA. Il Dipartimento usa, e continuerà a usare, tutti i mezzi di cui dispone per tutelare i consumatori sia statunitensi sia stranieri dalle pratiche sleali o ingannevoli attuate nel trasporto aereo da soggetti regolamentati.

Nei confronti delle compagnie aeree il DOT è parimenti responsabile del controllo dell'applicazione di altre leggi specifiche che prevedono tutele valide anche per i consumatori al di fuori degli Stati Uniti, come ad esempio la COPPA. Fra le altre disposizioni la COPPA impone agli operatori che gestiscono siti web e servizi in rete rivolti ai minori, ovvero siti generici che rilevano scientemente informazioni personali di minori di età inferiore a 13 anni, di prevedere un'avvertenza rivolta ai genitori e di ottenere da questi un consenso verificabile. I siti web e i servizi in rete basati negli USA che sono soggetti alla COPPA e rilevano informazioni personali da minori stranieri sono tenuti a conformarsi a tale legge. Anche i siti web e i servizi in rete basati all'estero devono conformarsi alla COPPA se si rivolgono a minori che si trovano negli USA o se rilevano scientemente informazioni personali di minori che si trovano negli USA. In tutti i casi in cui la compagnia aerea che opera negli USA, sia essa statunitense o straniera, viola la COPPA, il Dipartimento è competente di avviare un'azione coercitiva.

II. APPLICAZIONE DELLO SCUDO

Se riceve, contro una compagnia aerea o un rivenditore che fa servizio di biglietteria che ha scelto di aderire allo scudo, un reclamo per presunta violazione dei principi del regime, il Dipartimento lo fa rispettare attivamente e rigorosamente nel modo illustrato qui di seguito.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Priorità all'esame della presunta violazione**

L'Ufficio esamina ciascun reclamo presentato per presunta violazione dello scudo (compresi quelli ricevuti dalle autorità di protezione dei dati dell'UE) e, se la violazione è confermata da prove, avvia un'azione coercitiva. L'Ufficio collabora con l'FTC e il Dipartimento del Commercio e esamina in via prioritaria i casi in cui un soggetto regolamentato è accusato di non rispettare gli impegni assunti nell'ambito dello scudo.

Ricevuta la segnalazione di una presunta violazione del regime, l'Ufficio può muoversi su vari fronti nel quadro dell'indagine, ad esempio verificando le politiche della privacy seguite dalla compagnia aerea o dal rivenditore che fa servizio di biglietteria, ottenendo ulteriori informazioni dalla compagnia o dal rivenditore o da terzi, dando riscontri al soggetto richiedente e valutando se esista uno schema di violazione o se la violazione interessi un numero consistente di consumatori. Stabilisce inoltre se il caso verte su materie rientranti nella sfera di competenza del Dipartimento del Commercio o dell'FTC, valuta l'utilità di un'azione educativa sui consumatori e sulle imprese e, se del caso, avvia un procedimento coercitivo.

Se viene a conoscenza di una possibile violazione dello scudo da parte di un rivenditore che fa servizio di biglietteria, il Dipartimento coordina le iniziative con l'FTC. Provvede altresì a informare l'FTC e il Dipartimento del Commercio dell'esito delle azioni coercitive avviate nell'ambito dello scudo.

B. **Soluzione dei casi di millantata appartenenza allo scudo**

Il Dipartimento resta impegnato a indagare sulle violazioni dello scudo, compreso sotto forma di millantata adesione al regime, esaminando in via prioritaria i casi sottoposti dal Dipartimento del Commercio relativamente a organizzazioni che ha riscontrato millantare l'adesione al regime dello scudo o usare senza autorizzazione il relativo marchio di certificazione.

Si rileva altresì che, se la politica della privacy dell'organizzazione afferma la conformità ai principi sostanziali dello scudo, il fatto che l'organizzazione non si registri o non rinnovi la registrazione presso il Dipartimento del Commercio non dovrebbe di per sé esimerla dall'essere vincolata al controllo del DOT quanto all'applicazione degli impegni assunti in tale ambito.

C. **Controllo dell'esecuzione e pubblicazione dei provvedimenti coercitivi inerenti a violazioni dello scudo**

L'Ufficio resta parimenti impegnato a controllare l'esecuzione dei provvedimenti coercitivi per quanto necessario ad assicurare il rispetto del programma dello scudo. Nello specifico, se emana un provvedimento che diffida la compagnia aerea o il rivenditore che fa servizio di biglietteria dal violare in futuro lo scudo e l'articolo 41712, l'Ufficio controlla che questa disposizione inibitoria sia effettivamente rispettata. Provvede inoltre a mettere i provvedimenti emanati nei casi rientranti nello scudo a disposizione sul proprio sito web.

Il Dipartimento attende con interesse di continuare a lavorare sulle questioni inerenti allo scudo assieme ai partner federali e ai portatori d'interesse dell'UE.

Nell'auspicare che queste informazioni risultino utili, resto a disposizione per qualsiasi domanda o ulteriore chiarimento.

La prego di accogliere, signora Commissaria,
i sensi della mia più alta stima.

Anthony R. Foxx

Segretario ai Trasporti

ALLEGATO VI

Lettera del Giureconsulto Robert Litt
Ufficio del direttore dell'intelligence nazionale (ODNI)

22 febbraio 2016

Justin S. Antonipillai
Consigliere
Dipartimento del Commercio degli USA
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Vicesegretario aggiunto
Amministrazione del commercio internazionale
1401 Constitution Ave., NW
Washington, DC 20230

Egr. sig. Antonipillai, Egr. sig. Dean,

nell'ambito dei negoziati sul regime dello scudo UE-USA per la privacy («scudo» o «regime»), gli Stati Uniti d'America hanno fornito negli ultimi due anni e mezzo una mole consistente d'informazioni sul funzionamento dell'attività di raccolta dati tramite l'intelligence dei segnali svolta dalla comunità dell'intelligence statunitense. Con tali informazioni, concernenti la disciplina giuridica dell'attività, i vari livelli di vigilanza su di essa, la trasparenza diffusa che la contraddistingue e, in generale, le tutele previste in fatto di privacy e libertà civili, s'intendeva aiutare la Commissione europea a stabilire se dette tutele fossero adeguate, in considerazione del fatto che attengono all'eccezione allo scudo per motivi di sicurezza nazionale. Il presente documento riporta una sintesi delle informazioni fornite.

I. DIRETTIVA PRESIDENZIALE 28 E ATTIVITÀ DI INTELLIGENCE DEI SEGNALI NEGLI USA

La comunità dell'intelligence statunitense raccoglie, con modalità soggette a un rigoroso controllo, nel totale rispetto delle leggi statunitensi e subordinatamente a una vigilanza a più livelli, intelligence esterna concentrandosi sugli aspetti importanti e sulle priorità della sicurezza nazionale. Negli USA la raccolta dati tramite l'intelligence dei segnali è disciplinata da un mosaico di leggi e politiche, tra cui la Costituzione degli Stati Uniti, la legge relativa alla vigilanza sull'intelligence esterna (FISA) (Codice degli Stati Uniti d'America, titolo 50, articolo 1801e ss.), il decreto presidenziale 12333 e relative procedure attuative, gli orientamenti presidenziali, e le numerose procedure e linee guida approvate dalla Corte FISA e dal Procuratore generale, che stabiliscono regole supplementari a limitazione della raccolta, conservazione, uso e divulgazione delle informazioni di intelligence esterna ([1]).

a. **Breve presentazione della direttiva presidenziale 28**

A gennaio 2014 il presidente Obama ha annunciato in un discorso una serie di riforme delle attività di intelligence dei segnali svolte dagli Stati Uniti e ha emanato al riguardo la direttiva presidenziale 28 (PPD-28) ([2]). Il presidente ha sottolineato che tali attività contribuiscono a proteggere non solo gli Stati Uniti e le libertà degli americani, ma anche la sicurezza e le libertà degli altri paesi, compresi gli Stati membri dell'UE, che fanno affidamento sulle informazioni raccolte dai servizi di intelligence statunitensi per proteggere i propri cittadini.

La PPD-28 stabilisce una serie di principi e obblighi che si applicano a tutte le attività di intelligence dei segnali svolte dagli Stati Uniti e nei confronti di tutti, indipendentemente dalla cittadinanza o dal luogo in cui si trova la persona. In particolare, fissa determinate condizioni procedurali riguardo alla raccolta, conservazione e divulgazione delle informazioni personali riguardanti cittadini stranieri ottenute dagli USA nell'ambito delle attività di intelligence dei segnali. Tali condizioni sono esposte in maggior dettaglio, ma comunque in forma sintetica, qui di seguito.

— La PPD ribadisce che gli Stati Uniti raccolgono dati di intelligence dei segnali solo nei modi e limiti autorizzati dalle leggi, dai decreti presidenziali o da altra direttiva presidenziale.

([1]) Ulteriori informazioni sulle attività di intelligence esterna svolte dagli USA sono disponibili pubblicamente in rete tramite *IC on the Record* (www.icontherecord.tumblr.com), il sito web pubblico dell'ODNI dedicato a innalzare la visibilità pubblica delle attività d'intelligence del governo.

([2]) *Consultabile all'indirizzo* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— La PPD stabilisce procedure atte a garantire che l'attività di intelligence dei segnali sia svolta solo per finalità legittime e autorizzate di sicurezza nazionale.

— La PPD prescrive che la tutela della vita privata e le libertà civili siano aspetti di cui tenere obbligatoriamente conto nella pianificazione delle attività di raccolta dati nell'ambito dell'intelligence dei segnali. In particolare, gli Stati Uniti non raccolgono dati di intelligence al fine di soffocare o reprimere la critica o il dissenso, di sfavorire persone per motivi di origine etnica, razza, genere, orientamento sessuale o religione o di conferire un vantaggio commerciale concorrenziale alle imprese statunitensi o a comparti dell'imprenditoria statunitense.

— La PPD impone di effettuare una raccolta dati quanto più possibile mirata nell'ambito dell'intelligence dei segnali e dispone che, se raccolti in blocco, tali dati possano essere usati solo per determinati scopi stabiliti espressamente.

— La PPD impone alla comunità dell'intelligence di adottare procedure ragionevolmente intese a ridurre al minimo la divulgazione e la conservazione delle informazioni personali raccolte tramite attività di intelligence dei segnali, in particolare allargando alle informazioni personali che riguardano gli stranieri alcune tutele previste per i cittadini statunitensi o residenti negli USA.

— Le procedure adottate dagli enti in attuazione della PPD-28 sono state rese pubbliche.

È pacifico che le procedure e le tutele previste dalla norme vigenti si applicano allo scudo: quando i dati sono trasferiti all'impresa presente negli Stati Uniti nell'ambito dello scudo — o di fatto con qualsiasi mezzo — i servizi di intelligence statunitensi possono chiederli all'impresa solo se la richiesta è conforme alla FISA o se è avanzata in base alle disposizioni di legge che regolano le *National Security Letter*, di cui segue descrizione ([1]). Inoltre, senza voler confermare né negare le notizie apparse sui media secondo cui la comunità dell'intelligence statunitense raccoglierebbe dati dai cavi transatlantici durante la trasmissione verso gli USA, si sottolinea che, se li raccogliesse, varrebbero comunque le limitazioni e le tutele previste dalle norme applicabili, comprese le condizioni imposte dalla PPD-28.

b. **Limitazioni applicabili alla raccolta**

La PPD-28 stabilisce una serie di principi generali importanti che disciplinano la raccolta dati nell'ambito dell'intelligence dei segnali.

— La raccolta dati nell'ambito dell'intelligence dei segnali dev'essere autorizzata per legge o per disposizione presidenziale e deve avvenire nel rispetto della Costituzione e della legge.

— La tutela della vita privata e le libertà civili sono aspetti di cui tenere obbligatoriamente conto nella pianificazione delle attività di intelligence dei segnali

— I dati dell'intelligence dei segnali sono rilevati solo per finalità valide di intelligence esterna o di controspionaggio.

— Gli Stati Uniti non raccolgono dati di intelligence dei segnali al fine di soffocare o reprimere la critica o il dissenso.

— Gli Stati Uniti non raccolgono dati di intelligence dei segnali per sfavorire persone per motivi di origine etnica, razza, genere, orientamento sessuale o religione.

— Gli Stati Uniti non raccolgono dati di intelligence dei segnali per conferire un vantaggio commerciale concorrenziale alle imprese statunitensi o a comparti dell'imprenditoria statunitense.

— L'attività di intelligence dei segnali svolta dagli Stati Uniti dev'essere *sempre* mirata il più precisamente possibile, tenuto conto della disponibilità di altre fonti di informazione. Questo significa, tra l'altro, che, ogniqualvolta possibile, le attività di raccolta dati nell'ambito dell'intelligence dei segnali sono condotte in modo mirato e non in blocco.

L'obbligo di svolgere un'attività di intelligence dei segnali quanto più possibile mirata vale sia per le modalità di raccolta dati in tale ambito sia per le informazioni effettivamente raccolte. Per stabilire se debbano essere raccolti dati nell'ambito

([1]) Gli organi di applicazione della legge o di regolamentazione possono chiedere alle imprese di trasmettere loro informazioni per indagini condotte negli Stati Uniti in base a altri poteri penali, civili e di regolamentazione che esulano dal presente documento, limitato ai poteri in materia di sicurezza nazionale.

dell'intelligence dei segnali, ad esempio, la comunità dell'intelligence deve vagliare la disponibilità di altre informazioni, anche di fonte diplomatica o pubblica, e, se opportuno e fattibile, privilegiare questo secondo mezzo. Ciascun servizio della comunità dell'intelligence dovrebbe inoltre prevedere nella propria politica di usare, ogniqualvolta possibile, discriminanti (dispositivi specifici, selettori, identificatori ecc.) per poter concentrare la rilevazione dei dati su obiettivi o temi specifici dell'intelligence esterna.

È importante considerare le informazioni comunicate alla Commissione nel loro insieme. La decisione sulla «fattibilità» o «praticabilità» non è lasciata alla discrezionalità del singolo, ma è presa in base alla politica stabilita da ciascun ente in applicazione della PPD-28 (resa pubblica) e alle altre procedure ivi stabilite ([1]). La PPD-28 definisce la raccolta dati in blocco nell'ambito dell'intelligence dei segnali come la raccolta che, in base a considerazioni tecniche o operative, è effettuata senza il filtro delle discriminanti (dispositivi specifici, selettori ecc.). In questo la PPD-28 riconosce che, nell'ambito dell'intelligence dei segnali, talune circostanze obbligano i servizi della comunità dell'intelligence a raccogliere dati in blocco per poter individuare una minaccia nuova o emergente o ricavare altre informazioni di rilevanza fondamentale per la sicurezza nazionale, che spesso si nascondono nelle dimensioni e nella complessità del sistema moderno di comunicazione globale. Riconosce anche che le preoccupazioni circa la tutela della vita privata e le libertà civili si acuiscono quando, nell'ambito dell'intelligence dei segnali, i dati sono rilevati in blocco. Chiede pertanto alla comunità dell'intelligence di privilegiare le alternative che permettono di effettuare una raccolta mirata dei dati in tale ambito rispetto alla raccolta in blocco. Di conseguenza, i servizi della comunità dell'intelligence dovrebbero muoversi in tal senso ogniqualvolta possibile ([2]). Grazie a questi principi, l'eccezione della raccolta in blocco non fagociterà la regola generale.

La «ragionevolezza» è uno dei capisaldi del diritto statunitense, in base al quale non si chiede ai servizi della comunità dell'intelligence di adottare qualsiasi misura possibile in linea teorica, ma piuttosto di trovare nelle loro attività un punto di equilibrio fra i legittimi interessi di tutela della vita privata e delle libertà civili e le esigenze concrete delle attività di intelligence dei segnali. Anche per quanto riguarda quest'aspetto le politiche seguite dagli enti, che sono state rese pubbliche, sono in grado di garantire che la regola generale non sia intaccata dalla nozione di «ragionevolmente intese a ridurre al minimo la divulgazione e la conservazione delle informazioni personali».

A norma della PPD-28 i dati raccolti in blocco nell'ambito dell'intelligence dei segnali possono essere usati solo per sei finalità specifiche: rilevazione e contrasto di determinate attività condotte da potenze straniere; antiterrorismo; antiproliferazione; cibersicurezza; rilevazione e contrasto di minacce alle forze armate degli Stati Uniti o dei loro alleati; contrasto delle minacce criminali transnazionali, compresa l'elusione delle sanzioni. Il Consigliere presidenziale per la sicurezza nazionale valuta ogni anno, in consultazione con il Direttore dell'intelligence nazionale, l'opportunità di modificare detti usi ammissibili dei dati raccolti in blocco nell'ambito dell'intelligence dei segnali. Il Direttore dell'intelligence nazionale darà al risultante elenco la massima pubblicità possibile compatibilmente con le esigenze di sicurezza nazionale: il sistema assicura quindi una limitazione importante e trasparente dell'uso dei dati raccolti in blocco nell'ambito dell'intelligence dei segnali.

I servizi della comunità dell'intelligence che attuano la PPD-28 hanno potenziato le pratiche e i criteri analitici per le interrogazioni sui dati non scremati ottenuti tramite l'intelligence dei segnali ([3]). L'analista è tenuto a strutturare l'interrogazione o altro termine o tecnica di ricerca, in modo che sia adeguato a reperire le informazioni di intelligence d'interesse ai fini di un compito valido di intelligence esterna o di applicazione della legge. A tal fine i servizi della comunità dell'intelligence sono tenuti a incentrare le interrogazioni relative alle persone sulle categorie di dati dell'intelligence dei segnali che rispondono a un requisito di intelligence esterna o di applicazione della legge, in modo da impedire l'uso di informazioni personali non pertinenti a tali fini.

Si rilevi che qualsiasi attività di raccolta in blocco condotta sulle comunicazioni via Internet dalla comunità dell'intelligence statunitense nell'ambito dell'intelligence dei segnali interessa una bassa percentuale dell'intera reta. A questo si aggiunge il fatto che, come illustrato *supra*, le interrogazioni mirate permettono di sottoporre all'analista soltanto i dati considerati in potenza possedere un valore a fini di intelligence. Queste limitazioni intendono tutelare la vita privata e le libertà civili di chiunque, a prescindere dalla cittadinanza e dal luogo in cui vive.

([1]) *Consultabile all'indirizzo* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Le procedure danno attuazione ai concetti di obiettivo e di attività mirata esposti nella presente lettera secondo modalità proprie a ciascun servizio della comunità dell'intelligence.

([2]) Per citare un solo esempio, le procedure stabilite dall'Agenzia per la sicurezza nazionale (NSA) in attuazione della PPD-28 prevedono che, ogniqualvolta praticabile, siano usati per la raccolta dei dati uno o più selettori per concentrarla su obiettivi specifici dell'intelligence esterna (ad esempio, un determinato e noto terrorista o gruppo terroristico internazionale) o su temi specifici dell'intelligence esterna (ad es, proliferazione delle armi di distruzione di massa da parte di una potenza straniera o di suoi agenti).

([3]) *Consultabile all'indirizzo* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Gli Stati Uniti hanno predisposto procedure per assicurare che le attività di intelligence dei segnali siano condotte soltanto per scopi appropriati di sicurezza nazionale. Ogni anno il presidente stabilisce le massime priorità della raccolti di dati nell'ambito dell'intelligence esterna a conclusione di un'articolata procedura interservizi. Al Direttore dell'intelligence nazionale spetta il compito di trasporre le priorità indicate dal presidente nel quadro delle priorità dell'intelligence nazionale (NIPF). La PPD-28 ha potenziato e migliorato la procedura interservizi, in modo che tutte le priorità di intelligence della relativa comunità possano essere valutate e approvate ad alto livello politico. La direttiva per la comunità dell'intelligence (ICD) 204, che riporta ulteriori orientamenti sul NIPF, è stata aggiornata a gennaio 2015 per incorporarvi le prescrizioni della PPD-28 ([1]). Il NIPF è classificato, ma ogni anno il documento non classificato sulla valutazione della minaccia a livello mondiale (*Worldwide Threat Assessment*), anch'esso agevolmente accessibile sul sito web dell'ODNI, riporta informazioni su specifiche priorità degli USA in materia di intelligence esterna.

Il NIPF indica le priorità in termini assai generici: condotta di programmi sulle capacità nucleari e di missili balistici da parte di determinati avversari stranieri, effetti della corruzione nei cartelli della droga, abusi dei diritti umani in determinati paesi ecc. Le priorità valgono non soltanto per l'intelligence dei segnali, bensì per tutte le attività di intelligence. La competenza di concretare nella raccolta dati nell'ambito dell'intelligence dei segnali le priorità indicate nel NIPF spetta al Comitato nazionale sull'intelligence dei segnali (SIGCOM), il quale opera sotto l'egida del Direttore dell'Agenzia per la sicurezza nazionale (NSA); questi è indicato dal decreto presidenziale 12333 come responsabile di funzione per l'intelligence dei segnali, incaricato della relativa vigilanza e coordinamento per tutta la comunità dell'intelligence sotto la supervisione del segretario alla Difesa e del Direttore dell'intelligence nazionale. Siedono al SIGCOM i rappresentanti di tutti i servizi della comunità dell'intelligence e, via via che gli USA daranno piena attuazione alla PPD-28, anche rappresentanti di tutti gli altri dipartimenti e enti che hanno un interesse politico per l'intelligence dei segnali.

Tutti i dipartimenti e enti degli Stati Uniti che fruiscono dell'intelligenza esterna presentano la domanda di raccogliere dati al SIGCOM. Il SIGCOM esamina la richiesta, ne verifica la conformità al NIPF e le attribuisce una priorità secondo criteri basati sulla risposta a domande quali:

— È in grado l'intelligence dei segnali di offrire informazioni utili nel caso di specie oppure altre fonti di informazione possono rivelarsi migliori o più economiche, ad esempio immagini o fonti aperte?

— Quanto importante è l'esigenza d'informazione? Se il NIPF le attribuisce una priorità elevata, nella maggior parte dei casi la priorità sarà elevata anche nell'ambito dell'intelligence dei segnali.

— Che tipo di intelligence dei segnali si potrebbe usare?

— La raccolta è quanto più possibile mirata? Sono opportune limitazioni temporali, geografiche o di altro tipo?

La procedura di verifica dei requisiti per l'intelligence dei segnali seguita negli USA implica anche che si tenga conto di altre considerazioni:

— L'obiettivo della raccolta o la metodologia usata per la raccolta sono particolarmente sensibili? In caso affermativo è necessaria una valutazione politica ad alto livello.

— La raccolta presenta un rischio ingiustificato per la privacy e le libertà civili, a prescindere dalla cittadinanza?

— È necessario tutelare la privacy o la sicurezza nazionale con ulteriori garanzie in termini di divulgazione e conservazione?

A conclusione della procedura membri adeguatamente formati del personale dell'NSA studiano le priorità convalidate dal SIGCOM per individuare i selettori specifici, quali numeri di telefono o indirizzi di posta elettronica, da usare nella raccolta dei dati di intelligence esterna per rispondere alle priorità. Il selettore dev'essere verificato e approvato prima dell'inserimento nei sistema di raccolta dell'NSA. Anche quando tutte queste premesse sono assolte, l'opportunità di passare all'effettiva raccolta dei dati e il momento in cui procedervi dipendono comunque anche da altre considerazioni,

([1]) *Consultabile all'indirizzo*http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

ad esempio dalla disponibilità di risorse adeguate. La procedura assicura che, negli USA, l'obiettivo della raccolta dati nell'ambito dell'intelligence dei segnali rispecchi un'esigenza valida e importante di intelligence esterna. Se i dati sono raccolti in applicazione della FISA, l'NSA e gli altri enti devono ovviamente rispettare le ulteriori limitazioni approvate dalla Corte di vigilanza sull'intelligence esterna. In sostanza, né l'NSA né altro ente statunitense di intelligence decide da solo che dati raccogliere.

La procedura assicura pertanto che le priorità degli USA in materia di intelligence siano stabilite ad alto livello politico, ossia al livello che si trova nella migliore posizione per individuare le esigenze statunitensi in tema di intelligence esterna, tenendo conto non soltanto del valore potenziale dei dati raccolti ma anche dei rischi associati alla raccolta, compreso per la privacy, degli interessi economici nazionali e delle relazioni esterne.

Quanto ai dati trasmessi nell'ambito dello scudo, sebbene gli Stati Uniti non possano né confermare né negare il ricorso a metodi o operazioni d'intelligence specifici, va rilevato che le disposizioni della PPD-28 si applicano a qualsiasi operazione d'intelligence condotta dagli USA, a prescindere dal tipo di dati raccolti o dalla fonte cui sono attinti. Inoltre, le limitazioni e garanzie applicabili alla raccolta dati nell'ambito dell'intelligence dei segnali si applicano ai dati raccolti per qualsiasi finalità autorizzata, comprese le finalità inerenti alle relazioni esterne e alla sicurezza nazionale.

Le procedure descritte indicano un impegno chiaro a impedire la rilevazione arbitraria e indiscriminata di informazioni nell'ambito dell'intelligence dei segnali e a applicare, a partire dai massimi livelli del governo statunitense, il principio della ragionevolezza. La PPD-28 e le procedure attuative stabilite dagli enti precisano le limitazioni vigenti e nuove applicabili alla raccolta e all'uso dei dati acquisiti dagli USA nell'ambito dell'intelligence dei segnali e ne illustrano in maggior dettaglio la finalità, rassicurando così sul fatto che le attività di intelligence dei segnali sono e saranno sempre condotte solo per perseguire scopi legittimi di intelligence esterna.

c. **Limitazioni applicabili alla conservazione e alla divulgazione**

A norma della PPD-28, articolo 4, ciascun servizio della comunità dell'intelligence statunitense deve rispettare per i cittadini stranieri, relativamente alla conservazione e divulgazione delle informazioni personali rilevate nell'ambito dell'intelligence dei segnali, limiti fissati espressamente che siano comparabili a quelli applicati per i cittadini statunitensi o residenti negli USA. Queste norme sono previste nelle procedure per ciascun ente della comunità dell'intelligence pubblicate a febbraio 2015 e messe a disposizione del pubblico. Per essere ammesse alla conservazione o divulgazione come intelligence esterna, le informazioni personali devono riguardare un'esigenza di intelligence autorizzata emersa dalla procedura NIPF di cui sopra, essere ritenute, con ragionevolezza, prove di un reato oppure soddisfare uno degli altri criteri per la conservazione delle informazioni personali dei cittadini statunitensi o residenti negli USA indicati nel decreto presidenziale 12333, articolo 2.3.

Le informazioni non conformi a dette prescrizioni non possono essere conservate per oltre cinque anni, a meno che il Direttore dell'intelligence nazionale stabilisca espressamente che il prolungamento della conservazione è nell'interesse della sicurezza nazionale degli Stati Uniti d'America. I servizi della comunità dell'intelligence statunitense devono pertanto cancellare le informazioni personali relative ai cittadini stranieri cinque anni dopo averle rilevate, a meno che, ad esempio, l'informazione sia ritenuta pertinente ai fini di un'esigenza autorizzata di intelligence esterna o che il Direttore dell'intelligence nazionale stabilisca, sentiti il responsabile della tutela delle libertà civili dell'ODNI e i responsabili della tutela della vita privata e delle libertà civili degli enti, che il prolungamento della conservazione è nell'interesse della sicurezza nazionale degli Stati Uniti d'America.

Tutte le politiche adottate dagli enti in applicazione della PPD-28 vietano ora esplicitamente la divulgazione delle informazioni relative a una persona per il solo motivo che si tratta di uno straniero, e questa disposizione trova riscontra in una direttiva rivolta dall'ODNI a tutti i servizi della comunità dell'intelligence ([1]). Il personale della comunità dell'intelligence riceve l'istruzione specifica di tenere conto della necessità di tutelate la privacy degli stranieri nella stesura e divulgazione dei rapporti di intelligence. In particolare, i dati ricavati dall'intelligence dei segnali sulle attività abituali di uno straniero non possono essere considerati intelligence esterna da poter divulgare o conservare in via permanente per il solo fatto che riguardano uno straniero, a meno che rispondano altrimenti a un'esigenza autorizzata di intelligence esterna. È così riconosciuta una limitazione importante, in risposta ai dubbi sollevati dalla Commissione europea circa l'ampiezza della definizione di intelligence esterna ai sensi del decreto presidenziale 12333.

([1]) Direttiva sulla comunità dell'intelligence (ICD) 203, *consultabile all'indirizzo* http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Garanzia della conformità e vigilanza**

Il sistema statunitense di vigilanza sull'intelligence esterna prevede una vigilanza rigorosa e multilivello per assicurare la conformità alle leggi e procedure applicabili, anche in tema di raccolta, conservazione e divulgazione delle informazioni personali che riguardano stranieri acquisite tramite l'intelligence dei segnali secondo quanto disposto dalla PPD-28. Il sistema si articola negli elementi indicati qui di seguito.

— Lavorano per la comunità dell'intelligence centinaia di addetti alla vigilanza. La sola NSA impiega oltre 300 persone per la garanzia della conformità, cui si aggiungono altre persone che svolgono anche funzioni di vigilanza. Il Dipartimento della Giustizia assicura un'estesa vigilanza sulle attività d'intelligence, e un'analoga funzione svolge anche il Dipartimento della Difesa.

— Ciascun servizio della comunità dell'intelligence dispone di un proprio Ufficio dell'ispettore generale, incaricato tra l'altro di vigilare sulle attività di intelligence esterna. Gli ispettori generali sono indipendenti per legge, godono di ampi poteri di indagine, verifica e esame dei programmi, anche in materia di frode e abuso o violazione della legge, e hanno facoltà di raccomandare misure correttive. Sebbene le raccomandazioni dell'ispettore generale non siano vincolanti, le relazioni emananti dal suo ufficio sono spesso rese pubbliche, e comunque sono trasmesse al Congresso, comprese le relazioni di sollecito nei casi in cui non sia ancora stato realizzato l'intervento correttivo raccomandato in una relazione precedente. Il Congresso viene quindi informato di tutti i casi di mancata conformità e può esercitare pressione affinché sia realizzato il provvedimento correttivo, anche agendo sul bilancio. Sono stati pubblicati vari rapporti degli ispettori generali dedicati a programmi di intelligence ([1]).

— L' Ufficio per la tutela della vita privata e le libertà civili dell'ODNI è incaricato di assicurare che la comunità dell'intelligence operi con modalità che favoriscano la sicurezza nazionale sempre nel rispetto delle libertà civili e dei diritti alla tutela della vita privata ([2]). Addetti alla privacy lavorano presso altri servizi della comunità dell'intelligence.

— L'Autorità per la tutela della vita privata e delle libertà civili, organo indipendente costituito per legge, è incaricata dell'analisi e della verifica dei programmi e delle politiche di lotta al terrorismo, intelligence dei segnali compresa, per garantire che tutelino adeguatamente la privacy e le libertà civili. Diverse sue relazioni sulle attività d'intelligence sono state rese pubbliche.

— Come illustrato più diffusamente *infra*, la Corte di vigilanza sull'intelligence esterna, collegio composto di giudici federali indipendenti, ha la responsabilità della vigilanza sulle attività di raccolta dati nell'ambito dell'intelligence dei segnali condotte a norma della FISA, e del controllo della relativa conformità.

— Infine, il Congresso degli Stati Uniti d'America, e più precisamente le commissioni Giustizia e Intelligence della Camera dei rappresentanti e del Senato, ha importanti competenze di supervisione su tutte le attività d'intelligence esterna condotte dagli USA, intelligence dei segnali compresa.

Oltre a detti organi ufficiali, la comunità dell'intelligence ha predisposto vari meccanismi per assicurare il rispetto delle limitazioni della raccolta illustrate *supra*, per esempio:

— il Gabinetto è tenuto a convalidare ogni anno le rispettive esigenze di intelligence dei segnali;

— l'NSA controlla l'obiettivo dell'intelligence dei segnali durante l'intera procedura di raccolta dati, per verificare se da esso scaturiscano effettivamente valide informazioni d'intelligence esterna consone alle priorità, e cessa la raccolta sugli obiettivi che non rispondono a tale criterio. Grazie a altre procedure si assicura la verifica periodica dei selettori.

([1]) Cfr., *ad esempio*, rapporto dell'ispettore generale del Dipartimento della Giustizia statunitense «A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008» (settembre 2012), *consultabile all'indirizzo* https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Cfr. www.dni.gov/clpo.

— In base alla raccomandazione emanata da un gruppo indipendente di verifica nominato dal presidente Obama, il Direttore dell'intelligence nazionale ha istituito un nuovo meccanismo di monitoraggio della raccolta e diffusione dell'intelligence dei segnali di natura particolarmente sensibile dato l'obiettivo che riguarda o il mezzo con cui è rilevata, nell'intento di garantirne la conformità alle decisioni politiche;

— l'ODNI verifica a cadenza annuale come la comunità dell'intelligence distribuisca le risorse rispetto alle priorità del NIPF e l'adempimento della missione di intelligence nel suo insieme. La verifica si basa su valutazioni del valore di tutti i tipi di raccolta di dati d'intelligence, intelligence dei segnali compresa, sia in retrospettiva (è riuscita la comunità dell'intelligence a centrare gli obiettivi fissati?) sia in prospettiva (quali saranno in futuro le esigenze della comunità dell'intelligence?). In questo modo si assicura che le risorse dell'intelligence dei segnali siano dedicate alle priorità nazionali più importanti.

Come risulta dalla presente panoramica, la comunità dell'intelligence non decide autonomamente quali conversazioni ascoltare né cerca di raccogliere tutto né opera al di fuori di ogni controllo. Le sue attività si concentrano sulle priorità stabilite dai responsabili politici attraverso una procedura che implica contributi provenienti da tutto il governo ed è sottoposta sia alla vigilanza interna dell'NSA sia alla vigilanza dell'ODNI, del Dipartimento della Giustizia e del Dipartimento della Difesa.

La PPD-28 prevede numerose altre disposizioni per garantire che le informazioni personali nell'ambito dell'intelligence dei segnali siano tutelate a prescindere dalla cittadinanza della persona. Prevede, ad esempio, procedure per la sicurezza dei dati, l'accesso ai dati e la qualità, al fine di tutelare le informazioni personali raccolte nell'ambito dell'intelligence dei segnali, così come prevede per la forza lavoro una formazione obbligatoria sulla responsabilità di tutelare le informazioni personali a prescindere dalla cittadinanza della persona. La PPD-28 prevede anche ulteriori meccanismi di vigilanza e di garanzia della conformità, tra cui verifiche e controlli, ad opera degli addetti alla vigilanza e alla garanzia della conformità, delle pratiche seguite per tutelare le informazioni personali ricavate dall'intelligence dei segnali. Le verifiche devono controllare anche se l'ente opera in conformità delle procedure volte a tutelare tali informazioni.

A norma della PPD-28, i problemi di conformità rilevanti che interessano stranieri devono essere trattati dal governo ad alto livello. Se si pone un problema di questo tipo relativamente a informazioni personali di una persona raccolte nell'ambito di attività di intelligence dei segnali, ai vigenti obblighi di segnalazione si aggiunge l'obbligo di informarne immediatamente il Direttore dell'intelligence nazionale. Se sono interessate informazioni personali relative a un cittadino straniero, il Direttore dell'intelligence nazionale stabilisce, in consultazione con il segretario di Stato e il capo del pertinente servizio della comunità dell'intelligence, se occorra intervenire per informare il relativo governo straniero, ferma restando la necessità di proteggere la fonte, il metodo e il personale degli USA. Come prescritto dalla PPD-28, il segretario di Stato ha nominato un esponente di alto livello, la Sottosegretaria Catherine Novelli, referente per i governi stranieri che si pongono interrogativi sulle attività di intelligence dei segnali condotte dagli Stati Uniti d'America. Questo coinvolgimento a alto livello è esemplificativo degli sforzi compiuti negli ultimi anni dal governo degli Stati Uniti per instillare fiducia nelle numerose e intersecanti tutele della vita privata vigenti riguardo alle informazioni personali dei cittadini statunitensi o residenti negli USA e dei cittadini stranieri.

e. **Sintesi**

Le procedure seguite negli Stati Uniti per la raccolta, la conservazione e la divulgazione di intelligence esterna prevedono tutele importanti riguardo alle informazioni personali di tutti, indipendentemente dalla cittadinanza. Assicurano in particolare che la comunità dell'intelligence statunitense si concentri sull'adempimento della missione di sicurezza nazionale autorizzata dalle vigenti leggi, decreti e direttive presidenziali, protegga le informazioni dall'accesso, uso e divulgazione non autorizzati e operi sottostando a vari livelli di verifica e supervisione, compresa la vigilanza delle commissioni del Congresso. La PPD-28 e le relative procedure di attuazione sono l'elemento fondante degli sforzi degli USA tesi a estendere la minimizzazione della raccolta e altri principi rilevanti di protezione dei dati alle informazioni personali di tutti, indipendentemente dalla cittadinanza. Alle informazioni personali rilevate dagli USA nell'ambito dell'intelligence dei segnali si applicano i principi e gli obblighi stabiliti dalla legge statunitense e dagli indirizzi presidenziali, comprese le tutele previste dalla PPD-28. In linea con questi principi e obblighi, ognuno deve essere trattato con dignità e rispetto, a prescindere dalla cittadinanza o dal luogo di residenza, e a ciascuno è riconosciuto un legittimo interesse alla tutela della propria vita privata nel quadro del trattamento delle informazioni personali che lo riguardano.

II. LEGGE RELATIVA ALLA VIGILANZA SULL'INTELLIGENCE ESTERNA — ARTICOLO 702

A norma dell'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna (FISA) ([1]), le informazioni non possono essere rilevate in massa e indiscriminatamente: la raccolta deve limitarsi strettamente ai dati di intelligence esterna ricavati da obiettivi identificati individualmente e legittimamente, dev'essere autorizzata chiaramente da un potere esplicito stabilito dalla legge ed è soggetta sia a sindacato giurisdizionale indipendente sia alla verifica e alla vigilanza sostanziali dell'esecutivo e del Congresso. La raccolta di dati ai sensi dell'articolo 702 è considerata intelligence dei segnali vincolata alle disposizioni della PPD-28 ([2]).

La raccolta dati di cui all'articolo 702 è una delle fonti di intelligence più preziose per proteggere tanto gli Stati Uniti quanto i partner europei. Sono a disposizione del pubblico ampie informazioni sul funzionamento dell'articolo 702 e la relativa attività di vigilanza. Numerosi fascicoli giudiziari, decisioni giudiziarie e relazioni di vigilanza relativi al programma sono stati declassificati e sono consultabili sul sito web dell'ODNI dedicato alla divulgazione al pubblico (www.icontherecord.tumblr.com). Inoltre, l'Autorità per la tutela della vita privata e delle libertà civili ha presentato un'analisi generale dell'articolo 702 in un rapporto consultabile all'indirizzo https://www.pclob.gov/library/702-Report.pdf ([3]).

L'articolo 702, che è stato emanato con la legge di modifica della FISA del 2008 ([4]) a seguito di un ampio dibattito pubblico in sede di Congresso, autorizza l'acquisizione, assistita obbligatoriamente dai fornitori statunitensi di servizi di comunicazione elettronica, di informazioni di intelligence esterna ottenuta prendendo a obiettivo cittadini stranieri situati al di fuori degli Stati Uniti. L'articolo 702 conferisce al Procuratore generale e al Direttore dell'intelligence nazionale (entrambi membri del Gabinetto, nominati dal presidente e confermati dal Senato) il potere di presentare certificazioni annuali alla Corte FISA ([5]). Queste certificazioni indicano le categorie specifiche dei dati di intelligence esterna da rilevare, come ad esempio intelligence relativa alla lotta contro il terrorismo o alle armi di distruzione di massa, che devono rientrare nelle categorie di intelligence esterna stabilite dalla legge sulla FISA ([6]). Come ha rilevato l'Autorità per la tutela della vita privata e delle libertà civili, queste limitazioni *non* permettono la raccolta indiscriminata di informazioni sui cittadini stranieri ([7]).

La certificazione è necessaria anche per contemplare le procedure atte a rendere mirata e a minimizzare la raccolta dati, che devono essere verificate e approvate dalla Corte FISA ([8]). Scopo delle procedure atte a rendere mirata la raccolta dati è assicurare che questa sia effettuata solo nei limiti autorizzati dalla legge e sia contemplata dalla certificazione; le procedure di minimizzazione intendono limitare l'acquisizione, la divulgazione e la conservazione delle informazioni che riguardano cittadini statunitensi o residenti negli USA, ma prevedono anche disposizioni (illustrate qui di seguito) che offrono una protezione sostanziale delle informazioni riguardanti cittadini stranieri. Come illustrato supra, con la PPD-28 il presidente ha ordinato alla comunità dell'intelligence di offrire protezioni supplementari per le informazioni personali che riguardano i cittadini stranieri, e queste protezioni si applicano alle informazioni raccolte a norma dell'articolo 702.

Una volta che il giudice ha approvato le procedure atte a rendere mirata e a minimizzare la raccolta dati, i dati rilevati a norma dell'articolo 702 non sono raccolti in blocco o indiscriminatamente, bensì, come affermato dall'Autorità per la tutela della vita privata e delle libertà civili, sempre in modo mirato alla singola persona ([9]). Per rendere mirata la rilevazione dei dati si ricorre a singoli selettori, quali indirizzi di posta elettronica o numeri di telefono, di cui, secondo

([1]) Codice degli Stati Uniti d'America, titolo 50, articolo 1881a.

([2]) Gli Stati Uniti possono anche ottenere un'ordinanza del giudice ai sensi di altre disposizioni della FISA relativamente alla produzione di dati, compresi i dati trasferiti nell'ambito dello scudo (cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1801 e ss). A norma dei titoli I e III della FISA, che autorizzano rispettivamente la sorveglianza elettronica e le perquisizioni fisiche, sono necessari (tranne in situazioni d'emergenza) un'ordinanza del giudice e sempre un motivo plausibile per ritenere che l'obiettivo della raccolta dati sia una potenza straniera o l'agente di una potenza straniera. Il titolo IV della FISA autorizza, su ordinanza del giudice (tranne in situazioni d'emergenza), l'uso di dispositivi di intercettazione dei dati informativi della comunicazione (in entrata e in uscita) nelle indagini autorizzate di intelligence esterna, controspionaggio o antiterrorismo. Il titolo V della FISA consente all'FBI, su ordinanza del giudice (tranne in situazioni d'emergenza), di ottenere i documenti aziendali d'interesse per un'indagine autorizzata di intelligence esterna, controspionaggio o antiterrorismo. Come illustrato qui di seguito, la legge USA FREEDOM vieta specificamente l'uso dell'ordinanza relativa all'intercettazione dei dati informativi o ai documenti aziendali per una raccolta in blocco e impone l'impiego di un selettore specifico al fine di assicurare che i poteri in tal senso siano usati in modo mirato.

([3]) Autorità per la tutela della vita privata e delle libertà civili, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 luglio 2014 («rapporto PCLOB»).

([4]) Cfr. Pub. L. n. 110-261, 122 Stat. 2436 (2008).

([5]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1881a(a) e (b).

([6]) *Ibid*. articolo 1801(e).

([7]) Cfr. rapporto PCLOB, 99.

([8]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1881a(d) e (e).

([9]) Cfr. rapporto PCLOB, 111.

i servizi d'intelligence statunitensi, è probabile l'uso per la comunicazione di informazioni di intelligence esterna del tipo contemplato dalla certificazione presentata al giudice ([1]). Il motivo in base al quale è scelto l'obiettivo dev'essere documentato e per ciascun selettore la documentazione è successivamente verificata dal Dipartimento della Giustizia ([2]). Il governo degli Stati Uniti ha comunicato che, nel 2014, hanno costituito obiettivi a norma dell'articolo 702 circa 90 000 persone, ossia una percentuale minima degli oltre 3 miliardi di utenti Internet presenti nel mondo ([3]).

Alle informazioni raccolte a norma dell'articolo 702 si applicano le procedure di minimizzazione approvate dal giudice, le quali prevedono tutele tanto per i cittadini statunitensi o residenti negli USA quanto per gli stranieri e sono state rese pubbliche ([4]). Ad esempio, le comunicazioni acquisite a norma dell'articolo 702, riguardino esse cittadini statunitensi o residenti negli USA oppure cittadini stranieri, sono conservate in banche dati per cui vigono rigorosi controlli di accesso. Possono essere esaminate soltanto da personale addetto all'intelligence che è stato formato alle procedure di minimizzazione finalizzate alla tutela della privacy e il cui accesso a tali comunicazioni è stato approvato specificamente per lo svolgimento delle funzioni autorizzate ([5]). I dati possono essere usati solo per ricavare informazioni d'intelligence esterna o come prove di un reato ([6]). A norma della PPD-28 le informazioni possono essere divulgate solo in presenza di una finalità valida di intelligence esterna o di applicazione della legge: non è sufficiente il semplice fatto che una delle parti della comunicazione sia un cittadino straniero ([7]). Le procedure di minimizzazione e la PPD-28 fissano inoltre limiti temporali sul periodo di conservazione dei dati acquisiti a norma dell'articolo 702 ([8]).

L'applicazione dell'articolo 702 è sottoposta a un'ampia vigilanza esercitata da tutti e tre i rami del governo statunitense. L'ente che attua la legge dispone di vari livelli di verifica interna, anche da parte dell'ispettore generale indipendente, e di tecnologie che controllano l'accesso ai dati. Il Dipartimento della Giustizia e l'ODNI verificano e esaminano attentamente l'applicazione dell'articolo 702 per accertare che siano rispettate le norme di legge. All'ente è altresì imposto l'obbligo autonomo di segnalare i potenziali casi di inosservanza, su cui viene aperta un'indagine; tutti questi casi sono segnalati alla Corte di vigilanza sull'intelligence esterna, all'Autorità presidenziale di vigilanza sull'intelligence e al Congresso, e implicano l'adozione delle misure correttive del caso ([9]). Non si sono registrati finora casi di tentata violazione intenzionale della legge o di tentata elusione degli obblighi di legge ([10]).

La Corte FISA svolge un ruolo importante nell'attuazione dell'articolo 702. Si tratta di un collegio composto di giudici federali indipendenti che hanno un mandato specifico di sette anni, ma che, al pari di tutti i giudici federali, sono giudici a vita. Come osservato in precedenza, la Corte è incaricata di verificare le certificazioni annuali e le procedure atte a rendere mirata e a minimizzare la raccolta dati per accertare che siano conformi alla legge. Ribadiamo inoltre che il governo è tenuto a comunicarle immediatamente i problemi di conformità ([11]): dai vari pareri declassificati e pubblicati emerge il grado eccezionale di sindacato giurisdizionale e di indipendenza che contraddistingue i lavori della Corte.

Le procedure rigorose seguite dalla Corte sono descritte in una lettera che il suo ex presidente ha trasmesso al Congresso e che è stata resa pubblica ([12]). A seguito della legge USA FREEDOM, illustrata qui di seguito, la Corte è esplicitamente autorizzata a nominare un professionista esterno come avvocato indipendente a difesa della privacy nei casi che pongono questioni giuridiche rilevanti o inedite ([13]). Questo grado di coinvolgimento della magistratura indipendente di un paese nelle attività d'intelligence esterna che hanno come obiettivo una persona che non è cittadina del paese né si trova al suo interno è insolito, se non addirittura inedito, e contribuisce a garantire che la raccolta dati a norma dell'articolo 702 resti entro adeguati limiti di legge.

([1]) *Ibid*.

([2]) *Ibid*., 8; Codice degli Stati Uniti d'America, titolo 50, articolo 1881a(1). *Cfr. anche* Rapporto del Direttore dell'NSA per le libertà civili e la privacy «NSÀs Implementation of Foreign Intelligence Surveillance Act Section 702» («rapporto NSA»), 4, *consultabile all'indirizzo* http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Relazione del Direttore dell'intelligence nazionale sulla trasparenza 2014, *consultabile all'indirizzo* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Per le procedure di minimizzazione cfr.: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf(«procedure di minimizzazione dell'NSA»), http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf e http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Cfr. rapporto NSA, 4.

([6]) Cfr., *ad esempio*, procedure di minimizzazione dell'NSA, 6.

([7]) Per le procedure seguite dagli enti di intelligence in applicazione della PPD-28 cfr.: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Cfr. procedure di minimizzazione dell'NSA, PPD-28, articolo 4.

([9]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1881(1). cfr. *anche* Rapporto PCLOB, 66-76.

([10]) Cfr. Valutazione semestrale del rispetto delle procedure e degli orientamenti emanati a norma dell'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna, presentata dal Procuratore generale e dal Direttore dell'intelligence nazionale, 2-3; *consultabile all'indirizzo* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Articolo 13 del regolamento di procedura della Corte di vigilanza sull'intelligence esterna, *consultabile all'indirizzo* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) Lettera di Reggie B. Walton a Patrick J. Leahy del 29 luglio 2013, *consultabile all'indirizzo* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Cfr. articolo 401 della legge USA FREEDOM, P.L. 114-23.

La vigilanza del Congresso si esplica nell'obbligo di presentare le relazioni previste dalla legge alle commissioni Giustizia e Intelligence e nelle frequenti audizioni e riunioni informative, tra cui: la relazione semestrale in cui il Procuratore generale riferisce sull'applicazione dell'articolo 702 e segnala i casi di inosservanza ([1]), la distinta valutazione semestrale in cui il Procuratore generale e il Direttore dell'intelligence nazionale riferiscono sul rispetto delle procedure atte a rendere mirata e minimizzare la raccolta dati, comprese le procedure volte a garantire che i dati siano raccolti per una finalità valida di intelligence esterna ([2]), e la relazione annuale dei capi dei servizi della comunità dell'intelligence, in cui è tra l'altro certificato che la raccolta dati a norma dell'articolo 702 continua a produrre informazioni di intelligence esterna ([3]).

Riepilogando: la raccolta dati a norma dell'articolo 702 è autorizzata dalla legge, è sottoposta a vari livelli di verifica, di supervisione giudiziaria e di vigilanza e, come sostenuto dalla Corte FISA in un parere declassificato di recente, non è effettuata in blocco né in modo indiscriminato, bensì improntata a decisioni mirate di sorveglianza discreta su singoli sistemi di comunicazione ([4]).

III. LEGGE USA FREEDOM

L'USA FREEDOM, convertita in legge a giugno 2015, ha determinato modifiche rilevanti dei poteri di sorveglianza e di altri poteri in materia di sicurezza nazionale negli USA, aumentando nei confronti del pubblico la trasparenza sul relativo esercizio e sulle decisioni della Corte FISA, come illustrato qui di seguito ([5]). La legge assicura che, negli USA, i professionisti che operano nell'intelligence e nell'applicazione della legge abbiano i poteri necessari per proteggere il paese, garantendo nel contempo che li esercitino rispettando adeguatamente la privacy delle persone. La legge rafforza la tutela della vita privata e le libertà civili e migliora la trasparenza.

La legge vieta la raccolta in blocco di dati, riguardino essi cittadini statunitensi o residenti negli USA oppure cittadini stranieri, a norma di varie disposizioni della FISA o mediante le *National Security Letter*, che sono una forma di citazione amministrativa prevista per legge ([6]). Il divieto comprende specificamente i metadati relativi alle chiamate telefoniche tra persone che si trovano negli USA e persone che si trovano invece all'estero e include anche le informazioni rilevate nell'ambito dello scudo nell'esercizio di tali poteri. La legge prevede che il governo fondi la domanda di raccolta dati nell'esercizio di detti poteri su un selettore specifico, ossia un termine che identifica specificamente una persona, un account, un indirizzo o un dispositivo personale, in modo da limitare al minimo ragionevolmente possibile la gamma delle informazioni ricercate ([7]). Si assicura così anche che la raccolta delle informazioni a fini di intelligence sia mirata con precisione e concentrata sull'obiettivo.

La legge ha introdotto modifiche rilevanti anche riguardo al procedimento dinanzi alla Corte FISA, aumentandone la trasparenza e offrendo garanzie supplementari di tutela della privacy. Come già rilevato, ha autorizzato la creazione di un comitato permanente di avvocati in possesso del nulla osta di sicurezza e di chiara esperienza in materia di tutela della vita privata e libertà civili, raccolta di dati di intelligence, tecnologie della comunicazione o altri settori pertinenti, i quali possono essere designati per comparire dinanzi al giudice in veste di *amicus curiae* nei procedimenti che comportano un'interpretazione rilevante o inedita della legge. Tali avvocati sono autorizzati a presentare argomentazioni giuridiche a difesa della privacy e delle libertà civili e hanno accesso a tutte le informazioni, anche classificate, che il giudice reputa necessarie all'assolvimento della loro funzione ([8]).

La legge muove anche dalla trasparenza senza precedenti instaurata dal governo degli Stati Uniti sulle attività di intelligence, imponendo al Direttore dell'intelligence nazionale, in consultazione con il Procuratore generale, di declassificare, o di pubblicare in forma di sintesi non classificata, ogni decisione, ordinanza o parere pronunciati dalla Corte FISA o dalla Corte di controllo della vigilanza sull'intelligence esterna in cui è riportata una spiegazione o interpretazione rilevante di una disposizione di legge.

([1]) Cfr. Codice degli Stati Uniti d'America, titolo 50, articolo 1881f.
([2]) *Ibid*. articolo 1881a(l)(1).
([3]) *Ibid*. articolo 1881a(l)(3). Alcune di queste relazioni sono classificate.
([4]) Mem. parere e ordinanza, 26 (FISC 2014), *consultabile all'indirizzo* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) Cfr. legge USA FREEDOM del 2015, Pub. L. n. 114-23, articoli 401, 129 Stat. 268.
([6]) *Ibid*. articoli 103, 201, 501. Le *National Security Letter* sono autorizzate da una serie di norme e consentono all'FBI di ottenere, solo a fini di protezione dal terrorismo internazionale o da attività di intelligence clandestine, le informazioni contenute in rapporti di credito, documenti finanziari e archivi elettronici di abbonati e di dati transazionali ottenuti da alcuni tipi di società (*cfr.* Codice degli Stati Uniti d'America, titolo 12, articolo 3414; titolo 15, articoli 1681u-1681v; titolo 18, articolo 2709). Tipicamente l'FBI ricorre alle *National Security Letter* per ottenere, nelle prime fasi di un'indagine di antiterrorismo o controspionaggio, informazioni fondamentali non di contenuto, quali l'identità dell'abbonato a un dato account che potrebbe essere stato in comunicazione con membri di un'organizzazione terroristica come l'ISIL. Il destinatario della *National Security Letter* ha diritto di contestarla per via giudiziaria (*cfr.* Codice degli Stati Uniti d'America, titolo 18, articolo 3511).
([7]) *Ibid*.
([8]) *Ibid*. articolo 401.

La legge prevede un'ampia divulgazione delle richieste relative alle informazioni raccolte a norma della FISA e alle *National Security Letter*. Gli Stati Uniti devono dichiarare ogni anno al Congresso e al pubblico, tra l'altro, il numero delle ordinanze e delle certificazioni ai sensi della FISA chieste e ottenute, il numero stimato dei cittadini statunitensi o residenti negli USA e dei cittadini stranieri che hanno costituito obiettivi della sorveglianza e che ne sono stati interessati e il numero di *amici curiae* designati ([1]). La legge impone inoltre al governo altre comunicazioni al pubblico riguardo al numero di richieste di *National Security Letter* che hanno interessato cittadini statunitensi o residenti negli USA e cittadini stranieri ([2]).

Per quanto riguarda la trasparenza delle imprese, la legge offre alle imprese una serie di opzioni per la comunicazione pubblica del numero aggregato di ordinanze ai sensi della FISA e direttive o *National Security Letter* ricevute dal governo, e del numero di account di clienti interessati da tali provvedimenti ([3]). Le comunicazioni già effettuate da varie imprese hanno messo in luce il limitato numero di clienti di cui sono stati richiesti i dati.

Dalle relazioni sulla trasparenza elaborate dalle imprese emerge che le richieste di intelligence avanzate dagli Stati Uniti interessano soltanto una percentuale minima di dati. Ad esempio, nella recente relazione sulla trasparenza un'importante società indica di aver ricevuto richieste nell'ambito della sicurezza nazionale (richieste a norma della FISA o *National Security Letter*) relativamente a meno di 20 000 account a fronte degli oltre 400 milioni di abbonati, ossia, per il totale delle richieste avanzate dagli USA per ragioni di sicurezza nazionale, meno di.005 % dei suoi abbonati. Anche se ciascuna di tali richieste avesse riguardato dati nell'ambito dell'approdo sicuro (il che non è ovviamente il caso), risulta comunque evidente che le richieste sono mirate e adeguate per scala e che non implicano una raccolta di dati in blocco o indiscriminata.

Infine, sebbene le norme che autorizzano le National Security Letter abbiano già limitato le situazioni in cui può essere vietato al destinatario di divulgarle, la legge prevede anche che i rimanenti obblighi di non divulgazione siano sottoposti periodicamente a riesame e che il destinatario sia informato se i fatti non giustificano più l'obbligo di non divulgazione, e stabilisce procedure codificate mediante le quali il destinatario può contestare gli obblighi di non divulgazione ([4]).

In sostanza, le modifiche rilevanti dei poteri di intelligence introdotte dalla legge USA FREEDOM costituiscono la prova evidente del grande sforzo compiuto dagli Stati Uniti per improntare tutte le loro pratiche di intelligence alla tutela dei dati personali, al rispetto della vita privata, alle libertà civili e alla trasparenza.

IV. TRASPARENZA

Oltre alla trasparenza disposta dalla legge USA FREEDOM, la comunità dell'intelligence statunitense comunica al pubblico molte altre informazioni, affermandosi così come esempio di trasparenza sulle attività di intelligence svolte. Ha pubblicato molte delle politiche e procedure seguite, decisioni della Corte di vigilanza sull'intelligence esterna e altra documentazione declassificata, dimostrando un grado straordinario di trasparenza. La comunità dell'intelligence ha inoltre aumentato considerevolmente la pubblicazione dei dati statistici sull'esercizio, da parte del governo, dei poteri di raccolta a fini di tutela della sicurezza nazionale. Il 22 aprile 2015 la comunità dell'intelligence ha pubblicato la seconda relazione annuale in cui presenta i dati statistici relativi alla frequenza con cui il governo esercita tali importanti poteri. Anche l'ODNI ha pubblicato, sia sul proprio sito web sia su *IC On the Record*, una serie di principi sulla trasparenza ([5]) e un piano d'attuazione che li traduce in iniziative concrete e quantificabili ([6]). A ottobre 2015 il Direttore dell'intelligence nazionale ha chiesto a ciascun ente dell'intelligence di nominare, all'interno del gruppo dirigente, un responsabile della trasparenza nell'intelligence incaricato di promuovere la trasparenza e di guidare le iniziative in materia ([7]). In ciascun ente il responsabile della trasparenza collaborerà strettamente con l'addetto alla tutela della vita privata e alle libertà civili per assicurare che gli aspetti della trasparenza, della tutela della vita privata e delle libertà civili mantengano sempre la massima priorità.

([1]) *Ibid*. articolo 602.
([2]) *Ibid*.
([3]) *Ibid*. articolo 603.
([4]) *Ibid*. articoli 502(f)–503.
([5]) *Consultabile all'indirizzo* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) *Consultabile all'indirizzo* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) *Ibid*.

Per citare un esempio dell'impegno verso la trasparenza, negli ultimi anni il responsabile della tutela della vita privata e delle libertà civili dell'NSA ha pubblicato varie relazioni non classificate, tra cui rapporti sulle attività condotte a norma dell'articolo 702, del decreto presidenziale 12333 e della legge USA FREEDOM ([1]). La comunità dell'intelligence collabora da vicino con l'Autorità per la tutela della vita privata e delle libertà civili, con il Congresso e con il mondo associativo che si occupa di promozione della privacy negli USA per migliorare ulteriormente la trasparenza sulle attività di intelligence degli Stati Uniti, ogniqualvolta questo sia possibile e compatibile con la protezione delle fonti di intelligence sensibile e dei relativi metodi. Nel complesso le attività di intelligence degli Stati Uniti sono altrettanto trasparenti di quelle di qualsiasi altro paese al mondo, se non più trasparenti, e comunque il più trasparenti possibile in considerazione dell'esigenza di proteggere le fonti e i metodi sensibili.

Segue una sintesi degli aspetti che evidenziano l'ampia trasparenza sulle attività di intelligence condotte dagli Stati Uniti.

— La comunità dell'intelligence ha divulgato e pubblicato in rete pareri della Corte e procedure degli enti per migliaia di pagine, nelle quali sono delineati gli obblighi e le procedure specifici delle attività di intelligence condotte dagli USA. Sono state pubblicate anche relazioni sul rispetto delle limitazioni applicabili da parte degli enti di intelligence.

— Esponenti di alto livello dell'intelligence si esprimono regolarmente in pubblico sui ruoli e le attività della rispettiva organizzazione, illustrando anche il regime di controllo della conformità e le garanzie che presiedono alla relativa attività.

— La comunità dell'intelligence ha pubblicato vari altri documenti sulle attività di intelligence a norma della legge sulla libertà di informazione.

— Il presidente ha emanato la PPD-28, stabilendo pubblicamente limitazioni supplementari alle attività di intelligence, e l'ODNI ha emanato due relazioni pubbliche sull'attuazione di tali limitazioni.

— La comunità dell'intelligence è ora tenuta per legge a pubblicare i pareri giuridici rilevanti emessi dalla Corte FISA o una loro sintesi.

— Il governo è tenuto a riferire annualmente sulla misura in cui ha esercitato taluni poteri nell'ambito della sicurezza nazionale; altrettanto sono autorizzate a fare le imprese.

— L'Autorità per la tutela della vita privata e delle libertà civili ha pubblicato varie relazioni dettagliate sulle attività di intelligence e continuerà a pubblicarne.

— La comunità dell'intelligence trasmette ampie informazioni classificate alle commissioni di vigilanza del Congresso.

— Il Direttore dell'intelligence nazionale ha emanato principi sulla trasparenza cui deve attenersi la comunità dell'intelligence nelle proprie attività.

Quest'ampia trasparenza continuerà in futuro. Le informazioni divulgate pubblicamente sono ovviamente a disposizione del Dipartimento del Commercio e della Commissione europea. L'analisi annuale dell'attuazione dello scudo, cui si dedicheranno il Dipartimento del Commercio e la Commissione europea, offrirà alla Commissione europea l'occasione di affrontare tutte le questioni sollevate dalle nuove informazioni divulgate e di discutere qualsiasi altra questione inerente allo scudo e al relativo funzionamento: ci consta infatti che il Dipartimento del Commercio può scegliere di coinvolgere nel processo di analisi rappresentanti di altri enti, comunità dell'intelligence compresa. Questa possibilità viene ovviamente ad aggiungersi al meccanismo previsto dalla PPD-28, in base al quale gli Stati membri dell'UE possono sollevare questioni inerenti alla sorveglianza con il funzionario del Dipartimento di Stato designato a tal fine.

V. MEZZI DI RICORSO

La legge statunitense apre varie possibilità di ricorso alla persona sottoposta illecitamente a sorveglianza elettronica per finalità di sicurezza nazionale. A norma della FISA, il diritto di ricorso dinanzi a un giudice statunitense non è limitato ai cittadini statunitensi o residenti negli USA. La persona in grado di dimostrare la propria legittimazione ad agire in giustizia dispone, a norma della FISA, di mezzi di ricorso contro la sorveglianza elettronica illecita. La FISA consente ad

([1]) *Consultabili agli indirizzi* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

esempio alla persona sottoposta illecitamente a sorveglianza elettronica di citare in giudizio un agente del governo statunitense a titolo personale per ottenere un risarcimento pecuniario, compresi i danni punitivi e il rimborso delle spese legali (*cfr.* Codice degli Stati Uniti d'America, titolo 50, articolo 1810). La persona in grado di dimostrare la propria legittimazione ad agire in giudizio dispone inoltre della possibilità d'intentare contro gli Stati Uniti un'azione civile di risarcimento pecuniario, comprese le spese di giudizio, in caso di uso o divulgazione illeciti e deliberati di informazioni che la riguardano, ottenute da attività di sorveglianza elettronica a norma della FISA (*cfr.* Codice degli Stati Uniti d'America, titolo 18, articolo 2712). Se intende usare o divulgare informazioni ottenute o ricavate dalla sorveglianza elettronica della persona lesa a norma della FISA contro la persona stessa nell'ambito di un procedimento giudiziario o amministrativo negli Stati Uniti, il governo deve dare comunicazione preventiva di tale intenzione al giudice e alla persona, la quale può quindi contestare la legittimità della sorveglianza e chiedere la soppressione delle informazioni (*cfr.* Codice degli Stati Uniti d'America, titolo 50, articolo 1806). La FISA prevede infine sanzioni penali per la persona che procede intenzionalmente a un'attività illecita di sorveglianza elettronica compiendo un abuso di potere o che intenzionalmente usa o divulga informazioni ottenute da un'attività illecita di sorveglianza (*cfr.* Codice degli Stati Uniti d'America, titolo 50, articolo 1809).

Qualora il governo faccia un uso illegittimo dei dati o vi acceda illecitamente, il cittadino dell'UE dispone di altri mezzi di ricorso nei confronti degli agenti del governo statunitense, inclusi gli agenti che violano la legge accedendo illegalmente alle informazioni, o usandole illecitamente, per presunte finalità di sicurezza nazionale. La legge sulle frodi e gli abusi informatici vieta l'accesso intenzionale non autorizzato (o l'abuso dell'accesso autorizzato) finalizzato a ottenere informazioni da un istituto finanziario, da un sistema informatico del governo statunitense oppure da un computer in cui si è entrati via Internet, così come vieta la minaccia di danneggiare computer protetti finalizzata all'estorsione o alla frode (*cfr.* Codice degli Stati Uniti d'America, titolo 18, articolo 1030). Indipendentemente dall'esercizio o meno dell'azione penale, chiunque, a prescindere dalla cittadinanza, subisca un danno o una perdita a causa di una violazione di tale legge può avviare contro il trasgressore (anche se agente del governo) un'azione di risarcimento danni e chiedere nei suoi confronti un provvedimento inibitorio o altra forma di riparazione equa a norma dell'articolo 1030(g), a condizione che la condotta tenuta implichi almeno una delle diverse circostanze indicate dalla legge. La legge sulla privacy nelle comunicazioni elettroniche disciplina l'accesso del governo agli archivi di dati sulle comunicazioni elettroniche, ai dati transazionali e alle informazioni sugli abbonati detenuti da terzi fornitori di servizi di comunicazione (*cfr.* Codice degli Stati Uniti d'America, titolo 18, articoli 2701-2712). Detta legge autorizza la persona lesa a citare in giudizio l'agente del governo per accesso illecito intenzionale ad archivi di dati. Essa si applica a chiunque, indipendentemente dalla cittadinanza, e la persona lesa può ottenere un risarcimento danni e il rimborso delle spese legali. La legge sul diritto alla privacy finanziaria limita l'accesso del governo statunitense ai dati relativi al singolo cliente detenuti da banche e intermediari finanziari (*cfr.* Codice degli Stati Uniti d'America, titolo 12, articoli 3401-3422). A norma di detta legge, il cliente della banca o dell'intermediario può citare in giudizio, per ottenere il risarcimento dei danni effettivi e punitivi previsto dalla legge, il governo degli Stati Uniti in caso di accesso illecito ai dati che lo riguardano; se è appurato che tale accesso illecito è stato intenzionale, si determina automaticamente l'avvio di un'indagine per stabilire se occorra adottare un provvedimento disciplinare nei confronti dell'agente del governo interessato (*cfr.* Codice degli Stati Uniti d'America, titolo 12, articolo 3417).

La legge sulla libertà di informazione (FOIA) consente a chiunque di chiedere l'accesso ai dati esistenti presso gli enti federali su qualsiasi argomento, fatte salve talune categorie di esenzioni [*cfr.* Codice degli Stati Uniti d'America, titolo 5, articolo 552(b)]. Vigono in questo contesto le limitazioni dell'accesso alle informazioni classificate sulla sicurezza nazionale, alle informazioni personali di altre persone e alle informazioni relative a indagini giudiziarie; queste esenzioni sono comparabili alle limitazioni imposte dai diversi paesi tramite la rispettiva legge sull'accesso alle informazioni. Le limitazioni si applicano nello stesso modo sia agli americani sia agli stranieri. Avverso la decisione riguardante l'accesso a documenti richiesto nell'ambito della legge sulla libertà di informazione è possibile un ricorso amministrativo e, quindi, un ricorso dinanzi a un giudice federale. Il giudice è tenuto a stabilire nuovamente se l'accesso ai documenti sia negato legittimamente [Codice degli Stati Uniti d'America, titolo 5, articolo 552(a)(4)(B)] e può obbligare il governo a consentirlo. In alcuni casi il giudice ha ribaltato la decisione con cui il governo aveva negato l'acceso sostenendo che si trattasse di informazioni classificate ([1]). Il risarcimento pecuniario non è possibile, ma il giudice può disporre il rimborso delle spese legali.

VI. CONCLUSIONI

Gli Stati Uniti riconoscono che le attività statunitensi di intelligence dei segnali e altra intelligence devono tenere conto del fatto che ognuno dovrebbe essere trattato con rispetto e dignità, indipendentemente dalla cittadinanza o dal luogo di residenza, e che tutti hanno un legittimo interesse a che le informazioni personali che li riguardano siano trattate nel rispetto della vita privata. Gli Stati Uniti ricorrono all'intelligence dei segnali soltanto per portare avanti i propri interessi di sicurezza nazionale e di politica estera e per proteggere i loro cittadini e quelli degli alleati e partner. La comunità dell'intelligence statunitense non effettua una sorveglianza indiscriminata su nessuno, e quindi neppure sul comune cittadino europeo. La raccolta dati nell'ambito dell'intelligence dei segnali avviene solo se debitamente autorizzata,

([1]) Cfr. *ad esempio, New York Times/Dipartimento della Giustizia*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union/CIA*, 710 F.3d 422 (D.C. Cir. 2014).

secondo modalità rigorosamente conformi alle limitazioni previste, solo dopo aver vagliato la disponibilità di fonti alternative, comprese le fonti pubbliche e diplomatiche, e in un modo che dà priorità alle alternative adeguate e fattibili. Ogniqualvolta possibile, l'intelligence dei segnali si esplica solo, grazie all'uso di discriminanti, in una raccolta dati mirata a un obiettivo o argomento specifico di intelligence esterna.

La politica degli Stati Uniti al riguardo è esposta nella PPD-28. In questo contesto gli enti di intelligence statunitensi non dispongono del potere di legge, delle risorse, della capacità tecnica o del desiderio d'intercettare tutte le comunicazioni del mondo, non leggono i messaggi di posta elettronica di ogni singola persona negli Stati Uniti, e tantomeno di ogni singola persona nel mondo. In linea con la PPD-28, gli Stati Uniti offrono protezioni solide relativamente alle informazioni personali che riguardano cittadini stranieri raccolte attraverso attività di intelligence dei segnali. Per quanto possibile compatibilmente con la sicurezza nazionale, rientrano fra tali protezioni le politiche e procedure atte a minimizzare la conservazione e la divulgazione delle informazioni personali riguardanti i cittadini stranieri, che sono comparabili alle tutele di cui godono i cittadini statunitensi o residenti negli USA. Come esposto in precedenza, il regime di vigilanza globale sul potere mirato di cui all'articolo 702 della FISA è senza precedenti. Infine, le modifiche rilevanti della normativa statunitense sull'intelligence introdotte dalla legge USA FREEDOM e le iniziative guidate dall'ODNI per promuovere la trasparenza all'interno della comunità dell'intelligence migliorano notevolmente la tutela della vita privata e le libertà civili di ciascuno, indipendentemente dalla cittadinanza.

La prego di accogliere, signora Commissaria,
i sensi della mia più alta stima.

Robert S. Litt

21 giugno 2016

Justin S. Antonipillai
Consigliere
Dipartimento del Commercio degli USA
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Vicesegretario aggiunto
Amministrazione del commercio internazionale
1401 Constitution Ave., NW
Washington, DC 20230

Egr. sig. Antonipillai, Egr. sig. Dean,

con la presente intendo fornire ulteriori informazioni sul modo in cui gli Stati Uniti d'America effettuano la raccolta di dati in blocco nell'ambito dell'intelligence dei segnali. Come spiega la nota in calce 5 della direttiva presidenziale 28 (PPD-28), per raccolta in blocco s'intende l'acquisizione di un volume relativamente consistente di informazioni o dati nell'ambito dell'intelligence dei segnali in circostanze in cui la comunità dell'intelligence non può rendere mirata la raccolta ricorrendo a un identificatore associato a un obiettivo specifico (quale ad esempio l'indirizzo di posta elettronica o il numero di telefono dell'obiettivo). Questo non implica tuttavia che si tratti di una raccolta in massa o indiscriminata. La PPD-28 prevede infatti anche che le attività di intelligence dei segnali siano il più possibile mirate. In linea con questa disposizione, la comunità dell'intelligence si attiva per assicurare che, anche quando non si possono usare identificatori specifici per rendere mirata la raccolta, siano rilevati dati che presentano probabilità di contenere informazioni di intelligence esterna conformi alle esigenze dichiarate dai decisori politici statunitensi in base alla procedura illustrata nella precedente lettera, e minimizza il volume delle informazioni irrilevanti raccolte.

La comunità dell'intelligence può, ad esempio, essere chiamata a acquisire nell'ambito dell'intelligence dei segnali dati sulle attività di un gruppo terroristico che opera in una determinata regione di un paese mediorientale e che si ritiene stia progettando attentati contro paesi dell'Europa occidentale, senza tuttavia conoscere nomi, numeri di telefono, indirizzi di posta elettronica o altri identificatori specifici delle persone associate a questo gruppo terroristico. È possibile che si prenda di mira il gruppo raccogliendo dati sulle comunicazioni da e verso tale regione, per poi verificarli e esaminarli ulteriormente al fine di individuare le comunicazioni che interessano il gruppo. La comunità dell'intelligence cercherebbe in questo modo di restringere il più possibile la raccolta. Nell'esempio citato la raccolta sarebbe considerata fatta in blocco perché non è possibile usare discriminanti, ma non si tratta di una raccolta in massa o indiscriminata: è anzi mirata il più precisamente possibile.

Anche quando non è possibile rendere mirata la ricerca con selettori specifici, gli Stati Uniti non raccolgono quindi dati su tutte le comunicazioni provenienti da tutti i dispositivi di comunicazione di tutto il mondo, ma applicano filtri e altri strumenti tecnici per concentrare la raccolta sui dispositivi che presentano probabilità di contenere comunicazioni di valore nell'ambito dell'intelligence esterna. Le attività di intelligence dei segnali condotte dagli Stati Uniti interessano pertanto soltanto una percentuale minima delle comunicazioni che transitano su Internet.

Come già indicato nella lettera precedente, poiché la raccolta di dati in blocco comporta un rischio maggiore di rilevazione di comunicazioni irrilevanti, la PPD-28 limita a sei finalità specifiche l'uso che la comunità dell'intelligence può farne. La PPD-28 e le politiche adottate dagli enti in sua attuazione prevedono limitazioni anche riguardo alla conservazione e divulgazione delle informazioni personali acquisite mediante l'intelligence dei segnali, siano essere rilevate in blocco o tramite una raccolta mirata, a prescindere dalla cittadinanza della persona cui si riferiscono.

Pertanto, la raccolta di dati in blocco effettuata dalla comunità dell'intelligence non si configura come raccolta in massa o indiscriminata, ma implica l'applicazione di metodi e strumenti di filtro che permettono di concentrarla su materiali conformi alle esigenze di intelligence esterna dichiarate dai decisori politici, riducendo nel contempo al minimo la

raccolta di informazioni irrilevanti; al riguardo vigono inoltre norme rigorose a protezione delle eventuali informazioni irrilevanti acquisite. Le politiche e procedure illustrate nella presente lettera si applicano a tutte le raccolte di dati in blocco effettuate nell'ambito dell'intelligence dei segnali, quindi anche per le comunicazioni da e verso l'Europa, senza con questo confermare o negare che siffatta raccolta abbia luogo.

Sono state altresì chieste maggiori informazioni sull'Autorità per la tutela della vita privata e delle libertà civili (PCLOB o «Autorità») e sugli ispettori generali, nonché sui rispettivi poteri. La PCLOB è un ente indipendente dell'esecutivo. I cinque membri dell'Autorità, provenienti dai ranghi di entrambi i partiti, sono nominati dal presidente e confermati dal Senato ([1]). Ciascuno di essi resta in carica per un mandato di sei anni. Sia i membri sia il personale dell'Autorità sono in possesso dell'adeguato nulla osta di sicurezza che permette loro di assolvere pienamente gli obblighi e le responsabilità previsti dalla legge ([2]).

La PCLOB ha il compito di assicurare l'equilibrio tra gli sforzi compiuti dal governo federale per prevenire il terrorismo e la necessità di tutelare la vita privata e le libertà civili. All'Autorità sono conferite due competenze fondamentali: vigilanza e consulenza. La PCLOB stabilisce il proprio programma e decide quali attività di vigilanza o di consulenza intende intraprendere.

Nella funzione di *vigilanza* la PCLOB verifica e analizza gli interventi attuati dall'esecutivo per proteggere il paese dal terrorismo, accertando che vi sia un equilibrio fra la necessità di tali interventi e l'esigenza di tutelare la vita privata e le libertà civili ([3]). L'ultima verifica di vigilanza completata è stata dedicata ai programmi di sorveglianza attuati a norma dell'articolo 702 della FISA ([4]), mentre attualmente è in corso una verifica delle attività di intelligence condotte a norma del decreto presidenziale 12333 ([5]).

Nella sua veste di organo *consultivo* la PCLOB provvede a che l'elaborazione e l'attuazione delle leggi, dei regolamenti e delle politiche riguardanti gli sforzi per proteggere il paese dal terrorismo tengano adeguatamente conto delle considerazioni legate alle libertà ([6]).

Nell'assolvimento dei suoi compiti l'Autorità è autorizzata per legge ad accedere a tutti i pertinenti dati, rapporti, verifiche, controlli, documenti, carte, raccomandazioni e qualsiasi altra documentazione d'interesse dell'ente, comprese le informazioni classificate nei limiti previsti dalla legge ([7]). Può altresì interrogare qualsiasi agente o dipendente dell'esecutivo e raccoglierne le dichiarazioni, nonché assumere testimonianze pubbliche ([8]), e può chiedere per iscritto al Procuratore generale di emanare per suo conto inviti a comparire per obbligare parti estranee all'esecutivo a fornire informazioni d'interesse ([9]).

La legge impone infine alla PCLOB obblighi di trasparenza nei confronti del pubblico, ad esempio tenendolo informato delle attività svolte attraverso audizioni pubbliche e mettendo a disposizione del pubblico le relazioni elaborate, per quanto possibile compatibilmente con la protezione delle informazioni classificate ([10]). La PCLOB è tenuta a segnalare i casi in cui il suo parere è disatteso da un ente dell'esecutivo.

Nella comunità dell'intelligence gli ispettori generali conducono controlli, ispezioni e verifiche sui programmi e attività svolti, per reperire e superare i rischi sistemici, i punti deboli e le carenze. Inoltre, indagano sui reclami o le segnalazioni di presunte violazioni di leggi, norme o regolamenti oppure di cattiva gestione, sullo spreco palese di fondi, sull'abuso di

([1]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(a), (h).
([2]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(k).
([3]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(d)(2).
([4]) Cfr. *in generale* https://www.pclob.gov/library.html#oversightreports.
([5]) Cfr. *in generale* https://www.pclob.gov/events/2015/may13.html.
([6]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(d)(1). cfr. *anche* PCLOB Advisory Function Policy and Procedure, Policy 2015-004, *consultabile all'indirizzo* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(g)(1)(A).
([8]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(g)(1)(B).
([9]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee(g)(1)(D).
([10]) Codice degli Stati Uniti d'America, titolo 42, articolo 2000eee(f).

potere o ancora su un pericolo rilevante e specifico per la salute e la sicurezza pubbliche derivante dai programmi e attività della comunità dell'intelligence. L'indipendenza è un elemento fondamentale per l'obiettività e l'integrità di ogni relazione, constatazione e raccomandazione emessa dall'ispettore generale. Gli elementi più importanti per il mantenimento di quest'indipendenza comprendono il processo di nomina e di destituzione dell'ispettore generale, la separazione tra i poteri operativi, finanziari e amministrativi sul personale e il duplice obbligo di riferire sia ai capi degli enti dell'esecutivo sia al Congresso.

Il Congresso ha istituito un Ufficio dell'ispettore generale indipendente in ciascun ente dell'esecutivo, compresi tutti i servizi della comunità dell'intelligence ([1]). Con l'approvazione della legge autorizzativa dell'intelligence per l'esercizio finanziario 2015, quasi tutti gli ispettori generali che esercitano la vigilanza su un servizio della comunità dell'intelligence sono nominati dal presidente e confermati dal Senato, compreso al Dipartimento della Giustizia, alla *Central Intelligence Agency*, all'Agenzia per la sicurezza nazionale e nella comunità dell'intelligence ([2]). Gli ispettori generali sono funzionari apolitici assunti a tempo indeterminato, che solo il presidente può rimuovere dall'incarico. Sebbene questa facoltà sia prevista dalla Costituzione degli Stati Uniti, il presidente l'ha esercitata raramente; essa gli impone altresì di trasmettere al Congresso una motivazione scritta 30 giorni prima di rimuovere dall'incarico l'ispettore generale ([3]). La procedura stabilita assicura che gli esponenti dell'esecutivo non esercitino alcuna influenza indebita sulla scelta, nomina e destituzione degli ispettori generali.

La legge conferisce agli ispettori generali poteri rilevanti per lo svolgimento di controlli, indagini e verifiche dei programmi e operazioni dell'esecutivo. Oltre alle indagini e verifiche di vigilanza disposte dalla legge, gli ispettori generali godono di ampia discrezionalità circa il potere di verifica, potendo scegliere i programmi e le attività su cui esercitarlo ([4]). A norma della legge, nell'esercizio di tale potere gli ispettori generali dispongono di risorse autonome che permettono loro di esercitare le relative responsabilità, compresa la facoltà di assumere personale proprio e di documentare separatamente le richieste di finanziamenti presentate al Congresso ([5]). La legge assicura agli ispettori generali l'accesso alle informazioni necessarie per assolvere le loro responsabilità. Rientrano in quest'aspetto il potere di accedere direttamente a tutti i dati e informazioni relativi ai programmi e alle operazioni dell'ente, indipendentemente dalla loro classificazione, il potere di ordinare la presentazione di informazioni e documenti e il potere di sottoporre a giuramento ([6]). In un numero limitato di casi, il capo dell'ente dell'esecutivo può vietare una data attività dell'ispettore generale se, ad esempio, una sua verifica o indagine potrebbe compromettere seriamente gli interessi di sicurezza nazionale degli Stati Uniti d'America. Anche in questo caso, tale potere è esercitato molto di rado e implica che il capo dell'ente ne comunichi al Congresso il motivo nell'arco di 30 giorni ([7]). Di fatto il Direttore dell'intelligence nazionale non ha mai esercitato questo potere di limitazione su nessuna attività degli ispettori generali.

Gli ispettori generali hanno inoltre la responsabilità di tenere perfettamente informati e aggiornati i capi degli enti dell'esecutivo e il Congresso, segnalando loro i casi di frode e gli altri problemi gravi, gli abusi e le carenze inerenti ai programmi e attività dell'esecutivo ([8]). Questa doppia linea di riferimento rafforza l'indipendenza degli ispettori generali assicurando la trasparenza del processo di vigilanza e offrendo ai capi degli enti l'occasione di attuare le raccomandazioni formulate dall'ispettore generale prima che il Congresso possa intervenire per via legislativa. Ad esempio, gli ispettori generali sono tenuti per legge a compilare relazioni semestrali che illustrino tali problemi e le misure correttive adottate fino a quel momento ([9]). Gli enti dell'esecutivo prendono sul serio le constatazioni e raccomandazioni degli ispettori

([1]) Articoli 2 e 4 della legge sugli ispettori generali del 1978 e successive modifiche («legge IG»); articolo 103H(b) e (e) della legge sulla sicurezza nazionale del 1947 e successive modifiche («legge SN»); articolo 17 (a) della legge sulla CIA («legge CIA»).

([2]) Cfr. Pub. L. n. 113-293, 128 Stat. 3990 (19 dicembre 2014). Gli ispettori generali dell'Agenzia di intelligence della difesa e dell'Agenzia nazionale d'intelligence geospaziale sono gli unici non nominati dal presidente, ma l'ispettore generale del Dipartimento della Difesa e l'omologo della comunità dell'intelligence hanno competenza concorrente su tali agenzie.

([3]) Articolo 3 della legge IG del 1978 e successive modifiche; articolo 103H(c) della legge SN e articolo 17(b) della legge CIA.

([4]) Cfr. articoli 4(a) e 6(a)(2) della legge IG del 1947; articolo 103H(e) e (g)(2)(A) della legge SN; articolo 17(a) e (c) della legge CIA.

([5]) Articoli 3(d), 6(a)(7) e 6(f) della legge IG; articolo 103H(d), (i), (j) e (m) della legge SN; articolo 17(e)(7) e (f) della legge CIA.

([6]) Articolo 6(a)(1), (3), (4), (5), e (6) della legge IG; articolo 103H(g)(2) delle legge SN; articolo 17(e)(1), (2), (4), e (5) della legge CIA.

([7]) Cfr., *ad esempio*, articoli 8(b) e 8E(a) della legge IG; articolo 103H(f) della legge SN; articolo 17(b) della legge CIA.

([8]) Articolo 4(a)(5) della legge IG; articolo 103H(a)(b)(3) e (4) della legge SN; articolo 17(a)(2) e (4) della legge CIA.

([9]) Articoli 2(3), 4(a), e 5 della legge IG; articolo 103H(k) della legge SN; articolo 17(d) della legge CIA. L'ispettore generale del Dipartimento della Giustizia mette a disposizione su Internet le relazioni pubblicate, all'indirizzo http://oig.justice.gov/reports/all.htm. Anche l'ispettore generale della comunità dell'intelligence mette a disposizione del pubblico le relazioni semestrali, all'indirizzo https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

generali e spesso riescono a indicare il fatto di averne accettato e attuato le raccomandazioni in queste e in altre relazioni presentate al Congresso e, in alcuni casi, al pubblico ([1]). Oltre a questa duplice linea di riferimento, gli ispettori generali sono responsabili anche di indirizzare verso le opportune commissioni di vigilanza del Congresso i segnalanti appartenenti all'esecutivo che intendono rivelare casi di presunta frode, spreco o abuso nei programmi e attività dell'esecutivo. L'identità del segnalante è protetta dalla divulgazione all'esecutivo, il che lo mette al riparo da potenziali ritorsioni proibite, in termini di gestione del personale o dei nulla osta di sicurezza, adottate nei suoi confronti per aver segnalato il problema all'ispettore generale ([2]). Poiché spesso le indagini dell'ispettore generale prendono le mosse dalle rivelazioni di un segnalante, la capacità di trasmetterne i dubbi al Congresso senza ingerenze dell'esecutivo migliora l'efficacia della vigilanza esercitata. Grazie alla loro indipendenza, gli ispettori generali possono promuovere, con obiettività e integrità, l'economia, l'efficienza e l'assunzione di responsabilità all'interno degli enti dell'esecutivo.

Infine, il Congresso ha istituito il Consiglio degli ispettori generali per l'integrità e l'efficienza, il quale si occupa, tra l'altro, di mettere a punto le norme per la condotta dei controlli, delle indagini e delle verifiche e di promuovere la formazione; ha inoltre il potere di riesaminare le accuse di condotta irregolare di un ispettore generale, ossia di portare uno sguardo critico sulla persona che, per la funzione esercitata, controlla tutti gli altri ([3]).

Nell'auspicare che queste informazioni risultino utili, vi prego di accogliere i sensi della mia più alta stima

Robert S. Litt
Giureconsulto

([1]) Articoli 2(3), 4(a), e 5 della legge IG; articolo 103H(k) della legge SN; articolo 17(d) della legge CIA. L'ispettore generale del Dipartimento della Giustizia mette a disposizione su Internet le relazioni pubblicate, all'indirizzo http://oig.justice.gov/reports/all.htm. Anche l'ispettore generale della comunità dell'intelligence mette a disposizione del pubblico le relazioni semestrali, all'indirizzo https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Articolo 7 della legge IG; articolo 103H(g)(3) della legge SN; articolo 17(e)(3) della legge CIA.

([3]) Articolo 11 della legge IG.

ALLEGATO VII

Lettera del Viceprocuratore generale aggiunto e Consigliere per gli affari internazionali Bruce Swartz, Dipartimento della Giustizia degli USA

19 febbraio 2016

Justin S. Antonipillai
Consigliere
Dipartimento del Commercio degli USA
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Vicesegretario aggiunto
Amministrazione del commercio internazionale
1401 Constitution Ave., NW
Washington, DC 20230

Egr. sig. Antonipillai, Egr. sig. Dean,

segue una breve panoramica dei principali strumenti investigativi usati negli USA per ottenere dalle imprese dati commerciali e altre informazioni a fini di applicazione della normativa penale o per scopi (civili e regolamentari) d'interesse pubblico, corredata delle limitazioni di accesso che si applicano ai relativi poteri ([1]). Le procedure giuridiche previste a tali fini non sono discriminatorie: sono infatti seguite per ottenere informazioni dalle imprese presenti negli USA, comprese quelle che si autocertificano nell'ambito dello scudi UE-USA per la privacy, a prescindere dalla cittadinanza dell'interessato. Inoltre, l'impresa sottoposta a siffatta procedura negli Stati Uniti può contestarla in sede giudiziaria nelle modalità indicate qui di seguito ([2]).

Relativamente al sequestro di dati da parte delle autorità pubbliche, si rilevi in particolare il quarto emendamento della Costituzione degli Stati Uniti, in virtù del quale il diritto dei cittadini a godere della sicurezza per quanto riguarda la loro persona, la loro casa, le loro carte e le loro cose, contro perquisizioni e sequestri ingiustificati, non può essere violato; e nessun mandato giudiziario può essere emesso, se non in base a fondate supposizioni, appoggiate da un giuramento o da una dichiarazione sull'onore e con descrizione specifica del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare (Costituzione degli Stati Uniti d'America, quarto emendamento). Nella sentenza *Berger/Stato di New York* la Corte suprema degli Stati Uniti ha ribadito, come in innumerevoli decisioni precedenti, che lo scopo fondamentale del quarto emendamento è tutelare la privacy e la sicurezza delle persone contro le ingerenze arbitrarie di agenti del governo (388 U.S. 41, 53 (1967) (*in riferimento a Camara/Tribunale municipale di San Francisco*, 387 U.S. 523, 528 (1967)]. Nelle indagini penali nazionali, il quarto emendamento implica in genere che, prima di effettuare una perquisizione, gli agenti delle autorità di applicazione della legge devono ottenere un mandato dal giudice (*cfr. Katz/Stati Uniti d'America*, 389 U.S. 347, 357 (1967)]. Se non vale l'obbligo del mandato, l'attività del governo è testata a fronte del quarto emendamento per stabilire se sia «ragionevole». È quindi la stessa Costituzione a garantire che il governo degli Stati Uniti non disponga di un potere illimitato o arbitrario di sequestro delle informazioni private.

Autorità di contrasto penali

Nell'ambito di un'indagine penale, i procuratori federali, che dipendono dal Dipartimento della Giustizia, e gli inquirenti federali, compresi gli agenti del *Federal Bureau of Investigation* (FBI), autorità di contrasto inquadrata nel Dipartimento della Giustizia, hanno facoltà di obbligare le imprese presenti negli USA a comunicare documenti e altre informazioni;

([1]) La panoramica non descrive gli strumenti investigativi usati dalle autorità di contrasto nell'ambito delle indagini sul terrorismo e su altre questioni legate alla sicurezza nazionale, tra cui le *National Security Letter* per determinate informazioni contenute in rapporti di credito, documenti finanziari e archivi elettronici di abbonati e di dati transazionali (*cfr.* Codice degli Stati Uniti d'America, titolo 12, articolo 3414, titolo 15, articolo 1681u, titolo 15, articolo 1681v, titolo 18, articolo 2709), e, per la sorveglianza elettronica, i mandati di perquisizione, i documenti aziendali e la raccolta di altre comunicazioni a norma della legge relativa alla vigilanza sull'intelligence esterna (*cfr.* Codice degli Stati Uniti d'America, titolo 50, articoli 1801 e ss.).

([2]) Il presente documento verte sui poteri di applicazione della legge e di regolamentazione a livello federale: se la violazione riguarda la legge di uno Stato della federazione, le indagini sono effettuate da tale Stato e il procedimento giudiziario avviene dinanzi ai giudici di tale Stato. Le autorità di applicazione della legge degli Stati federati usano i mandati e le citazioni sostanzialmente nello stesso modo descritto nel presente documento, con la differenza tuttavia che la Costituzione dello Stato può prevedere per la procedura giuridica tutele superiori a quelle stabilite dalla Costituzione degli Stati Uniti. Le tutele previste dalla legge dello Stato federato devono essere almeno equivalenti a quelle della Costituzione degli Stati Uniti, compreso, ma non solo, il quarto emendamento.

possono al riguardo attivare varie procedure giuridiche obbligatorie, tra cui citazioni dinanzi al *grand jury*, citazioni amministrative e mandati di perquisizione, e possono acquisire altre comunicazioni in virtù dei poteri di intercettazione delle comunicazioni e dei dati informativi conferiti per le indagini penali federali.

Citazioni dinanzi al *grand jury* o in giudizio — In materia penale si ricorre alle citazioni come supporto di un'indagine di polizia mirata. La citazione dinanzi al *grand jury* è la richiesta ufficiale emessa dallo stesso (di solito su richiesta del procuratore federale) a supporto di un'indagine condotta in tale sede su una sospetta violazione specifica della normativa penale. Il *grand jury* è il ramo investigativo di un tribunale, formato da giurati scelti da un magistrato o giudice. La citazione può imporre alla persona di testimoniare in un procedimento o di comunicare o mettere a disposizione documenti aziendali, informazioni conservate su supporto elettronico o altri beni materiali. Le informazioni devono essere pertinenti all'indagine e la citazione non può essere irragionevole, vale a dire che non può essere eccessivamente ampia né vessatoria o eccessivamente gravosa: il destinatario della citazione può peraltro contestarla adducendo uno di questi motivi (*cfr.* Fed. R. Crim. P. 17). In determinate situazioni limitate, dopo che al *grand jury* il caso è sfociato in un'accusa formale è possibile ricorrere a una citazione in giudizio per ottenere documenti.

Potere di emissione di citazioni amministrative — Il potere di emettere citazioni amministrative è esercitabile nelle indagini sia penali sia civili. In materia penale, varie leggi federali autorizzano il ricorso alle citazioni amministrative per ottenere la comunicazione o la disponibilità di documenti aziendali, informazioni conservate su supporto elettronico o altri beni materiali nelle indagini riguardanti le frodi mediche, gli abusi su minori, la protezione dei servizi segreti e nei casi che implicano sostanze controllate, così come nelle indagini degli ispettori generali che interessano enti governativi. Se il governo intende far valere la citazione amministrativa in giudizio, il destinatario di tale citazione può, al pari del destinatario della citazione dinanzi al *grand jury*, contestarla in quanto irragionevole, vale a dire eccessivamente ampia o vessatoria o eccessivamente gravosa.

Provvedimenti giudiziari relativi ai dispositivi d'intercettazione dei dati informativi della comunicazione in entrata e in uscita — A norma delle disposizioni che disciplinano i dispositivi d'intercettazione dei dati informativi della comunicazione in entrata e in uscita, l'autorità di contrasto può ottenere dal giudice, certificando che le informazioni sono d'interesse per un'indagine penale in corso, un provvedimento che le permette di acquisire in tempo reale informazioni non di contenuto su un dato numero di telefono o indirizzo di posta elettronica (numero composto, instradamento della comunicazione, destinatario e segnale) (*cfr.* Codice degli Stati Uniti d'America, titolo 18, articoli 3121-3127). L'impiego o l'installazione di un tale dispositivo al di fuori della legge costituisce un reato federale.

Legge sulla privacy nelle comunicazioni elettroniche — L'accesso del governo alle informazioni sugli abbonati, ai dati di traffico e all'archivio dei contenuti delle comunicazioni in possesso delle società telefoniche che forniscono servizi Internet e di altri terzi fornitori di servizi è disciplinato da ulteriori norme adottate ai sensi del titolo II della legge sulla privacy nelle comunicazioni elettroniche, ossia dalla legge sulle comunicazioni archiviate (SCA) (Codice degli Stati Uniti d'America, titolo 18, articoli 2701–2712). Nel sistema di diritti alla privacy previsti per legge instaurato dalla SCA, la facoltà delle autorità di contrasto di accedere ai dati è limitata, fermi restando gli obblighi che la legge costituzionale impone al cliente o all'abbonato al fornitore di servizi Internet. La SCA prevede livelli crescenti di tutela della privacy in funzione dell'intrusività della raccolta dati: per le informazioni relative alla registrazione dell'abbonato, gli indirizzi IP e relative indicazioni temporali e i dati di fatturazione, le autorità di applicazione della legge in materia penale devono ottenere un'ingiunzione; per la maggior parte delle altre informazioni non di contenuto archiviate, come le intestazioni dei messaggi di posta elettronica senza indicazione dell'oggetto, le autorità di contrasto devono esporre al giudice fatti precisi per dimostrargli che le informazioni richieste sono pertinenti e rilevanti per un'indagine penale in corso. Per acquisire il contenuto archiviato delle comunicazioni elettroniche, le autorità di applicazione della legge in materia penale ottengono in genere un mandato del giudice, fondato su motivi plausibili per ritenere che l'*account* contenga prove di un reato. La SCA prevede inoltre la responsabilità civile e sanzioni penali.

Ordini giudiziari che dispongono la sorveglianza a norma della legge federale sull'intercettazione delle comunicazioni — A norma della legge federale sull'intercettazione delle comunicazioni, le autorità di contrasto possono intercettare in tempo reale le comunicazioni orali, via cavo o elettroniche (*cfr.* Codice degli Stati Uniti d'America, titolo 18, articoli 2510-2522). L'esercizio di questo potere presuppone un ordine giudiziario in cui il giudice riscontra, fra l'altro,

l'esistenza di motivi plausibili per ritenere che l'intercettazione via cavo o elettronica fornirà la prova di un reato federale o del luogo in cui si trova un latitante. La legge prevede la responsabilità civile e sanzioni penali in caso di violazione delle disposizioni sull'intercettazione delle comunicazioni.

Mandato di perquisizione — articolo 41 — Negli Stati Uniti i servizi di contrasto possono effettuare fisicamente perquisizioni di locali solo se autorizzati dal giudice. Questo implica dimostrare al giudice, adducendo «motivi plausibili», che un reato è stato commesso o sta per essere commesso e che è probabile rinvenire elementi connessi al reato nel luogo indicato nel mandato. Si ricorre spesso a questo potere quando, una volta notificata all'impresa una citazione o altra ingiunzione di presentare documenti, è necessaria una perquisizione fisica dei suoi locali per scongiurare il rischio di distruzione delle prove *cfr.* quarto emendamento della Costituzione degli Stati Uniti (illustrato in dettaglio supra), Fed. R. Crim. P. 41). Il destinatario può cercare di ottenerne l'annullamento del mandato di perquisizione in quanto eccessivamente ampio, vessatorio o altrimenti emesso indebitamente e le parti lese legittimate ad agire possono chiedere la soppressione di tutte le prove acquisite con una perquisizione illegale (*cfr. Mapp/Ohio*, 367 U.S. 643 (1961)].

Orientamenti e politiche del Dipartimento della Giustizia — Oltre alle citate limitazioni basate sulla Costituzione, sulla legge e sui regolamenti, l'accesso del governo ai dati per scopi di applicazione della legge è limitato ulteriormente dagli orientamenti emanati dal Procuratore generale, che prevedono anche tutele in materia di privacy e di libertà civili. Ad esempio, gli orientamenti del Procuratore generale per le operazioni del *Federal Bureau of Investigation* (FBI) all'interno degli USA (settembre 2008) («orientamenti» o «orientamenti AG FBI»), consultabili all'indirizzo http://www.justice.gov/archive/opa/docs/guidelines.pdf, limitano l'uso di metodi investigativi per ottenere informazioni collegate a indagini su reati federali. Impongono infatti all'FBI di applicare metodi di indagine meno intrusivi possibile, tenendo conto dell'effetto sulla vita privata e sulle libertà civili e del potenziale danno alla reputazione. Parafrasando gli orientamenti, va da sé che l'FBI deve condurre le indagini e le altre attività con modalità lecite e proporzionate nel rispetto delle libertà e della privacy, e evitare qualsiasi intrusione superflua nella vita delle persone rispettose della legge (*cfr.* orientamenti AG FBI, 5). L'FBI ha dato attuazione agli orientamenti con la Guida alle indagini e operazioni dell'FBI all'interno degli USA (consultabile all'indirizzo https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)], manuale completo in cui sono indicati i limiti specifici applicabili all'uso degli strumenti d'indagine e gli orientamenti cui attenersi per proteggere le libertà civili e la privacy in ogni indagine. Il manuale per i procuratori degli Stati Uniti (**United States Attorneys' Manual** — USAM), anch'esso disponibile in rete all'indirizzo http://www.justice.gov/usam/united-states-attorneys-manual, prevede ulteriori norme e politiche che limitano le attività investigative dei procuratori federali.

Poteri civili e regolamentari (interesse pubblico)

Riguardo all'accesso ai dati detenuti da imprese presenti negli Stati Uniti vigono limitazioni rilevanti anche sotto il profilo civile o regolamentare (ossia di «interesse pubblico»). Gli enti che hanno competenze civili o di regolamentazione possono citare le imprese ingiungendo loro di trasmettere documenti aziendali, informazioni conservate su supporto elettronico o altri beni materiali. L'esercizio di questo potere di citazione amministrativa o civile è limitato non solo dalla legge costitutiva dell'ente, ma anche dal sindacato giurisdizionale indipendente delle citazioni precedente alla potenziale esecuzione per via giudiziaria (*cfr., ad esempio,* Fed. R. Civ. P. 45). L'ente può chiedere l'accesso soltanto ai dati d'interesse per la materia rientrante nella sua competenza di regolamentazione. Il destinatario della citazione amministrativa può contestarne l'esecuzione in sede giudiziaria, presentando prove del fatto che l'ente non ha agito secondo i criteri minimi di accesso «ragionevole» illustrati in precedenza.

Secondo il settore specifico in cui opera e la tipologia di dati che detiene, l'impresa può addurre altre basi giuridiche per contestare la richiesta di dati presentata dall'ente amministrativo. Un istituto finanziario, ad esempio, può contestare la citazione amministrativa che gli ingiunge di comunicare determinati tipi di informazioni adducendo che, presentandole, violerebbe la legge sul segreto bancario e i relativi regolamenti di esecuzione (*cfr.* Codice degli Stati Uniti d'America, titolo 31, articolo 5318; Codice dei regolamenti federali, titolo 31, parte X), mentre un'altra società può invocare la legge sull'informativa corretta nel credito (*cfr.* Codice degli Stati Uniti d'America, titolo 15, articolo 1681b) o una delle molte altre leggi settoriali. L'abuso del potere di inviare citazioni può implicare la responsabilità dell'ente o la responsabilità personale dei suoi agenti (*cfr., ad esempio,* legge sul diritto alla privacy finanziaria, Codice degli Stati Uniti d'America, titolo 12, articoli 3401–3422). Negli Stati Uniti i giudici svolgono quindi il ruolo di custodi per bloccare le richieste indebite degli enti di regolamentazione e supervisionano in indipendenza l'operato degli enti federali.

Infine, il potere conferito dalla legge a un'autorità amministrativa di sequestrare fisicamente i dati a un'impresa presente negli USA nel quadro di una perquisizione amministrativa deve soddisfare le condizioni del quarto emendamento (*cfr. See/Città di Seattle*, 387 U.S. 541 (1967)].

Conclusioni

Negli Stati Uniti d'America tutte le attività di contrasto e di regolamentazione devono essere conformi alla normativa applicabile: Costituzione degli Stati Uniti, leggi, norme e regolamenti. Devono inoltre essere conformi alle politiche applicabili, compresi gli orientamenti del Procuratore generale che disciplinano le attività di applicazione della legge a livello federale. Il quadro giuridico illustrato limita le autorità statunitensi di applicazione della legge e di regolamentazione nella loro capacità di acquisire informazioni dalle imprese presenti negli Stati Uniti, a prescindere dal fatto che le informazioni riguardino cittadini statunitensi o residenti negli USA oppure cittadini stranieri; permette altresì di sottoporre a sindacato giurisdizionale qualsiasi richiesta di accesso ai dati avanzata dal governo in virtù di questi poteri.

La prego di accogliere, signora Commissaria, i sensi della mia più alta stima.

Bruce C. Swartz

Viceprocuratore generale aggiunto e Consigliere per gli affari internazionali