DECISIONE DI ESECUZIONE (UE) 2023/1795 DELLA COMMISSIONE

del 10 luglio 2023

a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali

[notificata con il numero C(2023)4745]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il 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) ([1]), in particolare l'articolo 45, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

(1) Il regolamento (UE) 2016/679 ([2]) (in appresso "GDPR") stabilisce le norme per il trasferimento di dati personali da titolari del trattamento o responsabili del trattamento nell'Unione verso paesi terzi e organizzazioni internazionali nella misura in cui tale trasferimento rientri nel suo ambito di applicazione. Le norme in materia di trasferimenti internazionali di dati sono stabilite nel capo V di tale regolamento. Sebbene la circolazione di dati personali verso e da paesi al di fuori dell'Unione europea sia essenziale per l'espansione degli scambi transfrontalieri e della cooperazione internazionale, occorre garantire che il livello di protezione offerto ai dati personali nell'Unione europea non sia compromesso da trasferimenti verso paesi terzi od organizzazioni internazionali ([3]).

(2) Ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 la Commissione può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo garantiscono un livello di protezione adeguato. Nel rispetto di tale condizione, i trasferimenti di dati personali verso un paese terzo possono avvenire senza la necessità di ottenere ulteriori autorizzazioni, come previsto dall'articolo 45, paragrafo 1, e dal considerando 103 di tale regolamento.

(3) Come specificato all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679, l'adozione della decisione di adeguatezza deve basarsi su un'analisi completa dell'ordinamento giuridico del paese terzo, per quanto riguarda tanto le norme applicabili agli importatori di dati quanto le limitazioni e le garanzie relative all'accesso ai dati personali da parte delle autorità pubbliche. Nella propria valutazione la Commissione deve stabilire se il paese terzo in questione assicura un livello di protezione "sostanzialmente equivalente" a quello garantito all'interno dell'Unione (considerando 104 del regolamento (UE) 2016/679). Tale determinazione deve essere valutata facendo riferimento alla legislazione dell'UE, in particolare al regolamento (UE) 2016/679, nonché alla giurisprudenza della Corte di giustizia dell'Unione europea (Corte di giustizia) ([4]).

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) Per comodità di riferimento, un elenco delle abbreviazioni utilizzate nella presente decisione figura nell'allegato VIII.
([3]) Cfr. considerando 101 del regolamento (UE) 2016/679.
([4]) Cfr., più di recente, la sentenza della Corte di giustizia del 16 luglio 2020, *Facebook Ireland e Schrems* (*Schrems II*), C-311/18, ECLI:EU:C:2020:559.

(4) Come chiarito dalla Corte di giustizia nella sua sentenza del 6 ottobre 2015 nella causa *Maximillian Schrems/Data Protection Commissioner* ([5]) *(Schrems)*, C-362/14 ciò non richiede la constatazione dell'esistenza di un livello di protezione identico. In particolare gli strumenti dei quali il paese terzo in questione si avvale per proteggere i dati personali possono essere diversi da quelli attuati all'interno dell'Unione, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello di protezione adeguato ([6]). Il livello di adeguatezza non comporta pertanto una duplicazione pedissequa delle norme dell'Unione. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero, nel suo insieme, offre il necessario livello di protezione ([7]). Inoltre, secondo tale sentenza, nell'applicare tale norma, la Commissione dovrebbe valutare in particolare se il quadro giuridico del paese terzo in questione preveda norme destinate a limitare le ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione, che le entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come sicurezza nazionale, e fornisca una tutela giuridica efficace nei confronti delle ingerenze di tale natura ([8]). Anche i "criteri di riferimento per l'adeguatezza" del comitato europeo per la protezione dei dati, che cercano di chiarire ulteriormente tale livello, forniscono indicazioni al riguardo ([9]).

(5) Il livello applicabile in relazione a tale ingerenza nei diritti fondamentali alla tutela della vita privata e alla protezione dei dati è stato ulteriormente chiarito dalla Corte di giustizia nella sua sentenza del 16 luglio 2020 nella causa *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems (Schrems II)*, C-311/18, che ha annullato la decisione di esecuzione (UE) 2016/1250 ([10]) della Commissione relativa a un precedente quadro transatlantico per il flusso di dati, lo scudo UE-USA per la privacy (scudo per la privacy). La Corte di giustizia ha ritenuto che le limitazioni alla protezione dei dati personali, che derivano dalla normativa interna degli Stati Uniti d'America ("Stati Uniti") in materia di accesso e utilizzo, da parte delle autorità pubbliche statunitensi, di dati trasferiti dall'Unione verso gli Stati Uniti per finalità di sicurezza nazionale non fossero inquadrate in modo da corrispondere a requisiti sostanzialmente equivalenti a quelli richiesti dal diritto dell'Unione, per quanto concerne la necessità e la proporzionalità di tali ingerenze rispetto al diritto alla protezione dei dati ([11]). La Corte di giustizia ha ritenuto altresì che non fossero disponibili mezzi di ricorso dinanzi a un organo che offra alle persone i cui dati sono trasferiti verso gli Stati Uniti garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta concernente il diritto ad un ricorso effettivo ([12]).

(6) A seguito della sentenza *Schrems II*, la Commissione ha avviato colloqui con il governo degli Stati Uniti in vista di un'eventuale nuova decisione di adeguatezza che soddisfi i requisiti di cui all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679, come interpretato dalla Corte di giustizia. A seguito di tali discussioni, il 7 ottobre 2022 gli Stati Uniti hanno adottato l'*Executive Order* (decreto presidenziale) 14086 "Enhancing Safeguards for US Signals Intelligence Activities" (decreto presidenziale 14086), integrato da un regolamento sul "Data Protection Review Court" (DPRC, tribunale del riesame in materia di protezione dei dati) emesso dal Procuratore generale degli Stati Uniti (regolamento del Procuratore generale) ([13]). Inoltre, è stato aggiornato il quadro che si applica ai soggetti commerciali che trattano dati trasferiti dall'Unione ai sensi della presente decisione, il "quadro UE-USA per la protezione dei dati personali" (DPF UE-USA o DPF, dall'inglese: *Data Privacy Framework*).

(7) La Commissione ha analizzato con attenzione le leggi e pratiche applicate negli Stati Uniti, compresi il decreto presidenziale 14086 e il regolamento del Procuratore generale. In base alle constatazioni illustrate nei considerando da 9 a 200, la Commissione giunge alla conclusione che gli Stati Uniti assicurano un livello di protezione adeguato dei dati personali trasferiti nell'ambito del DPF UE-USA da un titolare o responsabile del trattamento nell'Unione ([14]) alle organizzazioni statunitensi che si sono certificate come aderenti al regime.

([5]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Schrems/Data Protection Commissioner* (*Schrems*), C-362/14, ECLI:EU:C:2015:650, punto 73.

([6]) *Schrems*, punto 74.

([7]) Cfr. comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato (COM(2017) 7 final del 10.1.2017), sezione 3.1, pag. 7.

([8]) *Schrems*, punti 88 e 89.

([9]) Comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, disponibile al seguente indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 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 (GU L 207 dell'1.8.2016, pag. 1).

([11]) *Schrems II*, punto 185.

([12]) *Schrems II*, punto 197.

([13]) Codice dei regolamenti federali, titolo 28, parte 302.

([14]) 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 decisione che ha integrato il regolamento (UE) 2016/679 nell'allegato XI dell'accordo SEE è stata adottata dal comitato misto SEE il 6 luglio 2018 ed è entrata in vigore il 20 luglio 2018. Il regolamento rientra pertanto nell'ambito di applicazione dell'accordo. Ai fini della decisione, i riferimenti all'UE e agli Stati membri dell'UE dovrebbero quindi essere intesi anche come riferimenti agli Stati del SEE.

(8) Per effetto della presente decisione i trasferimenti di dati personali da titolari e responsabili del trattamento nell'Unione ([15]) verso organizzazioni certificate negli Stati Uniti possono aver luogo senza la necessità di ottenere ulteriori autorizzazioni. La presente decisione non incide sull'applicazione diretta del regolamento (UE) 2016/679 a tali organizzazioni qualora siano soddisfatte le condizioni relative all'ambito di applicazione territoriale di detto regolamento, di cui all'articolo 3 dello stesso.

2. IL QUADRO UE-USA PER LA PROTEZIONE DEI DATI PERSONALI

2.1 Ambito di applicazione soggettivo e materiale

2.1.1 *Organizzazioni certificate*

(9) Il DPF UE-USA si fonda su un sistema di certificazione in base al quale un'organizzazione statunitense si impegna a rispettare un insieme di principi in materia di protezione dei dati, ossia i "principi del DPF UE-USA", comprensivi dei principi supplementari (collettivamente i "principi"), emanati dal Dipartimento del Commercio degli USA e riportati nell'allegato I della presente decisione ([16]). Per essere ammissibile alla certificazione nel quadro del DPF UE-USA, un'organizzazione deve assoggettarsi ai poteri di indagine e di esecuzione della Commissione federale per il commercio (FTC) o del Dipartimento dei Trasporti (DOT) degli Stati Uniti ([17]). I principi si applicano immediatamente alla data di certificazione. Come spiegato più dettagliatamente nei considerando da 48 a 52, le organizzazioni del DPF UE-USA sono tenute a certificare nuovamente la loro adesione ai principi su base annuale ([18]).

2.1.2 *Definizione di dati personali e concetti di titolare del trattamento e "procuratore"*

(10) La protezione garantita dal DPF UE-USA si applica a tutti i dati personali trasferiti dall'Unione a organizzazioni negli Stati Uniti che hanno certificato la loro adesione ai principi presso il Dipartimento del Commercio, fatta eccezione per i dati raccolti per la pubblicazione, la trasmissione o altre forme di comunicazione pubblica di materiale giornalistico e di informazioni contenute in materiale già pubblicato e divulgato da archivi di mezzi di informazione ([19]). Tali informazioni non possono pertanto essere trasferite sulla base del DPF UE-USA.

(11) I principi definiscono i dati personali/le informazioni personali nello stesso modo del regolamento (UE) 2016/679 (GDPR), ossia come "i dati e le informazioni riguardanti singoli individui (identificati o identificabili) cui si applica il GDPR, che un'organizzazione presente negli Stati Uniti riceve dall'Unione europea e registrata in qualsiasi forma" ([20]). Di conseguenza tali dati e informazioni riguardano anche i dati di ricerca pseudonimizzati (o "codificati") (anche quando la chiave di codifica non è condivisa con l'organizzazione statunitense che riceve tali dati e informazioni) ([21]). Analogamente la nozione di "trattamento" è definita come "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" ([22]).

(12) Il DPF UE-USA si applica alle organizzazioni statunitensi che si qualificano come titolari del trattamento (ossia una persona o un'organizzazione che, da sola o congiuntamente ad altre, stabilisce le finalità e i mezzi del trattamento di dati personali) ([23]) o responsabili del trattamento (ossia procuratori che agiscono per conto di un titolare del trattamento) ([24]). I responsabili del trattamento statunitensi devono essere vincolati contrattualmente ad agire

([15]) La presente decisione lascia impregiudicati i requisiti del regolamento (UE) 2016/679 che si applicano ai soggetti (titolari e responsabili del trattamento) aventi sede nell'Unione che trasferiscono i dati in questione, ad esempio per quanto concerne la limitazione della finalità, la minimizzazione dei dati, la trasparenza e la sicurezza dei dati (cfr. anche l'articolo 44 del regolamento (UE) 2016/679).

([16]) Cfr. al riguardo la sentenza *Schrems*, punto 81, nel contesto della quale la Corte di giustizia ha confermato che un sistema di autocertificazione può garantire un livello di protezione adeguato.

([17]) Allegato I, parte I, punto 2. All'FTC è riconosciuta un'ampia giurisdizione sulle attività commerciali, con alcune eccezioni, ad esempio per quanto concerne le banche, le compagnie aeree, le attività assicurative e le attività di vettori comuni di fornitori di servizi di telecomunicazione (sebbene la decisione della Corte d'appello degli Stati Uniti per il Nono Circuito del 26 febbraio 2018 nella causa *FTC/AT&T* abbia confermato che l'FTC ha giurisdizione sulle attività di trasporto non comuni di tali soggetti). Cfr. anche allegato IV, nota 2. Il DOT è competente per garantire il rispetto delle norme da parte di compagnie aeree e rivenditori che fanno servizio di biglietteria (per il trasporto aereo), cfr. allegato V, parte A.

([18]) Allegato I, parte III, punto 6.

([19]) Allegato I, parte III, punto 2.

([20]) Allegato I, parte I, punto 8, lettera a).

([21]) Allegato I, parte III, punto 14, lettera g).

([22]) Allegato I, parte I, punto 8, lettera b).

([23]) Allegato I, parte I, punto 8, lettera c).

([24]) Cfr. ad esempio allegato I, parte II, punto 2, lettera b) e parte II, punto 3, lettera b) e punto 7, lettera d), che chiariscono che i procuratori agiscono per conto di un titolare del trattamento, nel rispetto delle istruzioni impartite da quest'ultimo e in base a obblighi contrattuali specifici.

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 ([25]). Inoltre, se il trattamento è delegato a un terzo, un responsabile del trattamento deve concludere con esso un contratto che garantisca lo stesso livello di protezione previsto dai principi e adottare misure per assicurarne la corretta attuazione ([26]).

2.2 **Principi del quadro UE-USA per la protezione dei dati personali**

2.2.1 ***Limitazione della finalità e scelta***

(13) I dati personali dovrebbero essere trattati in maniera lecita e corretta. Dovrebbero inoltre essere raccolti per una finalità specifica e, di conseguenza, essere utilizzati soltanto nella misura in cui l'uso non sia incompatibile con la finalità del trattamento.

(14) Nel quadro del DPF UE-USA, ciò è garantito da diversi principi. Innanzitutto, ai sensi del *principio sull'integrità dei dati e sulla limitazione della finalità*, analogamente a quanto previsto dall'articolo 5, paragrafo 1, lettera b), del regolamento (UE) 2016/679, un'organizzazione non può trattare dati personali in modo incompatibile con la finalità per la quale sono stati inizialmente raccolti o con la finalità successivamente autorizzata dall'interessato ([27]).

(15) In secondo luogo, prima di utilizzare i dati personali per una nuova finalità (modificata) sostanzialmente diversa ma comunque compatibile con quella originaria, oppure di divulgarli a terzi, l'organizzazione deve offrire agli interessati la possibilità di opporsi (rifiuto del trattamento, *opt-out*), conformemente al *principio sulla scelta* ([28]), attraverso un meccanismo chiaro, agevolmente riconoscibile e prontamente disponibile. In aspetto importante è dato dal fatto che tale principio non soppianta l'esplicito divieto di trattamento incompatibile ([29]).

([25]) Allegato I, parte III, punto 10, lettera a). Cfr. anche gli orientamenti elaborati dal Dipartimento del Commercio, in consultazione con il comitato europeo per la protezione dei dati, nell'ambito dello scudo per la privacy, che chiariscono gli obblighi dei responsabili del trattamento statunitensi che ricevono dati personali dall'Unione nel contesto di tale quadro. Poiché tali norme non sono cambiate, tali orientamenti/domande frequenti rimangono pertinenti nel contesto del DPF UE-USA (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Allegato I, parte II, punto 3, lettera b).

([27]) Allegato I, parte II, punto 5, lettera a). Tra le finalità compatibili possono figurare la revisione contabile, la prevenzione delle frodi o altre finalità coerenti con le aspettative di una persona ragionevole tenuto conto del contesto della raccolta (cfr. allegato I, nota 6).

([28]) Allegato I, parte II, punto 2, lettera a). Ciò non si applica quando un'organizzazione fornisce dati personali a un responsabile del trattamento che agisce per suo conto e nel rispetto delle sue istruzioni (allegato I, parte II, punto 2, lettera b)). Detto ciò, in questo caso l'organizzazione deve disporre di un contratto e garantire il rispetto del principio sulla *responsabilità in caso di trasferimento successivo*, come descritto più dettagliatamente al considerando 43. Inoltre il *principio sulla scelta* (nonché il *principio sull'informativa*) possono essere limitati quando i dati personali sono trattati nel contesto della dovuta diligenza (nell'ambito di una potenziale fusione o acquisizione) oppure di revisioni contabili, nella misura e per il tempo necessari a soddisfare prescrizioni di legge o esigenze di interesse pubblico, oppure nella misura in cui e per il tempo durante il quale l'applicazione di tali principi pregiudicherebbe i legittimi interessi dell'organizzazione nel contesto specifico delle indagini o delle revisioni contabili di dovuta diligenza (allegato I, parte III, punto 4). Il principio supplementare 15 (allegato I, parte III, punto 15, lettere a) e b)) prevede altresì un'eccezione al principio sulla *scelta* (nonché ai principi sull'*informativa* e sulla *responsabilità in caso di trasferimento successivo*) per i dati personali provenienti da fonti pubblicamente disponibili (fatto salvo il caso in cui l'esportatore di dati dell'UE indichi che le informazioni sono soggette a limitazioni che richiedono l'applicazione di tali principi) o i dati personali raccolti da registri aperti alla consultazione da parte del pubblico in generale (purché non siano combinati con informazioni non pubbliche e siano rispettate le condizioni per la consultazione). Analogamente, il principio supplementare 14 (allegato I, parte III, punto 14, lettera f)) prevede un'eccezione al principio sulla *scelta* (nonché ai principi sull'*informativa* e sulla *responsabilità in caso di trasferimento successivo*) per il trattamento dei dati personali da parte di un'azienda farmaceutica o di dispositivi medici per le attività di monitoraggio della sicurezza e dell'efficacia dei prodotti, nella misura in cui il rispetto di tali principi interferisca con il rispetto di prescrizioni normative.

([29]) Ciò vale per tutti i dati trasferiti nell'ambito del DPF UE-USA, compresi quelli raccolti nel contesto di un rapporto di lavoro. Benché possa pertanto 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 che si certifica deve osservare il divieto di trattamento incompatibile, e comunque procedere solo nel rispetto dei principi sull'*informativa* e sulla *scelta*. In via eccezionale, un'organizzazione può utilizzare i dati personali per una finalità supplementare compatibile senza fornire l'*informativa* e la *scelta*, ma soltanto nella misura e per il periodo necessari a non pregiudicare la capacità dell'organizzazione di effettuare promozioni, nomine o altre decisioni analoghe in materia di occupazione (cfr. allegato I, parte III, punto 9, lettera b), punto iv)). 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. Cfr. allegato I, parte III, punto 9, lettera b), punto i).

2.2.2 ***Trattamento di categorie particolari di dati personali***

(16) Garanzie specifiche dovrebbero essere applicate al trattamento di "categorie particolari" di dati.

(17) Conformemente al *principio sulla scelta*, si applicano garanzie specifiche al trattamento di "informazioni sensibili", ossia i dati personali che specificano le condizioni mediche o di salute, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, le informazioni sulla vita sessuale di una persona o qualsiasi altra informazione ricevuta da terzi identificati e trattati da tale parte come sensibili ([30]). Ciò significa che tutti i dati considerati sensibili ai sensi del diritto dell'Unione in materia di protezione dei dati (compresi i dati sull'orientamento sessuale, i dati genetici e i dati biometrici) saranno trattati come sensibili nell'ambito del DPF UE-USA da parte delle organizzazioni certificate.

(18) Come norma generale, le organizzazioni devono ottenere il consenso esplicito (*opt-in*) da parte delle persone al fine di utilizzare informazioni sensibili per finalità diverse da quelle per le quali sono state originariamente raccolte o successivamente autorizzate dalla persona (mediante il consenso) o al fine di divulgarle a terzi ([31]).

(19) Non è necessario che tale consenso sia ottenuto in circostanze limitate analoghe a eccezioni comparabili previste dal diritto dell'Unione in materia di protezione dei dati, ad esempio quando il trattamento di dati sensibili è: svolto nell'interesse vitale di una persona; necessario per accertare un diritto in sede giudiziaria; oppure necessario a fini di cura sanitaria o diagnosi medica ([32]);

2.2.3 ***Esattezza, minimizzazione e sicurezza dei dati***

(20) I dati dovrebbero essere esatti e, se necessario, dovrebbero essere aggiornati. Dovrebbero inoltre essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati; inoltre, in linea di principio, dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

(21) Secondo il *principio sull'integrità dei dati e sulla limitazione della finalità* ([33]) i dati personali devono limitarsi a quanto pertinente in considerazione della finalità di trattamento. Inoltre, per quanto necessario rispetto alle finalità del trattamento, l'organizzazione deve adottare misure ragionevoli per assicurare che i dati personali siano affidabili per l'uso previsto, accurati, completi e aggiornati.

(22) Inoltre è possibile conservare le informazioni personali in una forma che identifica o permette di identificare l'interessato (ossia in forma di dati personali) ([34]) solo per il tempo necessario per conseguire la o le finalità per cui sono stati raccolti in origine o quella o quelle successivamente autorizzate dalla persona ai sensi del *principio sulla scelta*. Tale obbligo non osta a che le organizzazioni continuino a trattare le informazioni personali per periodi più lunghi, ma limitatamente al periodo e alla misura in cui il trattamento sia ragionevolmente funzionale a una delle seguenti finalità specifiche analoghe alle eccezioni comparabili previste dal diritto dell'Unione in materia di protezione dei dati: archiviazione nel pubblico interesse, attività giornalistica, letteraria e artistica, ricerca scientifica e storica, analisi statistica ([35]). Qualora i dati personali siano conservati per una di tali finalità, il loro trattamento è subordinato alle garanzie previste dai principi ([36]).

(23) I dati personali dovrebbero inoltre essere trattati in maniera da garantirne la sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. A tal fine i titolari e responsabili del trattamento dovrebbero adottare misure tecniche od organizzative per proteggere i dati personali da possibili minacce. Tali misure dovrebbero essere valutate tenendo conto dello stato dell'arte, dei costi correlati e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti delle persone fisiche.

([30]) Allegato I, parte II, punto 2, lettera c).
([31]) Allegato I, parte II, punto 2, lettera c).
([32]) Allegato I, parte III, punto 1.
([33]) Allegato I, parte II, punto 5.
([34]) Cfr. allegato I, nota 7, che chiarisce che una persona è considerata "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), un'organizzazione o un terzo potrebbe ragionevolmente identificare la persona.
([35]) Allegato I, parte II, punto 5, lettera b).
([36]) *Ibidem*.

(24) Nell'ambito del DPF UE-USA, ciò è garantito dal *principio sulla sicurezza*, che impone, analogamente all'articolo 32 del regolamento (UE) 2016/679, di adottare misure di sicurezza ragionevoli e adeguate, tenuto conto dei rischi insiti nel trattamento dei dati e nella loro natura ([37]).

2.2.4 ***Trasparenza***

(25) Gli interessati dovrebbero essere informati dei principali aspetti del trattamento dei dati personali che li riguardano.

(26) Ciò è garantito dal *principio sull'informativa* ([38]), che, analogamente agli obblighi di trasparenza di cui al regolamento (UE) 2016/679, impone alle organizzazioni di informare gli interessati in merito, tra l'altro: i) all'adesione dell'organizzazione al DPF; ii) al tipo di dati raccolti; iii) alla finalità del trattamento; iv) al tipo o all'identità dei terzi cui possono essere comunicati i dati personali e alle finalità di tale divulgazione; v) ai loro diritti individuali; vi) alle modalità di contatto con l'organizzazione; e vii) ai mezzi di ricorso disponibili.

(27) Tali informazioni devono essere fornite in un linguaggio chiaro e in modo da attirare l'attenzione quando le persone sono invitate per la prima volta a fornire i dati personali o non appena possibile successivamente, ma in ogni caso prima che i dati siano utilizzati per una finalità sostanzialmente diversa da (ma compatibile con) quella per la quale sono stati raccolti o prima che siano divulgati a terzi ([39]).

(28) Inoltre le organizzazioni devono rendere pubbliche le loro politiche della privacy che rispecchiano i principi (o, nel caso dei dati relativi alle risorse umane, metterle prontamente a disposizione delle persone interessate) e fornire un collegamento ipertestuale al sito web del Dipartimento del Commercio (contenente ulteriori dettagli sulla certificazione, sui diritti degli interessati e sui meccanismi di ricorso disponibili), all'elenco degli aderenti al quadro per la protezione dei dati personali (elenco degli aderenti al DPF) che comprende le organizzazioni aderenti e al sito web di un adeguato prestatore di meccanismi alternativi di composizione delle controversie ([40]).

2.2.5 ***Diritti delle persone***

(29) Gli interessati dovrebbero disporre di determinati diritti azionabili nei confronti del titolare del trattamento o del responsabile del trattamento, in particolare il diritto di accesso ai dati, il diritto di opporsi al trattamento e il diritto di far rettificare e cancellare i dati.

(30) Il *principio sull'accesso* ([41]) di cui al DPF UE-USA conferisce tali diritti alle persone. In particolare gli interessati hanno il diritto, senza che sia necessaria alcuna giustificazione, di ottenere da un'organizzazione la conferma dell'eventualità o meno che quest'ultima stia trattando dati personali che li riguardano; di farsi comunicare i dati in questione; e di ottenere informazioni sulla finalità del trattamento, sulle categorie di dati personali trattati e sui destinatari (o sulle categorie di destinatari) a cui sono comunicati i dati ([42]). Le organizzazioni sono tenute a rispondere alle richieste di accesso entro un periodo di tempo ragionevole ([43]). Un'organizzazione può fissare limiti ragionevoli per il numero

([37]) Allegato I, parte II, punto 4, lettera a). Inoltre, per quanto riguarda i dati relativi alle risorse umane, il DPF UE-USA impone ai datori di lavoro di tener conto delle preferenze in materia di tutela della vita privata dei dipendenti limitando l'accesso ai dati personali, rendendo anonimi taluni dati oppure assegnando codici o pseudonimi (allegato I, parte III, punto 9, lettera b), punto iii).

([38]) Allegato I, parte II, punto 1.

([39]) Allegato I, parte II, punto 1, lettera b). Il principio supplementare 14 (allegato I, parte III, punto 14, lettere b e c)) stabilisce disposizioni specifiche per il trattamento dei dati personali nel contesto della ricerca sanitaria e delle sperimentazioni cliniche. In particolare tale principio consente alle organizzazioni di trattare i dati delle sperimentazioni cliniche anche dopo che una persona si ritira dalla sperimentazione in questione, se tale aspetto è stato chiarito nell'informativa fornita quando la persona ha acconsentito a partecipare alla sperimentazione. Analogamente, se un'organizzazione aderente al DPF UE-USA riceve dati personali per finalità di ricerca sanitaria, può utilizzarli soltanto per una nuova attività di ricerca conformemente ai principi sull'*informativa* e sulla *scelta*. In tal caso l'informativa resa alla persona dovrebbe fornire, in linea di principio, informazioni in merito a eventuali usi specifici futuri dei dati (ad esempio studi correlati). Qualora non sia possibile includere sin dall'inizio tutti gli usi futuri dei dati (perché un nuovo uso della ricerca potrebbe derivare da nuove conoscenze o da sviluppi medici/della ricerca), occorre includere nell'informativa una spiegazione del fatto che i dati potranno essere utilizzati in future attività di ricerca medica e farmaceutica non prevedibili in quel momento. Se tale ulteriore utilizzo non è coerente con le finalità generali di ricerca per le quali i dati sono stati raccolti (ossia se le nuove finalità sono sostanzialmente diverse dalla finalità originale, ma comunque compatibili con essa - cfr. considerando 14 e 15), è necessario ottenere un nuovo consenso. Cfr. inoltre le limitazioni/eccezioni specifiche al principio sull'*informativa* di cui alla nota 28.

([40]) Allegato I, parte III, punto 6, lettera d).

([41]) Cfr. anche il principio supplementare sull'accesso (allegato I, parte III, punto 8).

([42]) Allegato I, parte III, punto 8, lettera a), punti da i) a ii).

([43]) Allegato I, parte III, punto 8, lettera i).

di volte entro un determinato periodo di tempo per il quale può soddisfare le richieste di accesso di una determinata persona e può addebitare delle commissioni, non eccessive, ad esempio quando le richieste sono manifestamente eccessive, in particolare in ragione della loro natura ripetitiva ([44]).

(31) Il diritto di accesso può essere limitato soltanto in circostanze eccezionali analoghe a quelle previste dal diritto dell'Unione in materia di protezione dei dati, in particolare in caso di violazione dei diritti legittimi di terzi; quando l'onere o le spese della fornitura dell'accesso sarebbero sproporzionati rispetto ai rischi per la vita privata della persona nelle circostanze del caso (sebbene tali spese e tale onere non siano fattori di controllo per determinare se la fornitura dell'accesso sia ragionevole); nella misura in cui la divulgazione possa interferire con la salvaguardia di importanti interessi pubblici preponderanti, quali la sicurezza nazionale, la sicurezza pubblica o la difesa; le informazioni contengono informazioni commerciali riservate; oppure le informazioni sono trattate esclusivamente per finalità di statistica o ricerca ([45]). Il diniego di un diritto o la sua limitazione deve essere necessario/a e debitamente giustificato/a e l'onere di dimostrare il soddisfacimento di tali condizioni incombe all'organizzazione ([46]). Nell'effettuare tale valutazione, l'organizzazione deve tener conto, in particolare, degli interessi della persona ([47]). Qualora sia possibile separare le informazioni da altri dati cui si applica una limitazione, l'organizzazione deve omettere le informazioni protette e divulgare le informazioni rimanenti ([48]).

(32) Inoltre gli interessati hanno il diritto di ottenere la rettifica o la modifica di dati inesatti e di ottenere la cancellazione dei dati trattati in violazione dei principi ([49]). Come spiegato al considerando 15, le persone hanno altresì il diritto di opporsi/rifiutare il consenso al trattamento dei loro dati per finalità sostanzialmente diverse (ma compatibili) rispetto a quelle per le quali i dati sono stati raccolti, nonché alla divulgazione dei loro dati a terzi. Quando i dati personali sono utilizzati per finalità di marketing diretto, le persone hanno il diritto generale di revocare il consenso al trattamento in qualsiasi momento ([50]).

(33) I principi non affrontano in modo specifico la questione delle decisioni riguardanti l'interessato basate unicamente sul trattamento automatizzato di dati personali. Tuttavia, per quanto riguarda i dati personali raccolti nell'Unione, qualsiasi decisione basata sul trattamento automatizzato sarà generalmente presa dal titolare del trattamento nell'Unione (che ha un rapporto diretto con l'interessato) ed è, di conseguenza, direttamente soggetta al regolamento (UE) 2016/679 ([51]). Ciò comprende i casi di trasferimento in cui il trattamento è effettuato da un operatore economico straniero (ad esempio statunitense) che agisce in qualità di procuratore (responsabile del trattamento) per conto del titolare del trattamento stabilito nell'Unione (o come responsabile del trattamento in seconda battuta che agisce per conto del responsabile del trattamento dell'Unione, che ha ricevuto i dati dal titolare del trattamento dell'Unione che li ha raccolti) che, su questa base, prende la decisione.

(34) Ciò è stato confermato da uno studio commissionato dalla Commissione nel 2018 nel contesto del secondo riesame annuale del funzionamento dello scudo per la privacy ([52]), il quale ha concluso che, all'epoca, non vi erano elementi che suggerissero che le organizzazioni aderenti allo scudo effettuassero di norma un processo decisionale automatizzato sulla base di dati personali trasferiti nell'ambito dello scudo.

([44]) Allegato I, parte III, punto 8, lettera f), punti da i) a ii), e lettera g).
([45]) Allegato I, parte III, punto 4; punto 8, lettere b), c) ed e), punto 14, lettere e) ed f), e punto 15, lettera d).
([46]) Allegato I, parte III, punto 8, lettera e), punto ii). L'organizzazione deve informare la persona dei motivi del diniego o della limitazione e fornire un punto di contatto per eventuali ulteriori richieste di informazioni (parte III, punto 8, lettera a), punto iii).
([47]) Allegato I, parte III, punto 8, lettera a), punti da ii) a iii).
([48]) Allegato I, parte III, punto 8, lettera a), punto i).
([49]) Allegato I, parte II, punto 6 e parte III, punto 8, lettera a), punto i).
([50]) Allegato I, parte III, punti 8 e 12.
([51]) Di contro, nel caso eccezionale in cui l'organizzazione statunitense abbia un rapporto diretto con l'interessato dell'Unione, ciò sarà di norma una conseguenza del fatto che si sia rivolto a persone nell'Unione europea offrendo loro beni o servizi o monitorandone il comportamento. In questo scenario, l'organizzazione statunitense stessa rientrerà nell'ambito di applicazione dell'articolo 3, paragrafo 2, del regolamento (UE) 2016/679 ed è perciò tenuta a rispettare direttamente la normativa dell'Unione in materia protezione dei dati.
([52]) SWD(2018) 497 final, sezione 4.1.5. Lo studio in questione si è concentrato i) sulla misura in cui le organizzazioni aderenti allo scudo per la privacy negli Stati Uniti adottano decisioni riguardanti persone sulla base di un trattamento automatizzato dei dati personali trasferiti da imprese dell'UE nell'ambito di tale scudo; e ii) sulle garanzie offerte alle persone che il diritto federale statunitense prevede per questo tipo di situazioni e le condizioni per l'applicazione di tali garanzie.

(35) In ogni caso, 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 (ad esempio erogazione di credito, offerta di prestiti ipotecari, lavoro, alloggio e assicurazioni), il diritto statunitense offre garanzie specifiche contro le decisioni sfavorevoli ([53]). 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. Nel settore del credito ai consumatori, la legge sull'informativa corretta nel credito (FCRA) e la legge sulle pari opportunità nel credito (ECOA) contengono garanzie che conferiscono ai consumatori una qualche forma di diritto alla spiegazione e il diritto di impugnare la decisione. Tali leggi sono pertinenti in un'ampia serie di settori, tra cui il credito, il lavoro, gli alloggi e le assicurazioni. Inoltre talune leggi antidiscriminazione, quali il titolo VII della legge sui diritti civili (*Civil Rights Act*) e la legge sulle pari opportunità negli alloggi (*Fair Housing Act*), offrono alle persone tutele rispetto ai modelli utilizzati nel processo decisionale automatizzato che potrebbero condurre a discriminazioni sulla base di determinate caratteristiche e conferiscono alle persone il diritto di impugnare tali decisioni, comprese quelle basate su un trattamento automatizzato. Per quanto concerne le informazioni sanitarie, la norma sulla privacy della legge sulla portabilità e responsabilità dell'assicurazione sanitaria (HIPAA) crea alcuni diritti simili a quelli di cui al regolamento (UE) 2016/679 per quanto concerne l'accesso alle informazioni sanitarie personali. Inoltre gli orientamenti delle autorità statunitensi impongono ai prestatori di servizi medici di ricevere informazioni che consentano loro di informare le persone in merito ai sistemi basati su un processo decisionale automatizzato utilizzati nel settore medico ([54]).

(36) Pertanto tali norme offrono tutele analoghe a quelle previste dal diritto dell'Unione in materia di protezione dei dati nell'improbabile circostanza in cui decisioni automatizzate siano adottate dall'organizzazione stessa aderente al DPF UE-USA.

2.2.6 ***Limitazioni ai trasferimenti successivi***

(37) Il livello di protezione offerto ai dati personali trasferiti dall'Unione verso organizzazioni negli Stati Uniti non deve essere compromesso da ulteriori trasferimenti di tali dati a un destinatario che si trova negli Stati Uniti o in un altro paese terzo.

(38) Ai sensi del *principio sulla responsabilità in caso di trasferimento successivo* ([55]), al cosiddetto "trasferimento successivo", vale a dire il trasferimento di dati personali da un'organizzazione aderente al DPF UE-USA 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). Qualsiasi trasferimento successivo può aver luogo soltanto i) per finalità limitate e specifiche, ii) sulla base di un contratto stipulato tra l'organizzazione aderente al DPF UE-USA e il terzo ([56]) (o un accordo analogo all'interno di un gruppo aziendale ([57])) e iii) soltanto se tale contratto impone a detto terzo di fornire il medesimo livello di protezione garantito dai principi.

(39) Tale obbligo di garantire il medesimo livello di protezione garantito dai principi, letto in combinazione con il *principio sull'integrità dei dati e sulla limitazione della finalità*, significa in particolare che il terzo può trattare le informazioni personali che gli sono state trasmesse soltanto per finalità che non sono incompatibili con quelle per le quali sono state raccolte o che sono state successivamente autorizzate dall'interessato (conformemente al *principio sulla scelta*).

([53]) Cfr. ad esempio la legge sulle pari opportunità nel credito (codice degli Stati Uniti, titolo 15, articolo 1691 e seguenti), legge sull'informativa corretta nel credito (codice degli Stati Uniti, titolo 15, articolo 1681 e seguenti) o legge sulle pari opportunità negli alloggi (codice degli Stati Uniti, titolo 42, articolo 3601 e seguenti). Inoltre gli Stati Uniti hanno sottoscritto i principi dell'Organizzazione per la cooperazione e lo sviluppo economici in materia di intelligenza artificiale, che comprendono, tra l'altro, principi in materia di trasparenza, capacità di spiegare, sicurezza e responsabilizzazione.

([54]) Cfr. ad esempio gli orientamenti disponibili al seguente indirizzo: 2042-*What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans?* | HHS.gov.

([55]) Cfr. allegato I, parte II, punto 3, e il principio supplementare sui contratti obbligatori per i trasferimenti successivi (allegato I, parte III, punto 10).

([56]) In deroga a questo principio generale, un'organizzazione può trasferire successivamente i dati personali di un numero esiguo di dipendenti senza stipulare un contratto con il destinatario per esigenze operative occasionali legate all'occupazione, ad esempio la prenotazione di un volo, una camera d'albergo o una copertura assicurativa. Tuttavia, anche in questo caso, l'organizzazione deve comunque rispettare i principi sull'*informativa* e sulla *scelta* (cfr. allegato I, parte III, punto 9, lettera e)).

([57]) Cfr. principio supplementare sui contratti obbligatori per il trasferimento successivo (allegato I, parte III, punto 10), lettera 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 che si è certificata come aderente è fortemente incentivata a impiegare strumenti dalla sicura efficacia pratica.

(40) Anche il *principio sulla responsabilità in caso di trasferimento successivo* andrebbe letto in combinazione con il *principio sull'informativa* e, in caso di trasferimento successivo a un terzo titolare del trattamento ([58]), con il *principio sulla scelta*, secondo cui l'interessato deve essere informato (tra l'altro) del tipo/dell'identità di qualsiasi terzo destinatario dei dati, dello scopo del trasferimento successivo e della scelta offerta, e può opporsi al trasferimento successivo (facoltà di rifiuto) o, in caso di dati sensibili, deve necessariamente dare il "consenso esplicito" allo stesso (facoltà di accettazione).

(41) 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.

(42) In tutti i casi il contratto con il terzo destinatario deve prevedere che questi informi l'organizzazione aderente al DPF UE-USA se constata di non poter più assolvere quest'obbligo. A seguito della constatazione in tal senso, il terzo deve cessare il trattamento oppure deve adottare un'altra misura ragionevole e adeguata per rimediare alla situazione ([59]).

(43) In caso di trasferimento successivo a un terzo procuratore (ad esempio un responsabile del trattamento) si applicano tutele supplementari. In tal caso l'organizzazione statunitense deve garantire che il procuratore agisca soltanto secondo le istruzioni e 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 ([60]). Il Dipartimento del Commercio può imporre all'organizzazione di fornire una sintesi o una copia rappresentativa delle disposizioni del contratto in materia di protezione dei dati ([61]). Qualora sorgano problemi di conformità in una catena di trattamento (delegato), l'organizzazione che agisce in qualità di titolare del trattamento dei dati personali è in linea di principio responsabile, come specificato nel *principio su ricorso, controllo e responsabilità*, fatto salvo il caso in cui dimostri di non essere responsabile dell'evento che ha cagionato il danno ([62]).

2.2.7 ***Responsabilizzazione***

(44) Secondo il principio di responsabilizzazione, i soggetti che trattano dati sono tenuti a mettere in atto misure tecniche e organizzative adeguate per rispettare efficacemente i loro obblighi in materia di protezione dei dati e per essere in grado di dimostrare tale rispetto, in particolare all'autorità di controllo competente.

(45) Una volta che ha volontariamente deciso di certificarsi ([63]) nell'ambito del DPF UE-USA, un'organizzazione è tenuta a rispettarne i principi che sono effettivi ed azionabili. Ai sensi del *principio su ricorso, controllo e responsabilità* ([64]), le organizzazioni aderenti al DPF UE-USA devono fornire meccanismi efficaci per garantire il rispetto dei principi. Le organizzazioni devono altresì adottare misure atte a verificare ([65]) che la loro politica della privacy sia conforme ai principi e applicata effettivamente. La verifica può configurarsi come autovalutazione, nel cui sistema devono essere comprese procedure interne atte ad 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 conformità, nel cui sistema possono rientrare verifiche, controlli a campione o il ricorso a strumenti tecnologici.

([58]) 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.

([59]) 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 aderente al DPF UE-USA, intervenire in questo senso, perché è lei il titolare del trattamento in base alle cui istruzioni opera il procuratore. Cfr. allegato I, parte II, punto 3.

([60]) Allegato I, parte II, punto 3, lettera b).

([61]) *Ibidem*.

([62]) Allegato I, parte II, punto 7, lettera d).

([63]) Cfr. anche il principio supplementare sull'autocertificazione (allegato I, parte III, punto 6).

([64]) Cfr. anche il principio supplementare sulla composizione delle controversie e sul controllo dell'applicazione (allegato I, parte III, punto 11).

([65]) Cfr. anche il principio supplementare sulla verifica (allegato I, parte III, punto 7).

(46) Inoltre le organizzazioni devono tenere traccia dell'attuazione delle loro pratiche in materia di DPF UE-USA e, nell'ambito delle indagini o dei reclami per mancato soddisfacimento dei requisiti, metterle a disposizione, a richiesta, di un organo indipendente di composizione delle controversie o di un'autorità di contrasto competente ([66]).

2.3 **Amministrazione, vigilanza e controllo dell'attuazione**

(47) Il DPF UE-USA sarà amministrato e monitorato dal Dipartimento del Commercio. Il DPF prevede meccanismi di vigilanza e di controllo dell'attuazione atti a verificare e garantire che le organizzazioni aderenti al DPF UE-USA rispettino i principi e che qualsiasi caso di inosservanza sia affrontato. Tali meccanismi sono illustrati nei principi (allegato I) e negli impegni assunti dal Dipartimento del Commercio (allegato III), dall'FTC (allegato IV) e dal DOT (allegato V).

2.3.1 ***(Ri)certificazione***

(48) Per certificarsi ai sensi del DPF UE-USA (o per ricertificarsi annualmente), le organizzazioni sono tenute a dichiarare pubblicamente il loro impegno a rispettare i principi, a rendere disponibili le loro politiche della privacy e ad attuarle pienamente ([67]). Nel contesto della loro domanda di (ri)certificazione, le organizzazioni devono presentare al Dipartimento del Commercio informazioni riguardanti, tra l'altro, il nome dell'organizzazione pertinente, una descrizione delle finalità per le quali l'organizzazione tratterà i dati personali, i dati personali che saranno oggetto della certificazione, nonché il metodo di verifica scelto, il pertinente meccanismo di ricorso indipendente e l'ente competente a garantire il rispetto dei principi ([68]).

(49) Le organizzazioni possono ricevere dati personali sulla base del DPF UE-USA dalla data in cui sono inserite nell'elenco degli aderenti al DPF da parte del Dipartimento del Commercio. Al fine di garantire la certezza del diritto ed evitare "casi di millantata adesione", le organizzazioni che si certificano per la prima volta non possono fare pubblicamente riferimento alla loro adesione ai principi prima che il Dipartimento del Commercio abbia stabilito che la domanda di certificazione dell'organizzazione è completa e l'abbia aggiunta all'elenco degli aderenti al DPF ([69]). Per poter continuare a fruire del DPF UE-USA per ricevere dati personali dall'Unione, tali organizzazioni devono ricertificare ogni anno la loro adesione al regime. L'organizzazione che, per qualsiasi motivo, abbandona il DPF UE-USA deve eliminare tutte le dichiarazioni che lasciano intendere che l'organizzazione continui ad aderire al regime ([70]).

(50) Come rispecchiato negli impegni di cui all'allegato III, il Dipartimento del Commercio verificherà se le organizzazioni soddisfano tutti i requisiti di certificazione e hanno messo in atto una politica della privacy (pubblica) contenente le informazioni richieste ai sensi del *principio sull'informativa* ([71]). Sulla base dell'esperienza acquisita con il processo di (ri)certificazione nel contesto dello scudo per la privacy, il Dipartimento del Commercio effettuerà una serie di controlli, anche per verificare se le politiche della privacy delle organizzazioni contengano un collegamento ipertestuale al modulo corretto di reclamo sul sito web del pertinente meccanismo di risoluzione delle controversie e, qualora una domanda di certificazione comprenda più soggetti e filiali di un'organizzazione, per verificare se le politiche della privacy di ciascuno di tali soggetti soddisfino i requisiti di certificazione e siano prontamente a disposizione degli interessati ([72]). Inoltre, ove necessario, il Dipartimento del Commercio effettuerà controlli incrociati con l'FTC e il DOT al fine di verificare che le organizzazioni siano soggette all'organismo di vigilanza indicato nelle loro domande di (ri)certificazione e collaborerà con gli organi di composizione alternativa delle controversie al fine di verificare che le organizzazioni siano registrate presso il meccanismo di ricorso indipendente indicato nella loro domanda di (ri)certificazione ([73]).

([66]) Allegato I, parte III, punto 7.
([67]) Allegato I, parte I, punto 2.
([68]) Allegato I, parte III, punto 6, lettera b) e allegato III, parte "Verifica del soddisfacimento dei requisiti per l'autocertificazione".
([69]) Allegato I, nota 12.
([70]) Allegato I, parte III, punto 6, lettera h).
([71]) Allegato I, parte III, punto 6, lettera a) e nota 12, nonché allegato III, parte "Verifica del soddisfacimento dei requisiti per l'autocertificazione".
([72]) Allegato III, parte "Verifica del soddisfacimento dei requisiti per l'autocertificazione".
([73]) Analogamente il Dipartimento del Commercio collaborerà con il terzo che fungerà da depositario dei fondi riscossi tramite i contributi per le spese del comitato delle autorità di protezione dei dati (cfr. considerando 73) al fine di verificare che le organizzazioni che scelgono le autorità di protezione dei dati come loro meccanismo di ricorso indipendente abbiano versato il contributo spese per l'anno in questione. Cfr. allegato III, parte "Verifica del soddisfacimento dei requisiti per l'autocertificazione".

(51) Il Dipartimento del Commercio informerà le organizzazioni che, per completare la (ri)certificazione, devono affrontare tutte le questioni individuate durante il suo riesame. Nel caso in cui un'organizzazione non risponda entro un termine stabilito dal Dipartimento del Commercio (ad esempio per quanto concerne la ricertificazione si prevede che il processo sia completato entro 45 giorni) ([74]) o non completi altrimenti la sua certificazione, la domanda sarà considerata abbandonata. In tal caso, qualsiasi falsa dichiarazione in merito all'adesione al DPF UE-USA o al rispetto di tale regime può essere oggetto di un'azione coercitiva da parte dell'FTC o del DOT ([75]).

(52) Ai fini di una corretta applicazione del DPF UE-USA, 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. Al fine di garantire tale trasparenza a livello di "punto di entrata", il Dipartimento del Commercio si è impegnato a tenere e mettere a disposizione del pubblico un elenco delle organizzazioni che si sono certificate come aderenti ai principi e che rientrano nella sfera di competenza di almeno una delle autorità di applicazione della legge di cui agli allegati IV e V della presente decisione ([76]). Il Dipartimento del Commercio aggiornerà l'elenco in funzione delle domande annuali di ricertificazione presentate dalle organizzazioni e degli eventuali ritiri o delle eventuali esclusioni di organizzazioni dal regime del DPF UE-USA. Inoltre, al fine di garantire la trasparenza anche presso il "punto di uscita", il Dipartimento del Commercio tiene e mette a disposizione del pubblico anche un elenco ufficiale delle organizzazioni depennate dall'elenco, indicando per ciascuna il motivo dell'esclusione ([77]). Infine fornirà un collegamento ipertestuale alla pagina web dell'FTC dedicata al DPF UE-USA, che elencherà le azioni coercitive avviate dall'FTC nell'ambito del quadro ([78]).

2.3.2 *Controllo della conformità*

(53) Il Dipartimento del Commercio controllerà costantemente l'effettivo rispetto dei principi da parte delle organizzazioni aderenti al DPF UE-USA attraverso meccanismi diversi ([79]). In particolare effettuerà "controlli a campione" di organizzazioni selezionate in modo casuale, nonché controlli a campione ad hoc di organizzazioni specifiche quando vengono individuate potenziali questioni in materia di conformità (ad esempio organizzazioni segnalate al Dipartimento del Commercio da terzi) per verificare se: i) il punto o i punti di contatto per la gestione dei reclami e delle richieste degli interessati sono disponibili e reattivi; ii) la politica della privacy dell'organizzazione in questione è prontamente disponibile, sia sul suo sito web che tramite un collegamento ipertestuale sul sito web del Dipartimento del Commercio; iii) la politica della privacy dell'organizzazione continua a rispettare i requisiti di certificazione; e iv) il meccanismo indipendente di risoluzione delle controversie scelto dall'organizzazione è disponibile per la gestione dei reclami ([80]).

(54) Il Dipartimento del Commercio imporrà all'organizzazione di compilare e presentare un questionario dettagliato, qualora vi siano prove attendibili del fatto che un'organizzazione non rispetta gli impegni assunti nell'ambito del DPF UE-USA (anche qualora il Dipartimento del Commercio riceva reclami o l'organizzazione non risponda in modo soddisfacente alle richieste di informazioni formulate da detto Dipartimento) ([81]). Un'organizzazione che non risponda in modo soddisfacente e tempestivo al questionario sarà deferita all'autorità competente (FTC o DOT) ai fini dell'adozione di eventuali azioni coercitive ([82]). Nel contesto delle sue attività di controllo della conformità nell'ambito dello scudo, il Dipartimento del Commercio ha effettuato regolarmente i controlli a campione di cui al

([74]) Allegato III, nota 2.
([75]) Cfr. allegato III, parte "Verifica del soddisfacimento dei requisiti per l'autocertificazione".
([76]) Informazioni sulla gestione dell'elenco degli aderenti al DPF sono disponibili nell'allegato III (cfr. introduzione di cui alla parte "Gestione e supervisione del programma 'Quadro per la protezione dei dati personali (DPF) da parte del Dipartimento del Commercio") e nell'allegato I (parte I, punto 3, parte I, punto 4, parte III, punto 6), lettera d), e parte III, punto 11, lettera g)).
([77]) Allegato III, cfr. introduzione di cui alla parte "Gestione e supervisione del programma 'Quadro per la protezione dei dati personali (DPF) da parte del Dipartimento del Commercio".
([78]) Cfr. allegato III, parte "Adattamento del sito web dedicato al quadro per la protezione dei dati personali ai gruppi di destinatari".
([79]) Cfr. allegato III, parte "Svolgimento di controlli periodici d'ufficio della conformità e valutazioni del programma del DPF".
([80]) Nel contesto delle sue attività di controllo, il Dipartimento del Commercio può utilizzare diversi strumenti, tra cui la verifica di collegamenti ipertestuali interrotti di rimando a politiche della privacy o il monitoraggio attivo di notizie in merito a segnalazioni che forniscono prove credibili di casi di inosservanza.
([81]) Cfr. allegato III, parte "Svolgimento di controlli periodici d'ufficio della conformità e valutazioni del programma del DPF".
([82]) Cfr. allegato III, parte "Svolgimento di controlli periodici d'ufficio della conformità e valutazioni del programma del DPF".

considerando 53 e ha monitorato costantemente le segnalazioni pubbliche, attività queste che gli hanno consentito di individuare, affrontare e risolvere questioni in materia di conformità ([83]). Il Dipartimento depenna dall'elenco degli aderenti al DPF le organizzazioni che hanno commesso reiterate inosservanze dei principi, le quali devono restituire o cancellare i dati personali ricevuti nell'ambito del quadro ([84]).

(55) Negli altri casi di depennamento dall'elenco, come in caso di revoca volontaria dell'adesione o di mancata ricertificazione, l'organizzazione deve cancellare o restituire i dati oppure può conservarli a condizione che dichiari ogni anno al Dipartimento del Commercio il proprio impegno di continuare ad applicare i principi oppure li protegga adeguatamente con un altro mezzo autorizzato (ad esempio un contratto che rispecchi totalmente le condizioni delle pertinenti clausole contrattuali tipo approvate dalla Commissione) ([85]). In tal caso l'organizzazione deve designare altresì al suo interno un referente per tutte le questioni relative al DPF UE-USA.

2.3.3 *Individuazione e gestione di casi di millantata adesione*

(56) Il Dipartimento del Commercio monitorerà eventuali casi di millantata adesione al DPF UE-USA o l'uso improprio del marchio di certificazione di tale regime, sia d'ufficio che sulla base di reclami (ad esempio ricevuti dalle autorità di protezione dei dati) ([86]). In particolare il Dipartimento del Commercio verificherà su base continuativa che le organizzazioni che i) revocano l'adesione al DPF UE-USA, ii) non completano la ricertificazione annuale (ossia che hanno avviato il processo annuale di ricertificazione ma non lo hanno completato in modo tempestivo o non hanno neppure avviato detto processo), iii) sono depennate dall'elenco degli aderenti al regime, in particolare a causa di una "inosservanza reiterata", o iv) non hanno completato una certificazione iniziale (ossia che hanno avviato il processo di certificazione iniziale ma non lo hanno completato in modo tempestivo), eliminino da qualsiasi politica della privacy pertinente pubblicata eventuali riferimenti al DPF UE-USA che implicano che l'organizzazione aderisce attivamente a tale quadro ([87]). Il Dipartimento del Commercio effettuerà inoltre ricerche su internet per individuare riferimenti al DPF UE-USA nelle politiche della privacy delle organizzazioni, anche per individuare casi di millantata adesione da parte di organizzazioni che non hanno mai partecipato al DPF UE-USA ([88]).

(57) Se la Dipartimento del Commercio constata che i riferimenti al DPF UE-USA non sono stati rimossi o sono utilizzati in modo improprio, informa l'organizzazione in merito a un possibile deferimento all'FTC/al DOT ([89]). Se un'organizzazione non risponde in modo soddisfacente, il Dipartimento del Commercio deferisce la questione all'ente competente affinché siano adottate eventuali azioni coercitive ([90]). Se millanta pubblicamente l'adesione ai principi con dichiarazioni o pratiche fuorvianti, l'organizzazione si espone alle azioni coercitive dell'FTC, del DOT 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, titolo 18, articolo 1001).

([83]) Nel corso del secondo riesame annuale dello scudo per la privacy, il Dipartimento del Commercio ha comunicato di aver effettuato controlli a campione su 100 organizzazioni e di aver inviato questionari sulla conformità in 21 casi (attività in seguito alla quale le questioni individuate sono state risolte) (cfr. documento di lavoro dei servizi della Commissione SWD(2018) 497 final, pag. 9). Analogamente, nel corso del terzo riesame annuale dello scudo per la privacy, il Dipartimento del Commercio ha riferito di aver individuato tre casi di non conformità attraverso il monitoraggio delle segnalazioni pubbliche e di aver avviato la pratica di effettuare controlli a campione su 30 imprese ogni mese, il che ha portato ad attività di seguito con questionari sulla conformità nel 28 % dei casi (dopo tali attività le questioni rilevate sono state immediatamente sanate o, in tre casi, sono state risolte in seguito a una lettera di avvertimento) (cfr. Commissione europea, SWD(2019) 495 final, pag. 9).

([84]) Allegato I, parte III, punto 11, lettera g). Si verifica un'inosservanza reiterata in particolare quando un'organizzazione rifiuta di conformarsi a una decisione definitiva emessa da un'autorità di autoregolamentazione, di risoluzione indipendente delle controversie o di contrasto in materia di tutela della vita privata.

([85]) Allegato I, parte III, punto 6, lettera f).

([86]) Allegato III, parte "Reperimento dei casi di millantata adesione e loro soluzione".

([87]) *Ibidem*.

([88]) *Ibidem*.

([89]) *Ibidem*.

([90]) Nell'ambito dello scudo per la privacy, nel corso del terzo riesame annuale di tale quadro, il Dipartimento del Commercio ha riferito di aver individuato 669 casi di millantata adesione (tra ottobre 2018 e ottobre 2019), la maggior parte dei quali sono stati risolti in seguito a una lettera di avvertimento del Dipartimento del Commercio; mentre sono stati 143 i casi deferiti all'FTC (cfr. considerando 62). Cfr. Commissione europea, SWD(2019) 495 final, pag. 10.

2.3.4 ***Applicazione***

(58) Al fine di garantire un livello di protezione adeguato dei dati nella pratica, dovrebbe esistere un'autorità di controllo indipendente cui siano conferiti i poteri di monitorare e assicurare il rispetto delle norme in materia di protezione dei dati.

(59) Le organizzazioni aderenti al DPF UE-USA devono essere soggette alla competenza giurisdizionale delle autorità statunitensi competenti (FTC e DOT), che dispongono dell'autorità d'indagine e di controllo necessaria per garantire efficacemente il rispetto dei principi ([91]).

(60) L'FTC è un'autorità indipendente composta da cinque commissari, nominati dal presidente con il parere e il consenso del Senato ([92]). I commissari sono nominati per un mandato di sette anni e il loro incarico può essere revocato dal presidente soltanto per inefficienza, negligenza o concussione. L'FTC non può avere più di tre commissari del medesimo partito politico e i commissari non possono, durante la loro nomina, intraprendere altre attività commerciali o professionali o assumere altri impieghi.

(61) L'FTC può indagare sul rispetto dei principi, nonché sui casi di millantata adesione ai principi o al DPF UE-USA da parte di organizzazioni che non figurano più nell'elenco degli aderenti al DPF o non si sono mai certificate ([93]). L'FTC può imporre il rispetto delle norme chiedendo l'emissione di provvedimenti amministrativi o federali (comprese le "ordinanze consensuali" ottenute mediante transazione) ([94]) per ingiunzioni preliminari o permanenti oppure altri mezzi di ricorso, e controllerà sistematicamente il rispetto di tali provvedimenti ([95]). Se l'organizzazione non si conforma a tali provvedimenti, l'FTC ha facoltà di presentare un'istanza per ottenere sanzioni civili e altre riparazioni, anche per l'eventuale danno causato dal comportamento illecito. Ciascuna ordinanza consensuale emanata nei confronti di un'organizzazione aderente al DPF UE-USA prevede obblighi di informazione da parte dell'organizzazione ([96]), cui è imposto di rendere pubbliche le parti inerenti a tale regime 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 di un organo giurisdizionale in casi collegati al DPF UE-USA ([97]).

(62) Per quanto concerne lo scudo per la privacy, l'FTC ha adottato misure coercitive in circa 22 casi, sia per quanto riguarda violazioni di requisiti specifici del quadro (ad esempio: mancata dichiarazione al Dipartimento del Commercio del fatto che l'organizzazione continuava ad applicare le tutele di cui allo scudo per la privacy dopo aver abbandonato tale regime; mancata verifica, mediante un'autovalutazione o una verifica esterna della conformità, del fatto che l'organizzazione rispettava il regime) ([98]) e casi di millantata adesione al regime (ad esempio da parte di organizzazioni che non hanno completato le fasi necessarie per ottenere la certificazione o hanno lasciato scadere la loro certificazione, ma hanno millantato di continuare ad aderire al regime) ([99]). Tale azione coercitiva è sfociata tra l'altro in un uso proattivo delle citazioni amministrative al fine di ottenere materiale da taluni aderenti allo scudo per verificare l'esistenza di violazioni sostanziali degli obblighi di cui allo scudo per la privacy ([100]).

([91]) Un'organizzazione aderente al DPF UE-USA 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 (codice degli Stati Uniti, titolo 15, articolo 45) e a norma del codice degli Stati Uniti, titolo 49, articolo 41712, che vieta a un vettore o a un rivenditore che fa servizio di biglietteria di adottare pratiche sleali o ingannevoli nel trasporto aereo o nell'attività di vendita di trasporto aereo.

([92]) Codice degli Stati Uniti, titolo 15, articolo 41.

([93]) Allegato IV.

([94]) 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 a un organo giurisdizionale.

([95]) Cfr. allegato IV, parte "Ottenimento e controllo di provvedimenti".

([96]) L'ordinanza dell'FTC o dell'organo giurisdizionale può obbligare l'impresa ad attuare un programma in materia di tutela della vita privata e a trasmettere periodicamente all'FTC relazioni di conformità o valutazioni effettuate da terzi indipendenti in relazione a tale programma.

([97]) Allegato IV, parte "Ottenimento e controllo di provvedimenti".

([98]) Commissione europea, SWD(2019) 495 final, pag. 11.

([99]) Cfr. l'elenco dei casi sul sito web dell'FTC, disponibile all'indirizzo: https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Cfr. anche Commissione europea, SWD(2017) 344 final, pag. 17; Commissione europea, SWD(2018) 497 final, pag. 12 e SWD(2019) 495 final, pag. 11.

([100]) Cfr. ad esempio *Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review* (ftc.gov).

(63) Più in generale, negli ultimi anni l'FTC ha adottato azioni coercitive in una serie di casi riguardanti il rispetto di requisiti specifici in materia di protezione dei dati previsti anche dal DPF UE-USA, ad esempio per quanto concerne i principi di limitazione delle finalità e di conservazione dei dati ([101]), di minimizzazione dei dati ([102]), nonché di sicurezza ([103]) e di accuratezza dei dati ([104]).

(64) 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. I funzionari del DOT mirano innanzitutto a raggiungere una transazione e, se ciò non è possibile, possono avviare un'azione coercitiva che comporta un'udienza probatoria dinanzi a un giudice amministrativo del DOT che ha la facoltà di emettere provvedimenti inibitori e di infliggere sanzioni civili ([105]). I giudici amministrativi beneficiano di diverse tutele previste dalla legge sulle procedure amministrative (APA) per garantirne l'indipendenza e l'imparzialità. Ad esempio, possono essere rimossi dal loro incarico soltanto per giusta causa; sono assegnati ai casi a rotazione; non possono esercitare funzioni incompatibili con le loro funzioni e responsabilità in qualità di giudici amministrativi; non sono soggetti al controllo da parte della squadra investigativa dell'autorità di cui sono dipendenti (in questo caso il DOT); e devono svolgere la loro funzione di giudizio/esecutiva in modo imparziale ([106]). Il DOT si è impegnato a monitorare i provvedimenti coercitivi e a garantire che le ordinanze derivanti da casi di DPF UE-USA siano disponibili sul suo sito web ([107]).

2.4 **Mezzi di ricorso**

(65) Al fine di garantire una protezione adeguata e, in particolare, il rispetto dei diritti individuali, l'interessato dovrebbe avere a disposizione mezzi di ricorso efficaci in sede amministrativa e giudiziaria.

(66) Con il *principio su ricorso, controllo e responsabilità* il DPF UE-USA impone all'organizzazione aderente di mettere mezzi di ricorso a disposizione della persona lesa dall'inosservanza, offrendo quindi all'interessato dell'Unione la possibilità di sporgere reclamo per mancato rispetto dei principi da parte di organizzazioni aderenti al DPF UE-USA e di ottenere la soluzione del caso di reclamo, se necessario con una decisione che dispone un rimedio effettivo ([108]). Nell'ambito della certificazione l'organizzazione deve adempiere gli obblighi imposti da tale principio 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 ([109]).

([101]) Cfr. ad esempio l'ordinanza dell'FTC nel caso *Drizly, LLC.*, che ha imposto all'impresa, tra l'altro, 1) di distruggere tutti i dati personali raccolti dei quali non necessita per fornire prodotti o servizi ai consumatori; 2) di astenersi dal raccogliere o conservare informazioni personali, fatto salvo il caso in cui ciò sia necessario per finalità specifiche indicate in un programma di conservazione.

([102]) Cfr. ad esempio l'ordinanza dell'FTC nel caso *CafePress* (24 marzo 2022) che impone, tra l'altro, di ridurre al minimo la quantità di dati raccolti.

([103]) Cfr. ad esempio l'azione coercitiva dell'FTC nel contesto dei casi *Drizzly, LLC* e *CafePress*, nell'ambito dei quali ha imposto alle imprese interessate di mettere in atto un programma di sicurezza dedicato o misure di sicurezza specifiche. Inoltre, per quanto concerne le violazioni dei dati, cfr. anche l'ordinanza dell'FTC del 27 gennaio 2023 nel caso *Chegg* e l'accordo transattivo raggiunto con Equifax nel 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Cfr. ad esempio il caso *RealPage, Inc* (16 ottobre 2018), nel contesto del quale l'FTC ha adottato un'azione coercitiva nell'ambito dell'applicazione della legge sull'informativa corretta nel credito nei confronti di una società di vaglio dei locatari che forniva ai proprietari di immobili e alle società di gestione di immobili relazioni di contesto sulle persone sulla base di informazioni tratte da precedenti locativi, informazioni contenute in registri pubblici (compresi precedenti penali e di sfratto) e informazioni sul credito, che sono state utilizzate come fattore per determinare l'ammissibilità all'ottenimento dell'alloggio. L'FTC ha constatato che tale società non aveva adottato misure ragionevoli per garantire l'esattezza delle informazioni da essa fornite sulla base del proprio strumento di autodecisione.

([105]) Cfr. allegato V, parte "Pratiche di applicazione".

([106]) Cfr. codice degli Stati Uniti, titolo 5, articolo 3105, articolo 7521, lettera a), articolo 554, lettera d) e articolo 556, lettera b), punto 3).

([107]) Allegato V, parte "Controllo dell'esecuzione e pubblicazione dei provvedimenti coercitivi inerenti a violazioni dei principi del DPF UE-USA".

([108]) Allegato I, parte II, punto 7.

([109]) Allegato I, parte III, punto 11.

(67) L'organizzazione può scegliere meccanismi di ricorso indipendenti dell'Unione o degli Stati Uniti, compresa la possibilità di impegnarsi volontariamente a cooperare con le autorità di protezione dei dati dell'UE, come spiegato più in dettaglio al considerando 73. Quando le organizzazioni trattano dati relativi alle risorse umane, tale impegno a cooperare con le autorità di protezione dei dati dell'UE è obbligatorio. Fra le altre opzioni disponibili si annoverano gli organi di composizione alternativa delle controversie o i programmi per la privacy elaborati dal settore privato nei quali sono integrati i principi del DPF. Questi ultimi devono contemplare meccanismi di attuazione efficaci rispondenti ai requisiti indicati nel *principio su ricorso, controllo e responsabilità*.

(68) Il DPF UE-USA offre quindi all'interessato varie possibilità di far valere i propri diritti, di sporgere reclamo per inosservanza dei principi da parte di imprese dell'UE e statunitensi 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, al Dipartimento del Commercio oppure all'FTC. 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 (allegato I dell'allegato I 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 i meccanismi 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.

(69) Innanzitutto l'interessato nell'UE può sottoporre il caso di inosservanza dei principi direttamente alle organizzazioni aderenti al DPF UE-USA ([110]). 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), così come l'organo indipendente di composizione delle controversie (cfr. il considerando 70). 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'Unione entro il termine di 45 giorni ([111]). 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 ([112]) (se l'organizzazione si è impegnata a cooperare con tali autorità).

(70) 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 ([113]). 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 ([114]). L'organo indipendente di composizione delle controversie designato da un'organizzazione è tenuto a riportare sul proprio sito web pubblico le pertinenti informazioni relative al DPF UE-USA e ai servizi che presta in tale ambito ([115]). Deve pubblicare ogni anno una relazione che presenti, in forma aggregata, i dati statistici relativi ai servizi prestati ([116]).

([110]) Allegato I, parte III, punto 11, lettera d), punto i).
([111]) Allegato I, parte III, punto 11, lettera d), punto i).
([112]) 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 I, parte III, punto 5).
([113]) Allegato I, parte III, punto 11, lettera d).
([114]) Allegato I, parte II, punto 7 e parte III, punto 11, lettera e).
([115]) Allegato I, parte III, punto 11, lettera d), punto ii).
([116]) La relazione annuale deve indicare: 1) il numero complessivo dei reclami in virtù del DPF UE-USA 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; e 4) l'esito dei reclami ricevuti, in particolare il numero e il tipo delle riparazioni o delle sanzioni inflitte.

(71) Le procedure di controllo della conformità seguite dal Dipartimento del Commercio possono prevedere la verifica del fatto che le organizzazioni aderenti al DPF UE-USA siano effettivamente registrate presso i meccanismi di ricorso indipendenti a cui dichiarano di essere registrate ([117]). 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 al DPF UE-USA. Il Dipartimento del Commercio collaborerà con meccanismi di ricorso indipendenti al fine di verificare che includano informazioni sui propri siti web in merito ai principi e ai servizi forniti nell'ambito del DPF UE-USA e che pubblichino relazioni annuali ([118]).

(72) 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 ad un'altra autorità statunitense competente delle indagini in merito alla non conformità dell'organizzazione) ovvero al giudice competente ([119]). 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 od organo constata che l'organizzazione viola i principi frequentemente, si può configurare 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 degli aderenti al DPF ([120]). Se l'organizzazione depennata dall'elenco continua a millantare la certificazione rispetto al DPF UE-USA, il Dipartimento del Commercio la deferisce all'FTC o altra autorità di applicazione della legge ([121]).

(73) In terzo luogo, le persone possono promuovere altresì reclamo presso un'autorità nazionale di protezione dei dati nell'Unione, che può avvalersi dei propri poteri di indagine e di correzione a norma del regolamento (UE) 2016/679. L'organizzazione è tenuta a cooperare 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 ([122]). 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 ([123]). In caso di mancato rispetto del parere fornito dall'autorità di protezione dei dati, quest'ultima deferirà tali casi al Dipartimento del Commercio (che può depennare le organizzazioni dall'elenco degli aderenti al DPF) o, per eventuali azioni coercitive, all'FTC o al DOT (la mancata cooperazione con le autorità di protezione dei dati o la mancata conformità rispetto ai principi è perseguibile ai sensi del diritto statunitense) ([124]).

(74) Al fine di facilitare la cooperazione per una gestione efficace dei reclami, sia il Dipartimento del Commercio che l'FTC hanno istituito un apposito punto di contatto competente della gestione dei contatti diretti con le autorità di protezione dei dati ([125]). Tali punti di contatto forniscono assistenza in relazione alle richieste di informazioni dell'autorità di protezione dei dati in merito al rispetto dei principi da parte di un'organizzazione.

(75) Il parere fornito dalle autorità di protezione dei dati ([126]) è espresso dopo che le due parti della controversia hanno avuto ragionevoli possibilità di formulare commenti e addurre qualsiasi elemento di prova desiderino. Il comitato può esprimere 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 ([127]). 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 può notificarle l'intenzione di sottoporre il caso all'FTC (o ad altra autorità statunitense di

([117]) Allegato I, parte "Verifica del soddisfacimento dei requisiti per l'autocertificazione".
([118]) Cfr. allegato III, parte "Facilitazione della cooperazione con gli organi di composizione alternativa delle controversie che forniscono servizi connessi ai principi". Cfr. anche allegato I, parte III, punto 11, lettera d), punti da ii) a iii).
([119]) Cfr. allegato I, parte III, punto 11, lettera e).
([120]) Cfr. allegato I, parte III, punto 11, lettera g), in particolare ii) e iii).
([121]) Cfr. allegato III, parte "Reperimento dei casi di millantata adesione e loro soluzione".
([122]) Allegato I, parte II, punto 7, lettera b).
([123]) Allegato I, parte III, punto 5.
([124]) Allegato I, parte III, punto 5, lettera c), punto ii).
([125]) Allegato III (cfr. parte "Agevolazione della cooperazione con le autorità di protezione dei dati") e allegato IV (cfr. le parti "Attribuzione di priorità ai casi e indagini" e "Cooperazione esecutiva con le autorità di protezione dei dati dell'UE").
([126]) In considerazione della loro competenza a organizzare la propria attività e a cooperare tra loro, le autorità di protezione dei dati dovrebbero adottare il regolamento interno del comitato informale.
([127]) Allegato I, parte III, punto 5, lettera c), punto i).

applicazione della legge) ovvero di concludere che si è verificato un grave inadempimento dell'impegno a cooperare. Nel primo caso, la conseguenza può essere un'azione coercitiva ai sensi dell'articolo 5 della legge sull'FTC (o legge analoga) ([128]). 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 al DPF.

(76) 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 dell'UE.

(77) 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 cooperazione sulle questioni relative ai reclami individuali e all'inosservanza da parte delle organizzazioni aderenti al DPF UE-USA, 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 del DPF UE-USA ([129]). Analogamente l'FTC si è impegnata a istituire un punto di contatto dedicato ([130]).

(78) 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 ad adoperarsi al massimo per risolvere i casi ([131]). 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 organizzazioni per facilitare la soluzione del caso ([132]). 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 ([133]). Questo modus operandi permette all'interessato di sporgere reclamo per inosservanza dei principi da parte di organizzazioni aderenti al DPF UE-USA direttamente alla pertinente autorità nazionale di protezione dei dati, che provvede poi a inoltrarla al Dipartimento del Commercio in quanto autorità di gestione di tale regime negli Stati Uniti.

(79) 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 al DPF ([134]). 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 ([135]).

(80) In quinto luogo, le organizzazioni aderenti al DPF UE-USA devono essere soggette alla competenza giurisdizionale delle autorità statunitensi, in particolare dell'FTC ([136]), che dispone dell'autorità d'indagine e di controllo necessaria per garantire efficacemente il rispetto dei principi. L'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 ([137]). 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. Può accettare inoltre i reclami presentati direttamente dalle persone e avviare di propria iniziativa indagini nell'ambito del DPF UE-USA, in particolare nel quadro delle più ampie indagini in materia di tutela della vita privata.

([128]) Allegato I, parte III, punto 5, lettera c), punto ii).
([129]) Cfr. allegato III, parte "Agevolazione della cooperazione con le autorità di protezione dei dati".
([130]) Cfr. allegato IV, parti "Attribuzione di priorità ai casi e indagini" e "Cooperazione esecutiva con le autorità di protezione dei dati dell'UE".
([131]) Allegato III, cfr. ad esempio la parte "Agevolazione della cooperazione con le autorità di protezione dei dati".
([132]) Allegato I, parte II, punto 7, lettera e) e allegato III, parte "Agevolazione della cooperazione con le autorità di protezione dei dati".
([133]) *Ibidem*.
([134]) Allegato I, parte III, punto 11, lettera g).
([135]) Allegato I, parte III, punto 11, lettera g).
([136]) L'organizzazione aderente al DPF UE-USA 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.
([137]) Cfr. anche gli impegni analoghi assunti dal DOT (allegato V).

(81) In sesto luogo, l'interessato dell'Unione può chiedere l'arbitrato vincolante del collegio del quadro UE-USA per la protezione dei dati personali (collegio del DPF UE-USA) come *extrema ratio* nel caso in cui gli altri mezzi di ricorso disponibili non gli abbiano offerto una soluzione soddisfacente per il reclamo sporto ([138]). L'organizzazione deve informare la persona della possibilità di chiedere un arbitrato vincolante; una volta che la possibilità si concreta con l'invio dell'avviso all'organizzazione, questa è tenuta a darvi riscontro ([139]).

(82) Il collegio del DPF UE-USA è composto da un gruppo di almeno dieci 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 ([140]) arbitri.

(83) L'*International Centre for Dispute Resolution* (ICDR, Centro internazionale per la composizione delle controversie), la divisione internazionale dell'*American Arbitration Association* (AAA, Associazione americana per l'arbitrato), è stato selezionato dal Dipartimento del Commercio per amministrare gli arbitrati. I procedimenti dinanzi al collegio del DPF UE-USA saranno disciplinati da una serie di norme arbitrali concordate e da un codice di condotta per gli arbitri nominati. Il sito web dell'ICDR dell'AAA fornisce alle persone informazioni chiare e concise sul meccanismo di arbitrato e sulla procedura da seguire per depositare una domanda di arbitrato.

(84) Le norme arbitrali concordate tra il Dipartimento del Commercio e la Commissione integrano il DPF UE-USA, che contiene diverse caratteristiche che migliorano l'accessibilità a tale meccanismo da parte degli interessati dell'Unione: 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'Unione 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 in linea di massima 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 al DPF UE-USA 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 ([141]).

(85) Il collegio del DPF UE-USA ha il potere di imporre il necessario "provvedimento equo, specifico alla persona e di carattere non pecuniario" ([142]) 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 del DPF UE-USA, 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 organizzazioni aderenti al DPF UE-USA, di meccanismi di ricorso indipendenti o di 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'organizzazione aderente al DPF UE-USA, ossia quando l'organizzazione è tenuta a cooperare 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'organizzazione non si conforma alla decisione arbitrale.

([138]) Cfr. allegato I, allegato I "Modello arbitrale".
([139]) Cfr. allegato I, parte II, punto 1, lettera a) e parte II, punto 7, lettera c).
([140]) Il numero di arbitri nel collegio dev'essere concordato tra le parti.
([141]) Allegato I dell'allegato I, parte G, punto 6.
([142]) 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.

(86) In settimo luogo, se un'organizzazione non soddisfa il proprio impegno a rispettare i principi e la politica della privacy pubblicata, il diritto statunitense prevede ulteriori possibilità di ricorso giurisdizionale, anche per ottenere un risarcimento dei danni. Ad esempio, a determinate condizioni, le persone possono ottenere un ricorso giurisdizionale (compreso il risarcimento dei danni) ai sensi delle leggi statali sui consumatori in caso di millanteria fraudolenta, atti o pratiche sleali o ingannevoli ([143]), e ai sensi del diritto del risarcimento per fatto illecito (in particolare per quanto concerne i reati di intrusione in caso di isolamento ([144]), appropriazione del nome o delle sembianze ([145]) e divulgazione pubblica di fatti privati ([146])).

(87) Congiuntamente, le varie vie di ricorso di cui sopra garantiscono che ogni reclamo relativo all'inosservanza del DPF UE-USA da parte di organizzazioni certificate sia giudicato e risolto in modo efficace.

3. ACCESSO E USO DI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA DA PARTE DI AUTORITÀ PUBBLICHE NEGLI STATI UNITI

(88) La Commissione ha valutato altresì le limitazioni e le garanzie, compresi i meccanismi di vigilanza e di ricorso individuale messi a disposizione dal diritto statunitense per quanto concerne la raccolta e il successivo utilizzo da parte di autorità pubbliche statunitensi dei dati personali trasferiti verso titolari e responsabili del trattamento negli Stati Uniti per motivi di interesse pubblico, in particolare per finalità di contrasto penale e di sicurezza nazionale ("accesso da parte di pubbliche amministrazioni") ([147]). Nel valutare se le condizioni in base alle quali l'accesso da parte di pubbliche amministrazioni ai dati trasferiti verso gli Stati Uniti ai sensi della presente decisione soddisfino la verifica dell'"equivalenza sostanziale" ai sensi dell'articolo 45, paragrafo 1, del regolamento (UE) 2016/679, come interpretato dalla Corte di giustizia alla luce della Carta dei diritti fondamentali, la Commissione ha tenuto conto di diversi criteri.

(89) In particolare qualsiasi limitazione nell'esercizio del diritto alla protezione dei dati personali deve essere prevista dalla legge e implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato ([148]). Inoltre, per soddisfare il requisito di proporzionalità secondo cui le deroghe e le limitazioni alla protezione dei dati personali devono operare nei limiti dello stretto necessario in una società democratica per soddisfare gli obbiettivi specifici di interesse generale equivalenti a quelli riconosciuti dall'Unione, questa base giuridica deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e impongano requisiti minimi in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi ([149]).

([143]) Cfr. ad esempio leggi statali in materia di protezione dei consumatori in California (codice civile della California, articoli 1750-1785 (*West*), legge sui mezzi di ricorso a disposizione dei consumatori); Distretto della Columbia (codice del Distretto della Colombia, articoli 28-3901); Florida (*Fla. Stat.*, articoli 501.201-501.213, legge sulle pratiche commerciali ingannevoli e sleali); Illinois (*815 Ill. Comp. Stat. 505/1 - 505/12*, legge sulle pratiche aziendali ingannevoli e sleali nei confronti dei consumatori); Pennsylvania (*73 Pa. Stat. Ann., articoli 201-1 - 201-9.3 (West)*, legge sulle pratiche commerciali sleali e sulla protezione dei consumatori).

([144]) Ossia in caso di ingerenza intenzionale negli affari privati o nelle questioni private di una persona, in un modo che sarebbe altamente offensivo nei confronti di una persona ragionevole (*Restatement (2nd) of Torts*, articolo 652(b)).

([145]) Solitamente tale illecito si applica in caso di appropriazione e uso del nome o delle sembianze di una persona per pubblicizzare un'impresa o un prodotto o per una finalità commerciale analoga (cfr. *Restatement (2nd) of Torts*, articolo 652C).

([146]) Ossia quando le informazioni relative alla vita privata di una persona sono rese pubbliche, qualora ciò sia altamente offensivo nei confronti di una persona ragionevole e le informazioni non siano fonte di legittima preoccupazione per il pubblico (*Restatement (2nd) of Torts*, articolo 652D).

([147]) Ciò è pertinente altresì alla luce dell'allegato I, parte I, punto 5. Ai sensi di tale parte e in analogia con il GDPR, il rispetto dei requisiti in materia di protezione dei dati e dei diritti che fanno parte dei principi in materia di protezione dei dai può essere soggetto a limitazioni. Tuttavia tali limitazioni non sono assolute, ma possono essere invocate soltanto qualora siano soddisfatte diverse condizioni, ad esempio nella misura necessaria per conformarsi a un'ordinanza di un organo giurisdizionale o soddisfare l'interesse pubblico, applicare la legge o requisiti di sicurezza nazionale. In questo contesto e per motivi di chiarezza, la presente sezione fa riferimento anche alle condizioni di cui al decreto presidenziale 14086 che sono valutate tra l'altro nei considerando da 127 a 141.

([148]) Cfr. *Schrems II*, punti 174 e 175 e giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, sentenza della Corte di giustizia del 6 ottobre 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, punto 65; e sentenza della Corte di giustizia del 6 ottobre 2020, *La Quadrature du Net e a./Premier ministre e a.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, punto 175.

([149]) Cfr. *Schrems II*, punti 176 e 181, nonché la giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, *Privacy International*, punto 68; e *La Quadrature du Net e a.*, punto 132.

Inoltre tali norme e garanzie devono essere giuridicamente vincolanti e azionabili da parte delle persone ([150]). In particolare gli interessati devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati ([151]).

3.1 **Accesso e uso da parte delle autorità pubbliche statunitensi per motivi di contrasto penale**

(90) Per quanto concerne l'ingerenza nei dati personali trasferiti nell'ambito del DPF UE-USA per finalità di contrasto penale, il diritto statunitense impone una serie di limitazioni in materia di accesso ai dati personali e di loro utilizzo e prevede meccanismi di vigilanza e ricorso che sono in linea con i requisiti di cui al considerando 89 della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono. A tale riguardo, il governo degli Stati Uniti (attraverso il ministero della Giustizia) ha fornito altresì assicurazioni circa le limitazioni e le garanzie applicabili (allegato VI della presente decisione).

3.1.1 ***Basi giuridiche, limitazioni e garanzie***

3.1.1.1 *Limitazioni e garanzie per quanto concerne la raccolta di dati personali a fini di contrasto penale*

(91) I procuratori federali e gli inquirenti federali statunitensi possono accedere, per finalità di contrasto penale, ai dati personali trattati da organizzazioni statunitensi certificate che verrebbero trasferiti dall'Unione ai sensi del DPF UE-USA nel contesto di procedure diverse, come illustrato più dettagliatamente nei considerando da 92 a 99. Tali procedure si applicano allo stesso modo quando le informazioni sono ottenute da un'organizzazione statunitense, indipendentemente dalla cittadinanza o dal luogo di residenza dell'interessato ([152]).

(92) Innanzitutto, su richiesta di un funzionario delle autorità di contrasto federali o di un avvocato che agisce per il governo, un giudice può emettere un mandato di perquisizione o di sequestro (anche relativo a informazioni conservate su supporto elettronico) ([153]). Tale mandato può essere emesso soltanto qualora vi sia un "motivo plausibile ([154])" per ritenere che sia possibile rinvenire nel luogo specificato dal mandato "oggetti sequestrabili" (prove di un reato, oggetti detenuti illegalmente o beni progettati per o destinati ad essere utilizzati o che sono stati utilizzati per commettere un reato). Il mandato deve identificare i beni o gli oggetti da sequestrare e designare il

([150]) Cfr. *Schrems II*, punti 181 e 182.

([151]) Cfr. *Schrems I*, punto 95 e *Schrems II*, punto 194. A tale riguardo la Corte di giustizia dell'Unione europea ha sottolineato in particolare che il rispetto dell'articolo 47 della Carta dei diritti fondamentali, garantendo il diritto a un ricorso effettivo dinanzi un organo giurisdizionale indipendente e imparziale, "è anch'esso parte del livello di protezione richiesto all'interno dell'Unione e [...] deve essere constatato dalla Commissione prima di adottare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 1, del regolamento (UE) 2016/679" (*Schrems II*, punto 186).

([152]) Cfr. allegato VI. Cfr. ad esempio, per quanto riguarda la *Wiretap Act* (legge sulle intercettazioni), la *Stored Communications Act* (legge sulle comunicazioni archiviate) e la *Pen Register Act* (legge sui dispositivi di intercettazione) (citate più dettagliatamente nei considerando da 95 a 98), *Suzlon Energy Ltd/Microsoft Corp., 671 F.3d 726, 729* (9th Cir. 2011).

([153]) Norme federali di procedura penale, norma 41. In una sentenza del 2018, la Corte Suprema ha confermato che le autorità di contrasto necessitano di un mandato di perquisizione o di un'eccezione al mandato anche per l'accesso a registrazioni storiche dell'ubicazione del sito a livello di cella, che forniscono una panoramica completa dei movimenti di un utente, così come che l'utente può nutrire una ragionevole aspettativa di tutela della vita privata rispetto a tali informazioni (*Timothy Ivory Carpenter/United States of America*, n. 16-402, 585 U.S. (2018)). Di conseguenza, in generale, tali dati non possono essere ottenuti da una società di telefonia mobile in forza di un'ordinanza di un organo giurisdizionale che si basa su ragionevoli motivi per ritenere che le informazioni siano pertinenti e rilevanti per un'indagine penale in corso, ma è necessario dimostrare l'esistenza di un motivo plausibile in caso di ricorso a un mandato.

([154]) Secondo la Corte suprema, con "motivo plausibile" si intende una norma "pratica e non tecnica" che impone "considerazioni concrete e pratiche della vita quotidiana secondo le quali agisce un uomo ragionevole e prudente [...]" (*Illinois/Gates*, 462 U.S. 213, 232 (1983)). Per quanto concerne i mandati di perquisizione, un motivo plausibile sussiste in presenza di un'equa probabilità che una perquisizione porti alla scoperta di prove di un reato (ibidem).

giudice al quale il mandato deve essere restituito. Una persona soggetta a perquisizione o i cui beni sono soggetti a perquisizione può chiedere la cancellazione delle prove ottenute o derivate da una perquisizione illegale se tali prove vengono presentate contro tale persona durante un processo penale ([155]). Quando è tenuto a divulgare dati in forza di un mandato, il titolare dei dati (ossia un'impresa) può contestare l'obbligo di divulgazione in quanto indebitamente gravoso ([156]).

(93) In secondo luogo, nell'ambito di indagini in merito a determinati reati gravi ([157]), solitamente su richiesta di un procuratore federale, è possibile richiedere l'emissione di una citazione da parte di un *grand jury* (un ramo investigativo di un organo giurisdizionale, formato da giurati scelti da un giudice o un magistrato) al fine di imporre a qualcuno di produrre o mettere a disposizione documenti aziendali, informazioni conservate su supporto elettronico o altri beni materiali. Inoltre leggi diverse autorizzano il ricorso a 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 ([158]). In entrambi i casi le informazioni devono essere pertinenti ai fini dell'indagine e la citazione non può essere irragionevole, ossia eccessivamente ampia, vessatoria o gravosa (e può essere impugnata dal destinatario della citazione in ragione di tali motivi) ([159]).

(94) Condizioni molto analoghe si applicano alle citazioni amministrative emesse per chiedere l'accesso ai dati detenuti da società negli Stati Uniti per finalità civili o normative ("interesse pubblico"). L'autorità degli enti con competenze civili o di regolamentazione per l'emissione di tali citazioni amministrative deve essere stabilita per legge. L'uso di una citazione amministrativa è soggetto a una "prova di ragionevolezza", che richiede che l'indagine sia condotta ai sensi di una finalità legittima, che le informazioni richieste nel contesto della citazione siano pertinenti a tale finalità, che l'ente non disponga già delle informazioni richieste con la citazione e che siano state seguite le fasi amministrative necessarie per l'emissione della citazione ([160]). La giurisprudenza della Corte suprema ha inoltre chiarito la necessità di trovare un equilibrio tra l'importanza dell'interesse pubblico nelle informazioni richieste e l'importanza degli interessi personali e organizzativi in materia di vita privata ([161]). Sebbene il ricorso a una citazione amministrativa non sia soggetto a previa autorizzazione giudiziaria, esso è soggetto a sindacato giurisdizionale in caso di contestazione da parte del destinatario per i motivi summenzionati, o se l'ente emittente cerca di dare esecuzione alla citazione in giudizio ([162]). Oltre a queste limitazioni fondamentali generali, dalle singole leggi possono derivare requisiti specifici (più rigorosi) ([163]).

([155]) *Mapp/Ohio*, 367 U.S. 643 (1961).

([156]) Cfr. *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (nella quale si afferma che il giusto processo richiede un'audizione in merito alla questione dell'onerosità prima di obbligare una società telefonica a fornire assistenza in relazione a un mandato di perquisizione) e *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

([157]) Il quinto emendamento della costituzione degli Stati Uniti richiede un'incriminazione da parte del grand jury per qualsiasi reato che comporti la pena capitale o sia comunque infamante. Il *grand jury* è composto da 16 a 23 membri e constata l'eventuale sussistenza di un motivo plausibile per ritenere che sia stato commesso un reato. Per giungere a tale conclusione, ai *grand jury* sono conferiti poteri d'indagine che consentono loro di emettere citazioni.

([158]) Cfr. allegato VI.

([159]) Norme federali di procedura penale, norma 17.

([160]) *United States/Powell*, 379 U.S. 48 (1964).

([161]) *Oklahoma Press Publishing Co./Walling*, 327 U.S. 186 (1946).

([162]) La Corte Suprema ha chiarito che, in caso di contestazione di una citazione amministrativa, un organo giurisdizionale deve considerare se 1) l'indagine viene svolta per una finalità legittimamente autorizzata, 2) l'autorità che effettua la citazione in questione rientra nel potere di comando del Congresso e 3) i documenti richiesti sono pertinenti ai fini dell'indagine. La Corte ha rilevato altresì che una richiesta di citazione amministrativa deve essere ragionevole, ossia richiedere una specificazione adeguata dei documenti da presentare, ma non eccessiva, ai fini dell'indagine pertinente, compresa la particolarità nella descrizione del luogo da perquisire e delle persone o cose da sequestrare.

([163]) Ad esempio la legge sul diritto alla privacy finanziaria conferisce a un'autorità pubblica il potere di ottenere documenti finanziari detenuti da un istituto finanziario a norma di una citazione amministrativa soltanto se 1) vi è motivo di ritenere che i documenti richiesti siano pertinenti per un'indagine legittima per fini di contrasto e 2) una copia della citazione è stata fornita al cliente unitamente a un avviso che attesti con ragionevole specificità la natura dell'indagine (Codice degli Stati Uniti, titolo 12, articolo 3405). Un altro esempio è la legge sull'informativa corretta nel credito, che vieta agli enti che generano relazioni sui consumatori di divulgare le comunicazioni dei consumatori in risposta a richieste di citazioni amministrative (e consente loro soltanto di rispondere a richieste di citazione del *grand jury* o a ordinanze di un organo giurisdizionale, Codice degli Stati Uniti, titolo 15, articolo 1681 e seguenti). Per quanto concerne l'accesso alle informazioni sulle comunicazioni, si applicano i requisiti specifici della legge sulle comunicazioni archiviate, anche per quanto concerne la possibilità di ricorrere a citazioni amministrative (cfr. considerando 96 e 97 per una panoramica dettagliata).

(95) In terzo luogo, diverse basi giuridiche consentono alle autorità di contrasto in materia penale di ottenere l'accesso a dati relativi alle comunicazioni. Un organo giurisdizionale può emettere un'ordinanza che autorizza la raccolta in tempo reale di informazioni non di contenuto su un dato numero di telefono o indirizzo di posta elettronica (numero composto, instradamento della comunicazione, destinatario e segnale), tramite il ricorso a dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita, se constata che l'autorità ha certificato che le informazioni che potrebbero essere ottenute sono pertinenti per un'indagine penale in corso ([164]). Detta ordinanza deve specificare tra l'altro l'identità, se nota, della persona indiziata; gli attributi delle comunicazioni alle quali si applica e una dichiarazione del reato cui si riferiscono le informazioni da raccogliere. L'uso di un dispositivo di intercettazione dei dati informativi della comunicazione in entrata e in uscita può essere autorizzato per un periodo massimo di sessanta giorni, che può essere prorogato soltanto mediante una nuova ordinanza di un organo giurisdizionale.

(96) Inoltre l'accesso per finalità di contrasto penale a informazioni sugli abbonati, ai dati sul traffico e al contenuto archiviato delle comunicazioni detenute da prestatori di servizi internet, da società telefoniche e da altri prestatori terzi di servizi può essere ottenuto sulla base della legge sulle comunicazioni archiviate ([165]). Per acquisire il contenuto archiviato delle comunicazioni elettroniche, le autorità di contrasto in materia penale devono, in linea di principio, ottenere un mandato del giudice, fondato su motivi plausibili per ritenere che l'account contenga prove di un reato ([166]). 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 possono ricorrere a una citazione a comparire. Per la maggior parte delle altre informazioni non di contenuto archiviate, quali intestazioni di posta elettronica senza oggetto, un'autorità di contrasto in materia penale deve ottenere un'ordinanza di un organo giurisdizionale, che sarà emessa qualora il giudice ritenga che vi siano ragionevoli motivi per ritenere che le informazioni richieste siano pertinenti e rilevanti per un'indagine penale in corso.

(97) I prestatori che ricevono richieste ai sensi della legge sulle comunicazioni archiviate possono informare volontariamente un cliente o abbonato le cui informazioni sono oggetto di una richiesta, fatta eccezione per i casi in cui l'autorità di contrasto in materia penale competente ottenga un provvedimento cautelare che vieti tale notifica ([167]). Tale provvedimento cautelare è un'ordinanza di un organo giurisdizionale che impone a un prestatore di servizi di comunicazione elettronica o di servizi informatici a distanza destinatario di un mandato, una citazione o un'ordinanza di un organo giurisdizionale di non notificare a terzi l'esistenza di detto mandato o detta citazione od ordinanza, per tutto il tempo in cui il giudice lo ritenga opportuno. I provvedimenti cautelari sono concessi se un giudice ritiene che vi sia motivo di ritenere che la notifica in questione comprometterebbe gravemente un'indagine o ritarderebbe indebitamente un processo, ad esempio perché comporterebbe un pericolo per la vita o la sicurezza fisica di una persona, la fuga dall'azione penale, l'intimidazione di potenziali testimoni, ecc. Un memorandum del Procuratore generale aggiunto (vincolante per tutti gli avvocati e gli agenti del Dipartimento della Giustizia) impone ai procuratori di prendere una decisione dettagliata in merito alla necessità di un provvedimento cautelare e di fornire al giudice una giustificazione del modo in cui i criteri di legge per l'ottenimento di un tale provvedimento sarebbero soddisfatti nel caso specifico ([168]). Il memorandum impone inoltre che le domande per l'ottenimento di provvedimenti cautelari non debbano, in linea di principio, essere intese a ritardare la notifica per più di un anno. Qualora, in circostanze eccezionali, possano essere necessari provvedimenti di durata più lunga, tali provvedimenti possono essere richiesti soltanto con l'accordo scritto di un supervisore designato dal Procuratore degli Stati Uniti o dal Procuratore generale aggiunto pertinente. Inoltre, al momento della chiusura di un'indagine, il procuratore deve valutare immediatamente se vi sia la base per mantenere in essere eventuali provvedimenti cautelari esistenti e, in caso contrario, porre fine al provvedimento cautelare in questione e garantire che il prestatore di servizi ne sia informato ([169]).

([164]) Codice degli Stati Uniti, titolo 18, articolo 3123.

([165]) Codice degli Stati Uniti, titolo 18, articoli 2701-2713.

([166]) Codice degli Stati Uniti, titolo 18, articolo 2701, lettera a) e lettera b), punto 1), lettera A). Se l'abbonato o il cliente interessato riceve una notifica (preventiva o, in determinate circostanze, mediante una notifica tardiva), le informazioni di contenuto conservate per più di 180 giorni possono essere ottenute anche sulla base di una citazione amministrativa o del *grand jury* (Codice degli Stati Uniti, titolo 18, articolo 2701, lettera b), punto 1), lettera B)) o di un'ordinanza di un organo giurisdizionale (se vi sono ragionevoli motivi per ritenere che le informazioni siano pertinenti e rilevanti per un'indagine penale in corso (Codice degli Stati Uniti, titolo 18, articolo 2701, lettera d)). Tuttavia, conformemente a una sentenza della Corte d'appello federale, in generale gli investigatori governativi ottengono dai giudici mandati di perquisizione al fine di raccogliere il contenuto di comunicazioni private o dati archiviati da un prestatore di servizi di comunicazione commerciale. *United States/Warshak*, 631 F.3d 266 (6th Cir. 2010).

([167]) Codice degli Stati Uniti, titolo 18, articolo 2705, lettera b).

([168]) Cfr. il memorandum emesso dal Procuratore generale aggiunto Rod Rosenstein del 19 ottobre 2017 in merito a una politica più restrittiva in materia di domande di provvedimenti cautelari (o di non divulgazione), disponibile all'indirizzo: https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Memorandum emesso dalla Procuratrice generale aggiunta Lisa Moncao il 27 maggio 2022 in merito a una politica integrativa in materia di domande di provvedimenti cautelari ai sensi del codice degli Stati Uniti, titolo 18, articolo 2705, lettera b).

(98) Le autorità di contrasto in materia penale possono intercettare altresì in tempo reale comunicazioni orali, via cavo o elettroniche sulla base dell'ordinanza di un organo giurisdizionale nella quale 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 ([170]).

(99) Ulteriori tutele sono fornite da varie politiche e vari orientamenti del Dipartimento della Giustizia, tra cui gli orientamenti del Procuratore generale per le operazioni del *Federal Bureau of Investigation* (FBI) all'interno degli USA (AGG-DOM), che prevedono, tra l'altro, che l'FBI utilizzi i metodi investigativi meno intrusivi possibili, tenendo conto dell'effetto sulla vita privata e sulle libertà civili ([171]).

(100) Secondo le dichiarazioni trasmesse dal governo degli Stati Uniti, tutele equivalenti o superiori descritte sopra vigono per le indagini delle autorità di contrasto a livello di Stati federati (per le indagini svolte a norma di leggi dello Stato federato) ([172]). In particolare le disposizioni costituzionali, nonché le leggi e la giurisprudenza a livello di Stato, ribadiscono le suddette tutele contro perquisizioni e sequestri irragionevoli richiedendo l'emissione di un mandato di perquisizione ([173]). Analogamente alle tutele concesse a livello federale, i mandati di perquisizione possono essere emessi soltanto a fronte di una dimostrazione di una causa probabile e devono descrivere il luogo da perquisire e la persona o la cosa da sequestrare ([174]).

([170]) Codice degli Stati Uniti, titolo 18, articoli 2510-2522.

([171]) Orientamenti del Procuratore generale per le operazioni del *Federal Bureau of Investigation* (FBI) all'interno degli USA (settembre 2008), disponibili all'indirizzo: http://www.justice.gov/archive/opa/docs/guidelines.pdf. Il manuale per i procuratori degli Stati Uniti (*United States Attorneys' Manual* - USAM), disponibile all'indirizzo http://www.justice.gov/usam/united-states-attorneys-manual, prevede ulteriori norme e politiche che limitano le attività investigative dei procuratori federali. Per discostarsi da tali orientamenti, è necessario ottenere l'approvazione preventiva da parte del direttore dell'FBI, del vicedirettore o del direttore esecutivo aggiunto dell'FBI designato da detto direttore, fatto salvo il caso in cui tale approvazione non possa essere ottenuta per motivi di immediatezza o gravità di una minaccia per la sicurezza di persone o beni oppure per la sicurezza nazionale (nel qual caso occorre notificare tale circostanza al direttore o ad altra persona autorizzata al più presto). In caso di mancato rispetto degli orientamenti, l'FBI ne informa il Dipartimento della Giustizia, il quale a sua volta ne informa il Procuratore generale e il Procuratore generale aggiunto.

([172]) Allegato VI, nota 2. Cfr. anche *Arnold/City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) (nella quale si afferma che nei settori dei diritti individuali e delle libertà civili, la costituzione degli Stati Uniti, ove applicabile agli Stati, prevede una soglia al di sotto della quale le decisioni degli organi giurisdizionali statali non possono scendere); *Cooper/California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) (nella quale si afferma che la sentenza della corte non pregiudica chiaramente il potere dello Stato di imporre norme più rigorose in materia di perquisizioni e sequestri rispetto a quelle previste dalla costituzione federale, qualora decida di procedere in tal senso); *Petersen/City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) (nella quale si afferma che sebbene la costituzione dell'Arizona possa imporre norme più severe per le perquisizioni e i sequestri rispetto alla costituzione federale, gli organi giurisdizionali dell'Arizona non possono fornire una protezione inferiore a quella di cui al quarto emendamento).

([173]) La maggior parte degli Stati ha ripreso le tutele previste dal quarto emendamento nelle proprie costituzioni. Cfr. costituzione dell'Alabama, articolo I, § 5); costituzione dell'Alaska, articolo I, § 14; 1; costituzione dell'Arkansas, articolo II, § 15; costituzione della California, articolo I, § 13; costituzione del Colorado, articolo II, § 7; costituzione del Connecticut, articolo I, § 7; costituzione del Delaware, articolo I, § 6; costituzione della Florida, articolo I, § 12; costituzione della Georgia, articolo I, § I, para. XIII; costituzione delle Hawaii, articolo I, § 7; costituzione dell'Idaho, articolo I, § 17; costituzione dell'Illinois, articolo I, § 6; costituzione dell'Indiana, articolo I, § 11; costituzione dell'Iowa, articolo I, § 8; costituzione del Kansas, legge sui diritti, § 15; costituzione del Kentucky, § 10; costituzione della Louisiana, articolo I, § 5; costituzione del Maine, articolo I, § 5; costituzione del Massachusetts, dichiarazione dei diritti, articolo 14; costituzione del Michigan, articolo I, § 11; costituzione del Minnesota, articolo I, § 10; costituzione del Mississippi, articolo III, § 23; costituzione del Missouri, articolo I, § 15; costituzione del Montana, articolo II, § 11; costituzione del Nebraska, articolo I, § 7; costituzione del Nevada, articolo I, § 18; costituzione del New Hampshire, parte 1, articolo 19; costituzione del New Jersey, articolo II, § 7; costituzione del New Mexico, articolo II, § 10; costituzione del New York, articolo I, § 12; costituzione del North Dakota, articolo I, § 8; costituzione dell'Ohio, articolo I, § 14; costituzione dell'Oklahoma, articolo II, § 30; costituzione dell'Oregon, articolo I, § 9; costituzione della Pennsylvania, articola I, § 8; costituzione del Rhode Island, articolo I, § 6; costituzione del South Carolina, articolo I, § 10; costituzione del South Dakota, articolo VI, § 11; costituzione del Tennessee, articolo I, § 7; costituzione del Texas, articolo I, § 9; costituzione dello Utah, articolo I, § 14; costituzione del Vermont, capitolo I, articolo 11; costituzione del West Virginia, articolo III, § 6; costituzione del Wisconsin, articolo I, § 11; costituzione del Wyoming, articolo I, § 4. Altri (ad esempio Maryland, North Carolina e Virginia) hanno inserito nelle loro costituzioni una formulazione specifica in merito ai mandati che è stata interpretata dalla magistratura per fornire protezioni analoghe o superiori al quarto emendamento (cfr. dichiarazione dei diritti del Maryland, articolo 26; costituzione del North Carolina, articolo I, § 20; costituzione della Virginia, articolo I, § 10 e la relativa giurisprudenza, ad esempio *Hamel/State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; *State/Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) and *Lowe/Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Infine l'Arizona e Washington hanno disposizioni costituzionali che tutelano la vita privata in modo più generale (costituzione dell'Arizona, articolo 2, § 8; costituzione di Washington, articolo I, § 7), che sono state interpretate dagli organi giurisdizionali come disposizioni che forniscono protezioni maggiori rispetto al quarto emendamento (cfr. ad esempio *State/Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State/Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State/Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), *State/Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Cfr. ad esempio il codice penale della California § 1524,3(b); le norme da 3.6 a 3.13 delle norme di procedura penale dell'Alabama; l'articolo 10.79.035 del codice rivisto di Washington; l'articolo 19.2-59 del capitolo 5, titolo 19.2 della procedura penale del codice della Virginia.

3.1.1.2 *Ulteriore utilizzo delle informazioni raccolte*

(101) Per quanto concerne l'utilizzo ulteriore dei dati raccolti dalle autorità federali di contrasto in materia penale, leggi, orientamenti e norme diversi impongono garanzie specifiche. Fatta eccezione per gli strumenti specifici applicabili alle attività dell'FBI (AGG-DOM e Guida alle indagini e operazioni dell'FBI all'interno degli USA), i requisiti di cui alla presente sezione si applicano in generale all'ulteriore utilizzo dei dati da parte di qualsiasi autorità federale, compresi i dati a cui tali autorità hanno accesso per finalità civili o normative. Figurano in tale contesto i requisiti derivanti da note/normative dell'Office of Management and Budget (OMB, Ufficio per la gestione e il bilancio), dalla Federal Information Security Management Modernization Act (legge federale di modernizzazione della gestione della sicurezza delle informazioni), dall'E-Government Act (legge sull'e-Government) e dalla Federal Records Act (legge federale sulle registrazioni).

(102) Conformemente all'autorità conferita dalla legge Clinger-Cohen (P.L. 104-106, divisione E) e dalla legge sulla sicurezza informatica del 1987 (P.L. 100-235), l'OMB ha emanato la circolare n. A-130 per stabilire orientamenti generali vincolanti che si applicano a tutti gli enti federali (comprese le autorità di contrasto) quando trattano informazioni che consentono l'identificazione personale ([175]). In particolare, la circolare impone a tutti gli enti federali di limitare la creazione, la raccolta, l'uso, il trattamento, l'archiviazione, la manutenzione, la diffusione e la divulgazione di informazioni che consentono l'identificazione personale a quelle legalmente autorizzate, pertinenti e ragionevolmente ritenute necessarie per il corretto svolgimento delle funzioni di ente autorizzato ([176]). Inoltre, nella misura ragionevolmente praticabile, gli enti federali devono garantire che le informazioni che consentono l'identificazione personale siano accurate, pertinenti, tempestive e complete e ridotte al minimo necessario per il corretto svolgimento delle funzioni di un ente. Più in generale, gli enti federali devono istituire un programma globale in materia di tutela della vita privata al fine di garantire il rispetto dei requisiti applicabili in tale contesto, sviluppare e valutare le politiche della privacy e gestire i rischi per la vita privata; mantenere procedure per individuare, documentare e segnalare eventuali casi di non conformità in materia di tutela della vita privata; sviluppare programmi di sensibilizzazione in materia di tutela della vita privata e di formazione per i dipendenti e i contraenti; nonché mettere in atto politiche e procedure per garantire che il personale sia ritenuto responsabile del rispetto dei requisiti e delle politiche in materia di tutela della vita privata ([177]).

(103) Inoltre la legge sull'e-Government ([178]) impone a tutti gli enti federali (comprese le autorità di contrasto in materia penale) di predisporre tutele in materia di sicurezza delle informazioni commisurate al rischio e all'entità del danno che deriverebbe dall'accesso, dall'uso, dalla divulgazione, dall'alterazione, dalla modifica o dalla distruzione non autorizzati; disporre di un *Chief Information Officer* (responsabile delle informazioni) incaricato di garantire il rispetto dei requisiti in materia di sicurezza delle informazioni e di provvedere allo svolgimento di una valutazione annuale indipendente (ad esempio da parte di un ispettore generale, cfr. considerando 109) del programma e delle pratiche di tali enti in materia di sicurezza delle informazioni ([179]). Analogamente la legge federale sulle registrazioni (FRA) ([180]) e i regolamenti supplementari ([181]) impongono che le informazioni detenute dagli enti federali siano soggette a garanzie che garantiscano l'integrità fisica delle informazioni e siano protette contro l'accesso non autorizzato.

(104) Conformemente all'autorità federale stabilita per legge, compresa la *Federal Information Security Modernisation Act* (legge federale sulla modernizzazione della sicurezza delle informazioni) del 2014, l'OMB e il *National Institute of Standards and Technology* (NIST, Istituto nazionale per le norme e la tecnologia) hanno elaborato norme vincolanti per gli enti federali (comprese le autorità di contrasto in materia penale) che specificano ulteriormente i requisiti minimi in materia di sicurezza delle informazioni che devono essere posti in essere, compresi i controlli degli accessi, la garanzia della sensibilizzazione e della formazione, la pianificazione di emergenze, la risposta agli incidenti, gli strumenti di verifica e di responsabilizzazione, la garanzia dell'integrità del sistema e delle informazioni, lo svolgimento di valutazioni dei rischi in materia di vita privata e la sicurezza, ecc. ([182]). Inoltre,

([175]) Ossia informazioni che possono essere utilizzate per distinguere o rintracciare l'identità di una persona, da sole o se combinate con altre informazioni collegate o collegabili a una determinata persona, cfr. circolare OMB n. A-130, pag. 33 (definizione di "informazioni che consentono l'identificazione personale").

([176]) Circolare dell'OMB n. A-130, *Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information*, 81 Fed. Reg. 49,689 (28 luglio 2016), pag. 17.

([177]) Appendice II, articolo 5, lettere da a) a h).

([178]) Codice degli Stati Uniti, titolo 44, capitolo 36.

([179]) Codice degli Stati Uniti, titolo 44, articoli 3544-3545.

([180]) FAC, codice degli Stati Uniti, titolo 44, articolo 3105.

([181]) Codice dei regolamenti federali, titolo 36, articolo 1228,150 e seguenti e articolo 1228,228 e appendice A.

([182]) Cfr. ad esempio la circolare n. A-130 dell'OMB; NIST SP 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organisations* (10 dicembre 2020); e le norme federali in materia di trattamento delle informazioni FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*.

conformemente agli orientamenti dell'OMB, tutti gli enti federali (comprese le autorità di contrasto in materia penale) devono mantenere e attuare un piano per il trattamento delle violazioni dei dati, anche per quanto riguarda la risposta a tali violazioni e la valutazione dei rischi di danno ([183]).

(105) Per quanto riguarda la conservazione dei dati, la legge federale sulle registrazioni ([184]) impone agli enti federali statunitensi (comprese le autorità di contrasto in materia penale) di stabilire periodi di conservazione per le loro registrazioni (alla scadenza dei quali tali registrazioni devono essere smaltite), che devono essere approvati dalla *National Archives and Record Administration* ([185]) (NARA, agenzia nazionale per l'amministrazione di archivi e registrazioni). La durata di tale periodo di conservazione è fissata alla luce di diversi fattori, quali il tipo di indagine, l'eventualità che le prove siano comunque pertinenti per l'indagine, ecc. Per quanto concerne l'FBI, il documento AGG-DOM prevede che l'FBI debba disporre di un piano di conservazione delle registrazioni e mantenere un sistema in grado di recuperare tempestivamente lo status e le basi per le indagini.

(106) Infine la circolare n. A-130 dell'OMB contiene altresì alcuni requisiti per la diffusione di informazioni che consentono l'identificazione personale. In linea di principio, la diffusione e la divulgazione di informazioni che consentono l'identificazione personale deve essere limitata a quanto legalmente autorizzato, pertinente e ragionevolmente ritenuto necessario per il corretto svolgimento delle funzioni di un ente ([186]). Quando condividono informazioni che consentono l'identificazione personale con altri soggetti, gli enti pubblici federali statunitensi devono imporre, ove pertinente, condizioni (compresa l'attuazione di controlli specifici in materia di sicurezza e tutela della vita privata) che disciplinano il trattamento delle informazioni mediante accordi scritti (compresi contratti, accordi sull'uso dei dati, accordi sullo scambio di informazioni e protocolli d'intesa) ([187]). Per quanto concerne i motivi in base ai quali le informazioni possono essere diffuse, il documento AGG-DOM e la guida alle indagini e operazioni dell'FBI all'interno degli USA ([188]) prevedono fra l'altro che l'FBI possa essere tenuto per legge a procedere in tal senso (ad esempio nel quadro di un accordo internazionale) o sia autorizzato a divulgare informazioni in determinate circostanze, ad esempio: ad altri enti statunitensi qualora la divulgazione sia compatibile con la finalità per la quale le informazioni sono state raccolte e sia connessa alle loro responsabilità; alle commissioni del Congresso; ad enti stranieri, se le informazioni sono connesse alle loro responsabilità e se la diffusione è coerente con gli interessi degli Stati Uniti, in particolare se la diffusione è necessaria per tutelare l'incolumità o la sicurezza di persone o beni oppure per fornire protezione nei confronti di un reato o di una minaccia per la sicurezza nazionale o per prevenire tali reati o minacce e la divulgazione è coerente con la finalità per la quale le informazioni sono state raccolte ([189]).

3.1.2 ***Vigilanza***

(107) Le attività degli enti federali di contrasto in materia penale sono soggette a vigilanza da parte di diversi organismi ([190]). Come illustrato ai considerando da 92 a 99, nella maggior parte dei casi in tale contesto figurano una vigilanza preventiva da parte della magistratura, che deve autorizzare singole misure di raccolta prima che vi si possa fare ricorso. Inoltre altri enti vigilano sulle diverse fasi delle attività delle autorità di contrasto in materia penale, compresi la raccolta e il trattamento di dati personali. Congiuntamente tali organi giudiziari e non giudiziari garantiscono che le autorità di contrasto siano soggette a una vigilanza indipendente.

([183]) Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, disponibile all'indirizzo: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf e circolare n. A-130 dell'OMB. Ad esempio le procedure di risposta alle violazioni dei dati da parte del Dipartimento della Giustizia, *cfr.* https://www.justice.gov/file/4336/download.

([184]) Legge federale sulle registrazioni, codice degli Stati Uniti, titolo 44, articoli 3101 e seguenti.

([185]) La NARA ha la facoltà di valutare le pratiche di gestione delle registrazioni degli enti e può stabilire se sia giustificata la prosecuzione della conservazione di determinate registrazioni (codice degli Stati Uniti, titolo 44, articolo 2904, lettera c) e articolo 2906).

([186]) Circolare n. A-130 dell'OMB, sezione 5, lettera f), punto 1, lettera d).

([187]) Circolare n. A-130 dell'OMB, appendice I, punto 3, lettera d).

([188]) Cfr. anche la guida alle indagini e operazioni dell'FBI all'interno degli USA (DIOG), sezione 14.

([189]) AGG-DOM, sezione VI, lettere B e C; guida alle indagini e operazioni dell'FBI all'interno (DIOG), sezione 14.

([190]) I meccanismi menzionati nella presente sezione si applicano anche alla raccolta e all'uso dei dati da parte delle autorità federali per finalità civili e normative. Gli enti federali civili e di regolamentazione sono soggetti al controllo da parte dei rispettivi ispettori generali e al controllo del Congresso, anche da parte del *Government Accountability Office* (Ufficio governativo per la responsabilizzazione), l'ente di audit e investigativo del Congresso. Fatto salvo il caso in cui tale ente abbia designato un addetto alla tutela della vita privata e alle libertà civili, un ruolo solitamente presente presso enti quali il Dipartimento della Giustizia e il Dipartimento della Sicurezza interna (DHS) in ragione delle loro competenze in materia di contrasto e di sicurezza nazionale, tali compiti spettano al funzionario senior dell'ente competente per la tutela della vita privata (SAOP, *Senior Agency Official for Privacy*). Tutti gli enti federali sono giuridicamente obbligati a designare un tale funzionario, il quale è competente per la garanzia del rispetto da parte dell'ente delle leggi in materia di tutela della vita privata e per le attività di vigilanza sulle questioni correlate. Cfr. ad esempio OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (2016).

(108) Innanzitutto, in seno a svariati dipartimenti aventi responsabilità in materia di contrasto penale sono presenti addetti alla tutela della vita privata e alle libertà civili ([191]). Benché i poteri precisi di tali addetti possano variare leggermente in funzione dell'atto costitutivo, in ciascun caso è compresa tipicamente la vigilanza sulle procedure, per assicurare che il dipartimento/l'ente corrispondente tenga adeguatamente conto degli aspetti inerenti alla vita privata e alle libertà civili e abbia predisposto procedure adeguate per trattare i reclami sporti dalle persone che denunciano una violazione della loro vita privata o delle loro libertà civili. I capi di ciascun dipartimento o ente devono garantire che gli addetti alla tutela della vita privata e alle libertà civili dispongano dei materiali e delle risorse necessari per adempiere il loro mandato, abbiano accesso a tutto il materiale e al personale necessari per lo svolgimento delle loro funzioni, siano informati e consultati in merito alle modifiche politiche proposte ([192]). Gli addetti alla tutela della vita privata e alle libertà civili riferiscono periodicamente al Congresso, 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 ([193]).

(109) In secondo luogo, un ispettore generale indipendente supervisiona le attività del Dipartimento della Giustizia, compreso l'FBI ([194]). Gli ispettori generali sono giuridicamente indipendenti ([195]) e sono competenti per lo svolgimento di indagini, verifiche e ispezioni indipendenti dei programmi e delle operazioni di tale dipartimento. Sono autorizzati ad accedere a tutti i dati, le relazioni, le verifiche, gli esami, i documenti, le carte, le raccomandazioni o altro materiale pertinente, se necessario mediante l'emanazione di una citazione, e possono assumere testimonianze ([196]). Sebbene gli ispettori generali formulino soltanto raccomandazioni non vincolanti di azioni correttive, le relazioni che redigono, anche sugli interventi con cui vi si è dato seguito (o sull'assenza di tali interventi) ([197]), sono in genere rese pubbliche e trasmesse al Congresso, che su tale base può esercitare la sua funzione di vigilanza (cfr. considerando 111) ([198]).

([191]) Cfr. codice degli Stati Uniti, titolo 42, articolo 2000ee-1. Rientrano in tale contesto ad esempio il Dipartimento della Giustizia, il Dipartimento della Sicurezza interna e l'FBI. In seno al Dipartimento della Sicurezza interna, inoltre, un responsabile capo della tutela della vita privata è competente per la tutela e il rafforzamento delle tutele della vita privata e della promozione della trasparenza all'interno di tale dipartimento (Codice degli Stati Uniti, titolo 6, articoli 142 e 222). Tutti i sistemi, le tecnologie, i moduli e i programmi del Dipartimento della Sicurezza interna che raccolgono dati personali o incidono sulla vita privata sono soggetti alla vigilanza da parte del responsabile capo della tutela della vita privata, che ha accesso a tutti i dati, le relazioni, le verifiche, gli esami, i documenti, le carte, le raccomandazioni o altro materiale a diposizione di tale dipartimento, se necessario mediante l'emanazione di una citazione. Il responsabile della tutela della vita privata deve riferire annualmente al Congresso in merito alle attività del Dipartimento che incidono sulla vita privata, nonché sui reclami relativi a violazioni della vita privata.

([192]) Codice degli Stati Uniti, titolo 42, articolo 2000ee-1, lettera d).

([193]) Cfr. codice degli Stati Uniti, titolo 42, articolo 2000ee-1, lettera f), punti da 1) a 2). Ad esempio, dalla relazione dell'addetto capo alla tutela della vita privata e alle libertà civili del Dipartimento della Giustizia e dell'Ufficio per la tutela della vita privata e le libertà civili relativa al periodo ottobre 2020-marzo 2021 emerge che sono stati effettuati 389 esami della vita privata, anche in merito a sistemi informatici e altri programmi (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Analogamente, la legge sulla sicurezza interna del 2002 ha istituito un Ufficio dell'Ispettore generale presso il Dipartimento della sicurezza interna.

([195]) Gli ispettori generali sono nominati a tempo indeterminato e possono essere rimossi dall'incarico solo dal presidente, il quale deve comunicare per iscritto al Congresso i motivi della destituzione.

([196]) Cfr. legge sugli ispettori generali del 1978, articolo 6.

([197]) Cfr. a questo proposito, ad esempio, la panoramica elaborata dall'Ufficio dell'ispettore generale del Dipartimento della Giustizia in merito alle raccomandazioni formulate e alla misura in cui sono state attuate mediante azioni di seguito da parte dei dipartimenti e degli enti (https://oig.justice.gov/sites/default/files/reports/22-043.pdf).

([198]) Cfr. legge sugli ispettori generali del 1978, articolo 4, paragrafo 5, e articolo 5. Ad esempio, l'Ufficio dell'ispettore generale presso il Dipartimento della Giustizia ha pubblicato di recente la sua relazione semestrale al Congresso (1º ottobre 2021-31 marzo 2022, https://oig.justice.gov/node/23596), che fornisce una panoramica delle verifiche, delle valutazioni, delle ispezioni, degli esami speciali e delle indagini da esso condotti in merito ai programmi e alle operazioni del Dipartimento della Giustizia. Tali attività hanno compreso un'indagine di un ex contraente in merito alla divulgazione illecita di una sorveglianza elettronica (intercettazione di una persona) in un'indagine in corso, che ha portato alla condanna del contraente. L'Ufficio dell'ispettore generale ha inoltre condotto un'indagine sui programmi e sulle prassi in materia di sicurezza delle informazioni degli enti facenti capo al Dipartimento della Giustizia, che ha compreso la verifica dell'efficacia delle politiche, delle procedure e delle prassi in materia di sicurezza delle informazioni di un sottoinsieme rappresentativo di sistemi di tali enti.

(110) In terzo luogo, nella misura in cui svolgono attività antiterrorismo, i dipartimenti aventi competenze in termini di contrasto in materia penale sono soggetti a vigilanza da parte dell'Autorità per la tutela della vita privata e delle libertà civili (PCLOB, *Privacy and Civil Liberties Oversight Board*), un ente indipendente all'interno del ramo esecutivo composto da cinque membri provenienti dai ranghi di entrambi i partiti, nominati dal presidente per un mandato fisso di sei anni previa approvazione da parte del Senato ([199]). Ai sensi della legge che istituisce tale ente, alla PCLOB sono attribuite competenze nel settore delle politiche antiterrorismo e della loro attuazione, al fine di tutelare la vita privata e le libertà civili. Nel contesto delle sue attività di controllo, tale autorità ha facoltà di accedere a tutti i dati, le relazioni, le verifiche, i documenti, le carte e le raccomandazioni dell'ente interessato, comprese le informazioni classificate, di procedere a interrogatori e di assumere testimonianze ([200]). Riceve le relazioni trasmesse dagli addetti alla tutela della vita privata e alle libertà civili di vari dipartimenti/enti federali ([201]), può rivolgere raccomandazioni al governo e alle autorità di contrasto e riferisce periodicamente alle commissioni del Congresso e al presidente ([202]). Le relazioni della PCLOB, comprese quelle presentate al Congresso, devono essere messe a disposizione del pubblico nella misura più ampia possibile ([203]).

(111) Infine le attività di contrasto in materia penale sono soggette a vigilanza da parte di commissioni specifiche in seno al Congresso degli Stati Uniti (le commissioni Giustizia della Camera dei rappresentanti e del Senato). Le commissioni Giustizia esercitano una vigilanza regolare in vari modi, in particolare attraverso audizioni, indagini, riesami e relazioni ([204]).

3.1.3 ***Mezzi di ricorso***

(112) Come indicato, nella maggior parte dei casi le autorità di contrasto in materia penale devono ottenere un'autorizzazione giudiziaria preventiva per raccogliere dati personali. Sebbene ciò non sia necessario per le citazioni amministrative, queste sono limitate a situazioni specifiche e saranno soggette a un sindacato giurisdizionale indipendente almeno nei casi in cui il governo chieda l'esecuzione per via giudiziaria. In particolare i destinatari di citazioni amministrative possono contestarle dinanzi al giudice in quanto irragionevoli, vale a dire eccessivamente ampie o vessatorie o eccessivamente gravose ([205]).

(113) Le persone possono innanzitutto presentare richieste o reclami presso le autorità di contrasto in materia penale in merito al trattamento dei loro dati personali. Rientra in tale contesto la possibilità di richiedere l'accesso ai dati personali e la loro rettifica ([206]). Per quanto concerne le attività di contrasto del terrorismo, le persone possono altresì promuovere un reclamo presso gli addetti alla tutela della vita privata e alle libertà civili (o ad altri funzionari preposti alla tutela della vita privata) in seno alle autorità di contrasto ([207]).

(114) 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 ([208]). Fatto salvo il soddisfacimento delle condizioni applicabili, queste vie di ricorso, che comprendono in particolare la legge sulle procedure amministrative, la legge sulla libertà di informazione (FOIA) e legge sulla privacy nelle comunicazioni elettroniche (ECPA), sono aperte a tutti, indipendentemente dalla cittadinanza.

([199]) I membri della PCLOB devono essere selezionati unicamente sulla base delle loro qualifiche professionali, dei risultati da loro conseguiti, della loro reputazione pubblica, delle loro competenze in materia di libertà civili e tutela della vita privata e della loro esperienza pertinente, senza tener conto dell'appartenenza politica. In nessun caso vi possono essere più di tre membri di tale ente appartenenti al medesimo partito politico. Durante il periodo del suo incarico, una persona nominata a membro della PCLOB non può essere un funzionario eletto, un funzionario o un dipendente del governo federale, se non in qualità di membro della PCLOB. Cfr. Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera h).

([200]) Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera g).

([201]) Cfr. codice degli Stati Uniti, titolo 42, articolo 2000ee-1, lettera f), punto 1), lettera A), punto iii). Tra questi figurano almeno il Dipartimento della Giustizia, il Dipartimento della Difesa, il Dipartimento della Sicurezza interna, cui si aggiungono tutti gli altri dipartimenti, enti o servizi dell'esecutivo che la PCLOB ha ritenuto opportuno contemplare.

([202]) Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera e).

([203]) Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera f).

([204]) Ad esempio le commissioni organizzano audizioni tematiche (cfr. ad esempio un'audizione recente della commissione Giustizia della Camera dei rappresentanti sulle "retate digitali", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), nonché audizioni periodiche di vigilanza, ad esempio dell'FBI e del Dipartimento della Giustizia, cfr. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 e https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) Cfr. allegato VI.

([206]) Circolare n. A-130 dell'OMB, appendice II, sezione 3, lettere a) e f), che impone agli enti federali di garantire un accesso e una rettifica adeguati su richiesta delle persone, nonché di stabilire procedure per ricevere e trattare reclami e richieste in materia di tutela della vita privata.

([207]) Cfr. Codice degli Stati Uniti, titolo 42, articolo 2000ee-1 per quanto concerne, ad esempio, il Dipartimento della Giustizia e il Dipartimento della Sicurezza interna. Cfr. anche il memorandum M-16-24 dell'OMB, *Role and Designation of Senior Agency Officials for Privacy*.

([208]) I meccanismi di ricorso menzionati nella presente sezione si applicano anche alla raccolta e all'uso dei dati da parte delle autorità federali per finalità civili e normative.

(115) In generale, a norma delle disposizioni sul sindacato giurisdizionale previste dalla legge sulle procedure amministrative ([209]), chiunque subisca un illecito, un inconveniente o un torto a causa dell'azione di un ente pubblico ha diritto di ricorrere al sindacato giurisdizionale ([210]), 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 ([211]).

(116) Più precisamente, instaurando un sistema di diritti alla privacy sanciti per legge, il titolo II della legge sulla privacy nelle comunicazioni elettroniche ([212]) disciplina l'accesso ai contenuti delle comunicazioni orali, via cavo o elettroniche conservati da terzi prestatori di servizi ([213]). 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.

(117) 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 ([214]), legge sulle frodi e gli abusi informatici ([215]), legge federale sulle rivendicazioni per fatti illeciti ([216]), legge sul diritto alla privacy finanziaria ([217]) e legge sull'informativa corretta nel credito ([218]).

([209]) Codice degli Stati Uniti, titolo 5, articolo 702.

([210]) 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, titolo 5, articolo 704).

([211]) Codice degli Stati Uniti, titolo 5, articolo 706, punto 2), lettera A).

([212]) Codice degli Stati Uniti, titolo 18, articoli 2701-2712.

([213]) 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.

([214]) Codice degli Stati Uniti, titolo 18, articolo 2510 e seguenti. A norma della legge sulle intercettazioni (codice degli Stati Uniti, 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. Per la raccolta di 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, titolo 18, articoli 3121-3127 e, per l'azione civile, articolo 2707).

([215]) Codice degli Stati Uniti, 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.

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

([217]) Codice degli Stati Uniti, titolo 12, articolo 3401 e seguenti. A norma della legge sul diritto alla privacy finanziaria, in talune circostanze la persona può intentare contro gli Stati Uniti 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.

([218]) Codice degli Stati Uniti, 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.

(118) Inoltre, ai sensi della legge sulla libertà d'informazione, Codice degli Stati Uniti, titolo 5, articolo 552, chiunque ha il diritto di chiedere l'accesso alle registrazioni esistenti degli enti federali, anche se queste contengono dati personali ([219]). Una volta esperiti i mezzi di ricorso amministrativi, una persona fisica può invocare tale diritto di accesso adendo un organo giurisdizionale, fatto salvo il caso in cui le registrazioni in questione siano protette contro la divulgazione pubblica mediante un'esenzione o un'esclusione speciale per finalità di contrasto ([220]). In questo caso, l'organo giurisdizionale valuterà se un'eventuale esenzione si applichi o sia stata legittimamente invocata dall'autorità pubblica pertinente.

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

(119) Il diritto statunitense contempla varie limitazioni e garanzie in relazione all'accesso e all'uso di dati personali per finalità di sicurezza nazionale e prevede meccanismi di vigilanza e ricorso in questo settore che sono in linea con i requisiti di cui al considerando 89 della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono.

3.2.1 ***Basi giuridiche, limitazioni e garanzie***

3.2.1.1 *Quadro giuridico applicabile*

(120) I dati personali trasferiti dall'Unione alle organizzazioni del DPF UE-USA possono essere raccolti dalle autorità statunitensi per finalità di sicurezza nazionale sulla base di diversi strumenti giuridici, fatte salve condizioni e garanzie specifiche.

(121) Una volta che i dati personali sono stati ricevuti da organizzazioni situate negli Stati Uniti, gli enti di intelligence statunitensi possono chiedere l'accesso a tali dati per finalità di sicurezza nazionale soltanto nella misura consentita da leggi in vigore, in particolare ai sensi della legge relativa alla vigilanza sull'intelligence esterna (FISA) o di disposizioni di legge che autorizzano l'accesso attraverso cosiddette *National Security Letter* (NSL) ([221]). La FISA contiene diverse basi giuridiche che possono essere utilizzate per raccogliere (e successivamente trattare) dati personali di interessati dell'Unione trasferiti nell'ambito del DPF UE-USA (articolo 105 ([222]), articolo 302 ([223]), articolo 402 ([224]), articolo 501 ([225]) e articolo 702 ([226]) di detta legge), come descritto più dettagliatamente nei considerando da 142 a 152.

([219]) Codice degli Stati Uniti, titolo 5, articolo 552.

([220]) Tali esclusioni sono tuttavia circoscritte. A norma del codice degli Stati Uniti, titolo 5, articolo 552, lettera b), punto 7), i diritti conferiti dalla legge sulla libertà d'informazione sono preclusi per i dati o le informazioni raccolti 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, titolo 5, articolo 552, lettera c), punto 1)).

([221]) Codice degli Stati Uniti, titolo 12, articolo 3414; titolo 15, articoli 1681u-1681v; e titolo 18, articolo 2709. Cfr. considerando 153.

([222]) Codice degli Stati Uniti, titolo 50, articolo 1804, che riguarda la sorveglianza elettronica tradizionale individualizzata.

([223]) Codice degli Stati Uniti, titolo 50, articolo 1822, che riguarda le perquisizioni fisiche per finalità di intelligence esterna.

([224]) Codice degli Stati Uniti, titolo 50, articolo 1842, in combinato disposto con l'articolo 1841, punto 2), e con il titolo 18, articolo 3127, concernenti l'installazione di dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita.

([225]) Codice degli Stati Uniti, titolo 50, articolo 1861, che consente all'FBI di presentare una domanda per l'ottenimento di un'ordinanza che autorizzi un vettore comune, una struttura ricettiva pubblica, una struttura di immagazzinamento fisico o una struttura di noleggio veicoli a rilasciare i dati in suo possesso ai fini di un'indagine volta a raccogliere informazioni di intelligence esterna, o di un'indagine riguardante il terrorismo internazionale.

([226]) Codice degli Stati Uniti, titolo 50, articolo 1881a, che consente ai servizi della comunità dell'intelligence statunitense di chiedere a imprese statunitensi l'accesso a informazioni, compreso il contenuto di comunicazioni internet, rivolte a determinate persone non statunitensi al di fuori degli Stati Uniti con l'assistenza giuridicamente obbligatoria di prestatori di servizi di comunicazione elettronica.

(122) Gli enti di intelligence statunitensi hanno altresì la possibilità di raccogliere dati personali al di fuori degli Stati Uniti, che possono includere dati personali in transito tra l'Unione e gli Stati Uniti. La raccolta al di fuori degli Stati Uniti si basa sul decreto presidenziale 12333 ([227]), emesso dal presidente ([228]).

(123) La raccolta di intelligence dei segnali è la forma di raccolta di intelligence più pertinente per il presente accertamento dell'adeguatezza, in quanto riguarda la raccolta di comunicazioni elettroniche e dati da sistemi informatici. Tale raccolta può essere effettuata dagli enti di intelligence statunitensi sia all'interno degli Stati Uniti (sulla base della FISA) sia durante il transito dei dati verso gli Stati Uniti (sulla base del decreto presidenziale 12333).

(124) Il 7 ottobre 2022 il presidente degli Stati Uniti ha emesso il decreto presidenziale 14086 sul miglioramento delle garanzie per le attività di intelligence dei segnali degli Stati Uniti, che stabilisce limitazioni e garanzie per tutte le attività di intelligence dei segnali statunitensi. Tale decreto presidenziale sostituisce in larga misura la direttiva presidenziale 28 (PPD-28) ([229]) rafforza le condizioni, le limitazioni e le garanzie che si applicano a tutte le attività di intelligence dei segnali (ossia ai sensi della FISA e del decreto presidenziale 12333), indipendentemente dal luogo in cui si svolgono ([230]), e istituisce un nuovo meccanismo di ricorso attraverso il quale tali garanzie possono essere invocate e applicate dalle persone ([231]) (cfr. più in dettaglio i considerando da 176 a 194). Nel procedere in tal senso attua nel diritto statunitense l'esito dei colloqui che hanno avuto luogo tra l'UE e gli Stati Uniti a seguito dell'invalidamento da parte della Corte di giustizia della decisione di adeguatezza della Commissione sullo scudo per la privacy (cfr. considerando 6). Si tratta pertanto di un aspetto particolarmente importante del quadro giuridico valutato nel contesto della presente decisione.

(125) Le limitazioni e le garanzie introdotte dal decreto presidenziale 14086 integrano quelle previste dall'articolo 702 FISA e dal decreto presidenziale 12333. I requisiti descritti di seguito (nelle sezioni 3.2.1.2 e 3.2.1.3) devono essere applicati dagli enti di intelligence quando svolgono attività di intelligence dei segnali ai sensi dell'articolo 702 FISA e del decreto presidenziale 12333, ad esempio nel contesto della selezione/dell'identificazione delle categorie di informazioni di intelligence esterna da acquisire a norma dell'articolo 702 FISA; della raccolta di intelligence esterna o di attività di controspionaggio ai sensi del decreto presidenziale 12333; e dell'adozione di singole decisioni che individuano obiettivi prioritari ai sensi dell'articolo 702 FISA e del decreto presidenziale 12333.

(126) I requisiti previsti da tale decreto presidenziale emanato dal presidente sono vincolanti per l'intera comunità dell'intelligence e devono essere ulteriormente attuati attraverso politiche e procedure degli enti che le traducano in indicazioni concrete per le operazioni quotidiane. A questo proposito, il decreto presidenziale 14086 concede agli enti di intelligence statunitensi un anno al massimo per aggiornare le politiche e le procedure esistenti (ossia entro il 7 ottobre 2023) per renderle conformi ai requisiti di tale decreto presidenziale. Tali politiche e procedure aggiornate devono essere elaborate in consultazione con il Procuratore generale, l'addetto alla tutela della vita privata e alle libertà civili (CLPO) dell'Ufficio del direttore dell'intelligence nazionale (ODNI) e la PCLOB, un organo di vigilanza indipendente autorizzato a riesaminare le politiche dell'esecutivo e la loro attuazione, al fine di tutelare la vita privata e le libertà civili (cfr. considerando 110 per quanto concerne il ruolo e lo status della PCLOB), e a rendere pubblici tali riesami ([232]). Inoltre, una volta messe in atto le politiche e le procedure aggiornate, la PCLOB effettuerà

([227]) Decreto presidenziale 12333: *United States Intelligence Activities*, Registro federale vol. 40, n. 235 (8 dicembre 1981, come modificato il 30 luglio 2008). Il decreto presidenziale 12333 definisce in generale 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.

([228]) Ai sensi dell'articolo II della costituzione degli Stati Uniti, la competenza per garantire la sicurezza nazionale, compresa in particolare la raccolta di intelligence esterna, spetta all'autorità del presidente in veste di comandante in capo delle forze armate.

([229]) Il decreto presidenziale 14086 sostituisce una precedente direttiva presidenziale, la PPD-28, fatta eccezione per l'articolo 3 e un allegato integrativo (che impone agli enti di intelligence di riesaminare annualmente le loro priorità e i loro requisiti in materia di intelligence dei segnali, tenendo conto dei vantaggi delle attività di intelligence dei segnali per gli interessi nazionali degli Stati Uniti, nonché del rischio posto da tali attività) e l'articolo 6 (che contiene disposizioni generali) - cfr. documento *National Security Memorandum on Partial Revocation of President Policy Directive 28*, disponibile all'indirizzo: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Cfr. articolo 5, lettera f), del decreto presidenziale 14086, che spiega che tale atto ha il medesimo ambito di applicazione della direttiva presidenziale 28, che, ai sensi della nota 3 di tale direttiva, si applicava alle attività di intelligence dei segnali svolte al fine di raccogliere comunicazioni o informazioni in merito a comunicazioni, fatta eccezione per le attività di intelligence dei segnali intraprese per sottoporre a prova o sviluppare capacità di intelligence dei segnali.

([231]) Cfr. al riguardo, ad esempio, l'articolo 5, lettera h), del decreto presidenziale 14086, che chiarisce che le garanzie contenute in detto decreto creano un diritto legale e possono essere applicate dai singoli attraverso il meccanismo di ricorso.

([232]) Cfr. articolo 2, lettera c), punto iv), lettera C), del decreto presidenziale 14086.

un riesame per garantirne la coerenza rispetto al decreto presidenziale. Entro 180 giorni dal completamento di tale riesame da parte della PCLOB, ogni ente di intelligence deve esaminare attentamente e attuare o comunque dare seguito a tutte le raccomandazioni formulate dalla PCLOB. Il 3 luglio 2023 il governo degli Stati Uniti ha pubblicato tali politiche e procedure ([233]).

3.2.1.2 *Limitazioni e garanzie per quanto riguarda la raccolta di dati personali per finalità di sicurezza nazionale*

(127) Il decreto presidenziale 14086 stabilisce una serie di requisiti generali che si applicano a tutte le attività di intelligence dei segnali (raccolta, uso, diffusione, ecc. di dati personali).

(128) Innanzitutto, tali attività devono essere basate su una legge o un'autorizzazione presidenziale e devono essere svolte nel rispetto del diritto statunitense, compresa la costituzione ([234]).

(129) In secondo luogo, devono essere messe in atto garanzie adeguate volte ad assicurare che la vita privata e le libertà civili siano parte integrante della pianificazione di tali attività ([235]).

(130) In particolare, qualsiasi attività di intelligence dei segnali può essere svolta soltanto dopo aver accertato, sulla base di una valutazione ragionevole di tutti i fattori pertinenti, che tali attività sono necessarie per far progredire una priorità convalidata dell'intelligence (per quanto concerne la nozione di "priorità convalidata dell'intelligence", cfr. considerando 135) ([236]).

(131) Inoltre tali attività possono essere condotte soltanto in misura e in modo proporzionati alla priorità convalidata dell'intelligence per la quale sono state autorizzate ([237]). In altre parole, occorre trovare un giusto equilibrio tra l'importanza della priorità di intelligence perseguita e l'impatto sulla vita privata e sulle libertà civili delle persone interessate, indipendentemente dalla loro cittadinanza o dal loro luogo di residenza ([238]).

(132) Infine, per garantire il rispetto di tali requisiti generali, che rispecchiano i principi di legalità, necessità e proporzionalità, le attività di intelligence dei segnali sono soggette a vigilanza (cfr. più in dettaglio la sezione 3.2.2) ([239]).

(133) Tali requisiti generali sono ulteriormente corroborati per quanto concerne la raccolta dell'intelligence dei segnali attraverso una serie di condizioni e limitazioni che garantiscono che l'ingerenza nei diritti delle persone sia limitata a quanto necessario e proporzionato ai fini del conseguimento di un obiettivo legittimo.

(134) Innanzitutto, il decreto presidenziale limita in due modi i motivi per cui i dati possono essere raccolti nel contesto di attività di intelligence dei segnali. Da un lato, il decreto presidenziale stabilisce gli obiettivi legittimi che possono essere perseguiti dalla raccolta di intelligence dei segnali, ad esempio comprendere o valutare le capacità, le intenzioni o le attività di organizzazioni straniere, comprese le organizzazioni terroristiche internazionali, che rappresentano una minaccia corrente o potenziale per la sicurezza nazionale degli Stati Uniti; fornire protezione nei confronti di capacità e attività militari straniere; comprendere o valutare le minacce transnazionali che incidono sulla sicurezza globale, quali il clima e altri cambiamenti ecologici, i rischi per la salute pubblica e le minacce umanitarie ([240]). Dall'altro lato, il decreto presidenziale elenca alcuni obiettivi che non devono mai essere perseguiti

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Articolo 2, lettera a), punto i), del decreto presidenziale 14086.

([235]) Articolo 2, lettera a), punto ii), del decreto presidenziale 14086.

([236]) Articolo 2, lettera a), punto ii), lettera A), del decreto presidenziale 14086. Ciò non richiede sempre che l'intelligence dei segnali sia l'unico mezzo per far progredire gli aspetti di una priorità convalidata dell'intelligence. Ad esempio la raccolta di intelligence dei segnali può essere utilizzata per garantire percorsi alternativi per la convalida (ad esempio per corroborare informazioni ricevute da altre fonti di intelligence) o per mantenere un accesso affidabile alle stesse informazioni (articolo 2, lettera c), punto i), lettera A), del decreto presidenziale 14086).

([237]) Articolo 2, lettera a), punto ii), lettera B), del decreto presidenziale 14086.

([238]) Articolo 2, lettera a), punto ii), lettera B), del decreto presidenziale 14086.

([239]) Articolo 2, lettera a), punto iii), in combinato disposto con l'articolo 2, lettera d), del decreto presidenziale 14086.

([240]) Articolo 2, lettera b), punto i) del decreto presidenziale 14086. In ragione dell'elenco circoscritto di obiettivi legittimi di cui al decreto presidenziale, che non comprende eventuali minacce future, il decreto presidenziale prevede la possibilità per il presidente di aggiornare tale elenco qualora emergano nuovi imperativi di sicurezza nazionale, quali nuove minacce alla sicurezza nazionale. Tali aggiornamenti devono, in linea di principio, essere resi pubblici, fatto salvo il caso in cui il presidente ritenga che procedere a tale pubblicazione porrebbe di per sé un rischio per la sicurezza nazionale degli Stati Uniti (articolo 2, lettera b), punto i), lettera B), del decreto presidenziale 14086).

dalle attività di intelligence dei segnali, ad esempio la repressione della critica, del dissenso o della libera espressione di idee od opinioni politiche da parte delle persone o della stampa; la finalità di sfavorire persone per motivi di origine etnica, razza, genere, identità di genere, orientamento sessuale o religione o quella di offrire un vantaggio competitivo a imprese statunitensi ([241]).

(135) Gli obiettivi stabiliti nel decreto presidenziale 14086 non possono essere utilizzati dagli enti di intelligence stessi per giustificare la raccolta di intelligence dei segnali, ma devono essere ulteriormente concretizzati, per fini operativi, in priorità più concrete per le quali è possibile raccogliere intelligence dei segnali. In altre parole, la raccolta effettiva può avvenire soltanto al fine di far progredire una priorità più specifica. Tali priorità sono stabilite attraverso un processo specifico volto a garantire il rispetto dei requisiti giuridici applicabili, compresi quelli relativi alla vita privata e alle libertà civili. Più specificamente, le priorità in materia di intelligence sono elaborate innanzitutto dal direttore dell'intelligence nazionale (attraverso il cosiddetto quadro delle priorità nazionali in materia di intelligence) e sottoposte quindi all'approvazione da parte del presidente ([242]). Conformemente al decreto presidenziale 14086, prima di proporre al presidente priorità in materia di intelligence, il direttore deve ottenere dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI una valutazione per ciascuna priorità in merito all'eventualità o meno che la priorità in questione 1) persegua uno o più obiettivi legittimi di cui al decreto presidenziale; 2) non sia concepita né si prevede che dia luogo a una raccolta di intelligence dei segnali per uno degli obiettivi vietati di cui al decreto presidenziale; e 3) sia stata stabilita dopo un'adeguata considerazione della vita privata e delle libertà civili di tutte le persone, indipendentemente dalla loro cittadinanza o dal loro luogo di residenza ([243]). Nel caso in cui il direttore non sia d'accordo con la valutazione dell'addetto alla tutela della vita privata e alle libertà civili, entrambe le opinioni devono essere presentate al presidente ([244]).

(136) Di conseguenza tale processo garantisce in particolare che le considerazioni in materia di tutela della vita privata siano prese in considerazione sin dalla fase iniziale in cui vengono elaborate le priorità in materia di intelligence.

(137) In secondo luogo, una volta stabilita una priorità in materia di intelligence, la decisione di stabilire se e in quale misura l'intelligence dei segnali possa essere raccolta per promuovere tale priorità è disciplinata da una serie di requisiti. Tali requisiti rendono operative le norme generali in materia di necessità e proporzionalità di cui all'articolo 2, lettera a), del decreto presidenziale.

(138) In particolare l'intelligence dei segnali può essere raccolta soltanto dopo aver accertato, sulla base di una valutazione ragionevole di tutti i fattori pertinenti, che tale raccolta è necessaria per far progredire una specifica priorità in materia di intelligence ([245]). Nello stabilire se sia necessaria una specifica attività di raccolta di intelligence dei segnali per far progredire una priorità convalidata dell'intelligence, gli enti di intelligence statunitensi devono considerare la disponibilità, la fattibilità e l'adeguatezza di altre fonti e metodi meno intrusivi, compreso da fonti diplomatiche e pubbliche ([246]). Se disponibili, occorre dare priorità a tali fonti e metodi alternativi e meno intrusivi ([247]).

(139) Quando, nell'applicazione di tali criteri, la raccolta dell'intelligence dei segnali è ritenuta necessaria, essa deve essere quanto più possibile mirata e non deve incidere in modo sproporzionato sulla vita privata e sulle libertà civili ([248]). Al fine di garantire che la vita privata e le libertà civili non siano colpite in modo sproporzionato, ossia al fine di trovare un giusto equilibrio tra le esigenze di sicurezza nazionale e la tutela della vita privata e delle libertà civili, occorre tenere debitamente conto di tutti i fattori pertinenti, quali la natura dell'obiettivo perseguito; l'invasività dell'attività di raccolta, compresa la sua durata; il probabile contributo della raccolta all'obiettivo perseguito; le conseguenze ragionevolmente prevedibili per le persone; la natura e la sensibilità dei dati da raccogliere ([249]).

([241]) Articolo 2, lettera b), punto ii) del decreto presidenziale 14086.
([242]) Articolo 102A della legge sulla sicurezza nazionale (*National Security Act*) e articolo 2, lettera b), punto iii), del decreto presidenziale 14086.
([243]) In casi eccezionali (in particolare, quando tale processo non può essere svolto a causa della necessità di affrontare un requisito di intelligence nuovo o in evoluzione), tali priorità possono essere fissate direttamente dal presidente o dal capo di un servizio della comunità dell'intelligence, che in linea di principio deve applicare i medesimi criteri di cui all'articolo 2, lettera b), punto iii), lettera A), punti da 1) a 3) (cfr. articolo 4, lettera n), del decreto presidenziale 14086).
([244]) Articolo 2, lettera b), punto iii), lettera C), del decreto presidenziale 14086.
([245]) Articolo 2, lettere b) e c), punto i), lettera A), del decreto presidenziale 14086.
([246]) Articolo 2, lettera c), punto i), lettera A), del decreto presidenziale 14086.
([247]) Articolo 2, lettera c), punto i), lettera A), del decreto presidenziale 14086.
([248]) Articolo 2, lettera c), punto i), lettera B), del decreto presidenziale 14086.
([249]) Articolo 2, lettera c), punto i), lettera B), del decreto presidenziale 14086.

(140) Per quanto concerne il tipo di raccolta dell'intelligence dei segnali, la raccolta di dati all'interno degli Stati Uniti, che è la più pertinente per la presente constatazione di adeguatezza in quanto riguarda dati che sono stati trasferiti a organizzazioni negli Stati Uniti, deve sempre essere mirata, come spiegato più dettagliatamente nei considerando da 142 a 153.

(141) La "raccolta in blocco" ([250]) può essere svolta soltanto al di fuori degli Stati Uniti, sulla base del decreto presidenziale 12333. Anche in questo caso, ai sensi del decreto presidenziale 14086, deve essere data priorità alla raccolta mirata ([251]). Al contrario, la raccolta in blocco è consentita soltanto se le informazioni necessarie per far progredire una priorità convalidata dell'intelligence non possono essere ottenute ragionevolmente mediante una raccolta mirata ([252]). Quando è necessario effettuare una raccolta di dati in blocco al di fuori degli Stati Uniti, si applicano garanzie specifiche ai sensi del decreto presidenziale 14086 ([253]). Innanzitutto, devono essere applicati metodi e misure tecniche per limitare i dati raccolti a quanto necessario per far progredire una priorità convalidata dell'intelligence, riducendo al minimo la raccolta di informazioni non pertinenti ([254]). In secondo luogo, il decreto presidenziale limita l'uso delle informazioni raccolte in blocco (comprese le interrogazioni) a sei obiettivi specifici, tra cui la protezione contro il terrorismo, la presa di ostaggi e l'imprigionamento di persone da parte o per conto di un governo, un'organizzazione o una persona straniera; la protezione contro lo spionaggio straniero, il sabotaggio o l'assassinio; la protezione contro le minacce derivanti dallo sviluppo, dal possesso o dalla proliferazione di armi di distruzione di massa o di tecnologie e minacce correlate, ecc. ([255]). Infine qualsiasi interrogazione dell'intelligence dei segnali ottenuta in blocco può avvenire soltanto se necessario per far progredire una priorità convalidata dell'intelligence nel perseguimento dei sei obiettivi summenzionati e conformemente a politiche e procedure che tengano adeguatamente conto dell'impatto delle interrogazioni sulla vita privata e sulle libertà civili di tutte le persone, indipendentemente dalla loro cittadinanza o dal luogo di residenza ([256]).

(142) Oltre ai requisiti di cui al decreto presidenziale 14086, la raccolta di dati da parte dell'intelligence dei segnali trasferiti a un'organizzazione negli Stati Uniti è soggetta a limitazioni e garanzie specifiche disciplinate dall'articolo 702 FISA ([257]). L'articolo 702 FISA autorizza l'acquisizione, assistita obbligatoriamente da prestatori statunitensi di servizi di comunicazione elettronica, di informazioni di intelligence esterna ottenuta prendendo a obiettivo cittadini stranieri che si ritiene ragionevolmente siano situati al di fuori degli Stati Uniti ([258]). Al fine di raccogliere informazioni di intelligence esterna ai sensi dell'articolo 702 FISA, il Procuratore generale e il direttore

([250]) Ossia la raccolta di grandi quantità di intelligence dei segnali che, per motivi tecnici od operativi, viene acquisita senza l'impiego di discriminanti (ad esempio identificatori o selettori specifici) (cfr. articolo 4, lettera b), del decreto presidenziale 14086). Ai sensi del decreto presidenziale 14086 e come ulteriormente spiegato al considerando 141, la raccolta in blocco ai sensi del decreto presidenziale 12333 avviene soltanto quando necessario per promuovere specifiche priorità convalidate dell'intelligence ed è soggetta a una serie di limitazioni e garanzie volte a garantire che l'accesso ai dati non sia indiscriminato. La raccolta in blocco deve pertanto essere distinta da una raccolta effettuata su base generalizzata e indiscriminata ("sorveglianza di massa") senza limitazioni e garanzie.

([251]) Articolo 2, lettera c), punto ii), lettera A), del decreto presidenziale 14086.

([252]) Articolo 2, lettera c), punto ii), lettera A), del decreto presidenziale 14086.

([253]) Le norme specifiche in materia di raccolta in blocco di dati di cui al decreto presidenziale 14086 si applicano anche a un'attività di raccolta mirata di intelligence dei segnali che utilizza temporaneamente dati acquisiti senza discriminanti (ad esempio in assenza di una selezione specifica di termini o identificatori), ossia "in blocco" (che è possibile soltanto al di fuori del territorio degli Stati Uniti). Ciò non avviene quando tali dati sono utilizzati soltanto per sostenere la fase tecnica iniziale dell'attività di raccolta mirata di intelligence dei segnali, conservati soltanto per un breve periodo di tempo necessario per completare tale fase e cancellati immediatamente dopo (articolo 2, lettera c), punto ii), lettera D), del decreto presidenziale 14086). In tal caso l'unica finalità della raccolta iniziale priva di discriminanti è consentire una raccolta mirata di informazioni mediante l'applicazione di un identificatore o un selettore specifico. In tale scenario, soltanto i dati che rispondono all'applicazione di una determinata discriminante sono inseriti nelle banche dati governative, mentre i dati rimanenti vengono distrutti. Tale raccolta mirata resta pertanto disciplinata dalle norme generali che si applicano alla raccolta dell'intelligence dei segnali, compreso l'articolo 2, lettere a) e b) e lettera c), punto i), del decreto presidenziale 14086.

([254]) Articolo 2, lettera c), punto ii), lettera A), del decreto presidenziale 14086.

([255]) Articolo 2, lettera c), punto ii), lettera B), del decreto presidenziale 14086. Qualora emergano nuovi imperativi di sicurezza nazionale, quali nuove minacce alla sicurezza nazionale, il presidente può aggiornare tale elenco. Tali aggiornamenti devono, in linea di principio, essere resi pubblici, fatto salvo il caso in cui il presidente ritenga che procedere a tale pubblicazione porrebbe di per sé un rischio per la sicurezza nazionale degli Stati Uniti (articolo 2, lettera c), punto ii), lettera C), del decreto presidenziale 14086). Per quanto riguarda le interrogazioni dei dati raccolti in blocco, cfr. articolo 2, lettera c), punto iii), lettera D), decreto presidenziale 14086.

([256]) Articolo 2, lettera a), punto ii), lettera A), in combinato disposto con l'articolo 2, lettera c), punto iii), lettera D), del decreto presidenziale 14086. Cfr. anche allegato VII.

([257]) Codice degli Stati Uniti, titolo 50, articolo 1881.

([258]) Codice degli Stati Uniti, titolo 50, articolo 1881a, lettera a). In particolare, come osservato dall'Autorità per la tutela della vita privata e delle libertà civili, la sorveglianza a norma dell'articolo 702 si esplica totalmente in una concentrazione delle rilevazioni su determinate persone [straniere] selezionate su base personalizzata (PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 if the Foreign Intelligence Surveillance Act*, 2 luglio 2014, pag. 111) (in appresso: "relazione relativa all'articolo 702"). Cfr. anche NSA CLPO, *NSA's Implementation of Foreign Intelligence Act Section 702*, 16 aprile 2014. Il termine "prestatore di servizi di comunicazione elettronica" è definito nel Codice degli Stati Uniti, titolo 50, articolo 1881, lettera a), punto 4).

dell'intelligence nazionale presentano ogni anno alla Corte di vigilanza sull'intelligence esterna (Corte FISA) certificazioni che individuano le categorie di informazioni di intelligence esterna da acquisire ([259]). Tali certificazioni devono essere accompagnate da procedure di individuazione degli obiettivi, minimizzazione e interrogazione, approvate anche dalla Corte e giuridicamente vincolanti per gli enti di intelligence statunitensi.

(143) La Corte FISA è un organo giurisdizionale indipendente ([260]), istituito mediante legge federale, le cui decisioni possono essere impugnate dinanzi alla Corte di controllo della vigilanza sull'intelligence esterna (FISCR) ([261]) e, in ultima analisi, alla Corte suprema degli Stati Uniti ([262]). La Corte FISA (così come la FISCR) è coadiuvata da un comitato permanente formato da cinque avvocati e cinque esperti tecnici aventi competenze in materia di sicurezza nazionale e di libertà civili ([263]). 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 ([264]). Il sistema garantisce in particolare che la valutazione della Corte tenga adeguatamente conto degli aspetti inerenti alla tutela della vita privata. 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* ([265]).

(144) La Corte FISA riesamina le certificazioni e le relative procedure (in particolare le procedure di individuazione degli obiettivi e minimizzazione) per verificarne la conformità rispetto ai requisiti della FISA. Se detta Corte ritiene che i requisiti non siano soddisfatti, può negare la certificazione in toto o in parte e richiedere la modifica delle procedure ([266]). A questo proposito la Corte FISA ha confermato ripetutamente che i suoi riesami delle procedure di individuazione degli obiettivi e di minimizzazione a norma dell'articolo 702 non si limitano alle procedure così come scritte, ma comprendono anche le modalità con cui le procedure sono attuate dal governo ([267]).

(145) Le determinazioni relative alle singole individuazioni degli obiettivi sono effettuate dall'Agenzia per la sicurezza nazionale (National Security Agency, NSA) (l'ente di intelligence responsabile dell'individuazione degli obiettivi ai sensi dell'articolo 702 FISA) conformemente alle procedure di individuazione degli obiettivi approvate dalla Corte FISA, che impongono all'NSA di valutare, sulla base di tutte le circostanze, che è probabile che concentrare le attività di raccolta dati su una determinata persona consenta di acquisire una categoria di informazioni di intelligence esterna identificata in una certificazione ([268]). Tale valutazione deve essere dettagliata e basata sui fatti,

([259]) Codice degli Stati Uniti, titolo 50, articolo 1881a, lettera g).

([260]) 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. Codice degli Stati Uniti, titolo 50, articolo 1803, lettera a)). 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. lettera di Reggie B. Walton, presidente della Corte di vigilanza sull'intelligence esterna degli Stati Uniti, a Patrick J. Leahy, presidente della Commissione Giustizia del Senato degli Stati Uniti (29 luglio 2013) ("lettera di Walton"), pag. 2, disponibile all'indirizzo: https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) La FISCR è composta da 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. codice degli Stati Uniti, titolo 50, articolo 1803, lettera b)).

([262]) Cfr. codice degli Stati Uniti, titolo 50, articolo 1803, lettera b), articolo 1861a, lettera f) e articolo 1881a, lettera h) e lettera i), punto 4).

([263]) Codice degli Stati Uniti, titolo 50, articolo 1803, lettera i) e lettera l), punto 3), lettera A).

([264]) Codice degli Stati Uniti, titolo 50, articolo 1803, lettera i), punto 2), lettera A).

([265]) Codice degli Stati Uniti, titolo 50, articolo 1803, lettera i), punto 2), lettera B).

([266]) Cfr. ad esempio il parere della Corte FISA del 18 ottobre 2018, disponibile all'indirizzo https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, come confermato dalla Corte di controllo della vigilanza sull'intelligence esterna (FISCR) nel suo parere del 12 luglio 2019, disponibile all'indirizzo https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Cfr. ad esempio Corte FISA, Memorandum Opinion and Order at 35 (18 novembre 2020) (autorizzato al rilascio pubblico il 26 aprile 2021) (allegato D).

([268]) Codice degli Stati Uniti, titolo 50, articolo 1881a, lettera a), e documento *Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978*, come modificato, del marzo 2018 ("procedure di individuazione degli obiettivi da parte dell'NSA"), disponibile all'indirizzo https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, pagg. 1-4, ulteriormente spiegato nella relazione della PCLOB, pagg. 41-42.

fondata su un giudizio analitico, sulla formazione e sulle competenze specializzate dell'analista, nonché sulla natura delle informazioni di intelligence esterna da ottenere ([269]). L'individuazione degli obiettivi avviene individuando i cosiddetti selettori che identificano dispositivi di comunicazione specifici, quali l'indirizzo di posta elettronica o il numero di telefono dell'obiettivo, ma mai parole chiave o nomi di persone ([270]).

(146) Gli analisti dell'NSA individuano innanzitutto i cittadini stranieri all'estero che, in base alla loro valutazione, se sorvegliati porteranno a ottenere i pertinenti dati d'intelligence esterna indicati nella certificazione ([271]). Come indicato nelle procedure di individuazione degli obiettivi da parte dell'NSA, quest'ultima può sottoporre a sorveglianza un obiettivo soltanto se ha già appreso qualcosa in merito a tale obiettivo ([272]). Tali conoscenze possono derivare da informazioni provenienti da fonti diverse, ad esempio l'intelligence umana. Attraverso tali altre fonti, l'analista deve altresì conoscere un selettore specifico (ossia un account di comunicazione) utilizzato dal potenziale obiettivo. Una volta individuate le persone e approvata, al termine di un processo ampio di verifica interno all'NSA ([273]), 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 ([274]).

(147) L'NSA deve documentare la base fattuale per la selezione dell'obiettivo ([275]) e, a intervalli regolari dopo l'individuazione iniziale dell'obiettivo in questione, deve confermare che le norme applicabili in materia di individuazione degli obiettivi continuano ad essere rispettate ([276]). Se tali norme non risultano più soddisfatte, è necessario cessare la raccolta di dati ([277]). La selezione da parte dell'NSA di ciascun obiettivo e la corrispondente registrazione di ciascuna valutazione e logica alla base dell'individuazione dell'obiettivo in questione sono oggetto di riesame, con cadenza bimestrale, ai fini di una verifica della loro conformità rispetto alle procedure in materia di individuazione degli obiettivi, da parte di funzionari degli uffici di vigilanza sull'intelligence presso il Dipartimento della Giustizia, che sono tenuti a segnalare qualsiasi violazione alla Corte FISA e al Congresso ([278]). La documentazione scritta dell'NSA facilita la vigilanza da parte della Corte FISA in merito all'eventualità o meno che determinate persone siano considerate un obiettivo ai sensi dell'articolo 702 FISA, conformemente ai suoi poteri di vigilanza, illustrati ai considerando 173 e 174 ([279]). Infine il direttore dell'intelligence nazionale (DNI) è altresì tenuto a comunicare ogni anno il numero totale degli obiettivi a norma dell'articolo 702 FISA nelle relazioni pubbliche statistiche annuali sulla trasparenza. Le imprese che ricevono direttive a norma dell'articolo 702 FISA possono pubblicare dati aggregati (tramite relazioni sulla trasparenza) sulle richieste ricevute ([280]).

([269]) Procedure di individuazione degli obiettivi da parte dell'NSA, pag. 4.

([270]) Cfr. PCLOB, Relazione relativa all'articolo 702, pagg. 32-33 e 45 con ulteriori rimandi. Cfr. anche Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, pag. 41 (ottobre 2018), disponibile all'indirizzo: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB, Relazione relativa all'articolo 702, pagg. 42-43.

([272]) Procedure di individuazione degli obiettivi da parte dell'NSA, pag. 2.

([273]) PCLOB, Relazione relativa all'articolo 702, pag. 46. Ad esempio 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, *NSA's Implementation of Foreign Intelligence Act Section 702*, 16 aprile 2014.

([274]) Codice degli Stati Uniti, titolo 50, articolo 1881a, lettera h).

([275]) Procedure di individuazione degli obiettivi da parte dell'NSA, pag. 8. Cfr. anche PCLOB, Relazione relativa all'articolo 702, pag. 46. La mancata presentazione di una giustificazione scritta costituisce un caso di non conformità della documentazione che deve essere segnalato alla Corte FISA e al Congresso. Cfr. *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017*, pag. 41 (ottobre 2018), relazione del Dipartimento della Giustizia/dell'ODNI alla Corte FISA in materia di conformità per dicembre 2016-maggio 2017, pag. A-6, disponibile all'indirizzo: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Cfr. documento presentato dal governo degli Stati Uniti alla Corte di vigilanza sull'intelligence esterna, 2015 Summary of Notable Section 702 Requirements, pagg. 2 e 3 (15 luglio 2015) e informazioni fornite all'allegato VII.

([277]) Cfr. documento presentato dal governo degli Stati Uniti alla Corte di vigilanza sull'intelligence esterna, 2015 Summary of Notable Section 702 Requirements, pagg. 2 e 3 (15 luglio 2015), il quale afferma che se successivamente il governo valuta che non ci si possa attendere che la prosecuzione dell'attivazione del selettore si traduca nell'acquisizione di informazioni di intelligence esterna, il governo deve provvedere a una rapida disattivazione e un ritardo in merito a quest'ultima può comportare un caso di non conformità segnalabile. Cfr. anche le informazioni di cui all'allegato VII.

([278]) PCLOB, Relazione relativa all'articolo 702, pagg. 70-72). Norma 13, lettera b), del regolamento di procedura della Corte di vigilanza sull'intelligence esterna degli Stati Uniti, disponibile all'indirizzo https://www.fisc.uscourts.gov/sites/default/files/Corte FISA%20Rules%20of%20Procedure.pdf.

([279]) Cfr. anche relazione del Dipartimento della Giustizia/dell'ODNI alla Corte FISA in materia di conformità per il periodo da dicembre 2016 a maggio 2017, pag. A-6.

([280]) Codice degli Stati Uniti, titolo 50, articolo 1874.

(148) Per quanto concerne le altre basi giuridiche per la raccolta di dati personali trasferiti ad organizzazioni negli Stati Uniti, si applicano diverse limitazioni e garanzie. In generale la raccolta di dati in blocco è espressamente vietata a norma dell'articolo 402 FISA (autorità in materia di dispositivi di intercettazione) e facendo affidamento su National Security Letter, mentre è necessario ricorrere all'uso di "selettori" specifici ([281]).

(149) Al fine di svolgere attività di sorveglianza elettronica individualizzata (ai sensi dell'articolo 105 FISA), gli enti di intelligence devono presentare una domanda alla Corte FISA contenente una dichiarazione dei fatti e delle circostanze su cui si basano per giustificare la convinzione che vi sia un motivo plausibile per ritenere che il dispositivo di comunicazione in questione sia utilizzato o stia per essere utilizzato da una potenza straniera o da un agente di una potenza straniera ([282]). La Corte FISA valuta, tra l'altro, se dai fatti esposti risultino motivi plausibili per ritenere fondata l'ipotesi di un uso a detti fini ([283]).

(150) Al fine di effettuare una perquisizione di locali o beni destinata a sfociare in un'ispezione, un sequestro, ecc. di informazioni, materiali o beni (ad esempio un computer) sulla base dell'articolo 301 FISA, è necessaria una domanda per l'ottenimento di un'ordinanza dalla Corte FISA ([284]). Tale applicazione deve dimostrare tra l'altro che è probabile che l'obiettivo della perquisizione sia una potenza straniera o un agente di una potenza straniera; che il locale o il bene da sottoporre a perquisizione contenga informazioni di intelligence esterna e che il locale da sottoporre a perquisizione sia di proprietà, sia utilizzato, posseduto o in transito verso o da (un agente di) una potenza straniera ([285]).

(151) Analogamente l'installazione di dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita (a norma dell'articolo 402 FISA) richiede la presentazione di una domanda di ordinanza da parte della Corte FISA (o di un magistrato degli Stati Uniti) e l'uso di un selettore specifico, ossia un termine che identifica specificamente una persona, un account, ecc. ed è utilizzato per limitare, nella misura più ampia ragionevolmente possibile, la portata delle informazioni ricercate ([286]). Il potere in questione 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).

(152) Anche l'articolo 501 FISA ([287]), che consente la raccolta di documenti aziendali di un vettore pubblico (ossia qualsiasi persona o ente che trasporta persone o beni per via terrestre, ferroviaria, marittima o aerea a titolo oneroso), di una struttura ricettiva pubblica (ad esempio un albergo, un motel o una pensione), di una struttura di noleggio veicoli o di una struttura di immagazzinamento fisico (ossia che fornisce spazio o servizi connessi all'immagazzinamento di beni e materiali) ([288]), impone la presentazione di una domanda alla Corte FISA o a un magistrato. Tale domanda deve specificare le registrazioni richieste e i fatti specifici e circostanziabili che inducono a ritenere che la persona alla quale le registrazioni fanno riferimento sia una potenza straniera o un agente di potenza straniera ([289]).

(153) Infine le National Security Letter sono autorizzate da leggi diverse e consentono agli enti investigativi di ottenere determinate informazioni (escluso il contenuto delle comunicazioni) da determinati soggetti (ad esempio istituti finanziari, enti di segnalazione del credito, prestatori di servizi di comunicazioni elettroniche) contenute in rapporti di credito, documenti finanziari e archivi elettronici di abbonati e di dati transazionali ([290]). La legge in materia di National Security Letter che autorizza l'accesso alle comunicazioni elettroniche può essere invocata soltanto dall'FBI e prevede che le richieste utilizzino un termine che identifichi specificamente una persona, un soggetto, un numero di telefono o un conto e certifichino che le informazioni sono pertinenti per un'indagine in materia di sicurezza nazionale autorizzata al fine di fornire protezione contro il terrorismo internazionale o attività clandestine di intelligence ([291]). Il destinatario di una National Security Letter ha diritto di contestarla per via giudiziaria ([292]).

([281]) Codice degli Stati Uniti, titolo 50, articolo 1842, lettera c), punto 3) e, per quanto concerne le *National Security Letter*, codice degli Stati Uniti, titolo 12, articolo 3414, lettera a), punto 2), titolo 15, articolo 1681u e articolo 1681v, lettera a), e titolo 18, articolo 2709, lettera a).

([282]) L'espressione "agente di una potenza straniera" può comprendere persone non statunitensi che praticano il terrorismo internazionale o la proliferazione internazionale di armi di distruzione di massa (compresi gli atti preparatori) (codice degli Stati Uniti, titolo 50, articolo 1801, lettera b), punto 1)).

([283]) Codice degli Stati Uniti, titolo 50, articolo 1804. Cfr. anche articolo 1841, punto 4), per quanto riguarda la scelta dei selettori.

([284]) Codice degli Stati Uniti, titolo 50, articolo 1821, punto 5).

([285]) Codice degli Stati Uniti, titolo 50, articolo 1823, lettera a).

([286]) Codice degli Stati Uniti, titolo 50, articolo 1842 in combinato disposto con l'articolo 1841, punto 2), e titolo 18, articolo 3127.

([287]) Codice degli Stati Uniti, titolo 50, articolo 1862.

([288]) Codice degli Stati Uniti, titolo 50, articoli 1861-1862.

([289]) Codice degli Stati Uniti, titolo 50, articolo 1862, lettera b).

([290]) Codice degli Stati Uniti, titolo 12, articolo 3414; titolo 15, articoli 1681u-1681v; e titolo 18, articolo 2709.

([291]) Codice degli Stati Uniti, titolo 18, articolo 2709, lettera b).

([292]) Ad esempio codice degli Stati Uniti, titolo 18, articolo 2709, lettera d).

3.2.1.3 *Ulteriore utilizzo delle informazioni raccolte*

(154) Il trattamento dei dati personali raccolti dagli enti di intelligence statunitensi attraverso l'intelligence dei segnali è soggetto a una serie di garanzie.

(155) Innanzitutto ogni ente di intelligence deve garantire una sicurezza adeguata dei dati e impedire l'accesso da parte di persone non autorizzate ai dati personali raccolti attraverso l'intelligence dei segnali. A tale riguardo, strumenti diversi, tra i quali leggi, orientamenti e norme, specificano ulteriormente i requisiti minimi di sicurezza delle informazioni che devono essere posti in essere (ad esempio autenticazione a più fattori, cifratura, ecc.) ([293]). L'accesso ai dati raccolti deve essere limitato al personale autorizzato e formato avente la necessità di conoscere le informazioni per svolgere la propria missione ([294]). Più in generale gli enti di intelligence devono fornire una formazione adeguata ai propri dipendenti, anche per quanto concerne le procedure di segnalazione e di contrasto delle violazioni della legge (compreso il decreto presidenziale 14086) ([295]).

(156) In secondo luogo gli enti di intelligence devono rispettare le norme della comunità dell'intelligence in materia di accuratezza e obiettività, in particolare per quanto concerne la garanzia della qualità e dell'affidabilità dei dati, la considerazione di fonti di informazione alternative e l'obiettività nello svolgimento di analisi ([296]).

(157) In terzo luogo, per quanto concerne la conservazione dei dati, il decreto presidenziale 14086 chiarisce che i dati personali di persone non statunitensi sono soggetti ai medesimi periodi di conservazione che si applicano ai dati delle persone statunitensi ([297]). Gli enti di intelligence sono tenuti a definire periodi di conservazione specifici e/o i fattori che devono essere presi in considerazione per stabilire la durata dei periodi di conservazione applicabili (ad esempio se le informazioni costituiscono prova di un reato; se le informazioni costituiscono informazioni di intelligence esterna; se le informazioni sono necessarie per proteggere la sicurezza di persone od organizzazioni, compresi vittime od obiettivi del terrorismo internazionale), che sono stabiliti in diversi strumenti giuridici ([298]).

(158) In quarto luogo, si applicano norme specifiche per quanto concerne la diffusione di dati personali raccolti attraverso l'intelligence dei segnali. Come requisito generale, i dati personali relativi a persone non statunitensi possono essere divulgati soltanto se riguardano il medesimo tipo di informazioni che possono essere diffuse sulle persone statunitensi, ad esempio le informazioni necessarie per proteggere la sicurezza di una persona o di un'organizzazione (quali obiettivi, vittime od ostaggi di organizzazioni terroristiche internazionali) ([299]). Inoltre i dati personali non possono essere diffusi soltanto in ragione della cittadinanza o del paese di residenza di una persona o al fine di eludere i requisiti di cui al decreto presidenziale 14086 ([300]). La divulgazione all'interno degli

([293]) Articolo 2, lettera c), punto iii), lettera B), punto 1), del decreto presidenziale 14086. Cfr. anche il titolo VIII della legge sulla sicurezza nazionale (che specifica i requisiti per l'accesso alle informazioni classificate), l'articolo 1.5 del decreto presidenziale 12333 (che impone ai capi degli enti della comunità dell'intelligence di seguire gli orientamenti in materia di condivisione delle informazioni e di sicurezza, la riservatezza delle informazioni e altri requisiti giuridici), la direttiva 42 sulla sicurezza nazionale, il documento National Policy for the Security of National Security Telecommunications and Information Systems (che impone al comitato sui sistemi di sicurezza nazionale (Committee on National Security Systems) di fornire orientamenti in materia di sicurezza dei sistemi per i sistemi di sicurezza nazionale ai servizi e agli enti esecutivi), e il memorandum sulla sicurezza nazionale n. 8, Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (che stabilisce tempistiche e orientamenti per le modalità di attuazione dei requisiti di cibersicurezza per i sistemi di sicurezza nazionali, compresi l'autenticazione a più fattori, la cifratura, le tecnologie cloud e i servizi di rilevamento degli *endpoint*).

([294]) Articolo 2, lettera c), punto iii), lettera B), punto 2), del decreto presidenziale 14086. Inoltre i dati personali per i quali non è stata stabilita la conservazione definitiva possono essere consultati soltanto per effettuare o sostenere tale determinazione o per svolgere funzioni amministrative, di prova, di sviluppo, di sicurezza o di vigilanza autorizzate (articolo 2, lettera c), punto iii), lettera B), punto 3), del decreto presidenziale 14086.

([295]) Articolo 2, lettera d), punto ii), del decreto presidenziale 14086.

([296]) Articolo 2, lettera c), punto iii), lettera C), del decreto presidenziale 14086.

([297]) Articolo 2, lettera c), punto iii), lettera A), punto 2), lettere da a) a c), del decreto presidenziale 14086. Più in generale, ciascun ente deve mettere in atto politiche e procedure volte a ridurre al minimo la diffusione e la conservazione dei dati personali raccolti attraverso l'intelligence dei segnali (articolo 2, lettera c), punto iii), lettera A), del decreto presidenziale 14086).

([298]) Cfr. ad esempio l'articolo 309 della legge autorizzativa dell'intelligence per l'esercizio finanziario 2015; le procedure di minimizzazione adottate dai singoli enti di intelligence ai sensi dell'articolo 702 FISA e autorizzate dalla Corte FISA; le procedure approvate dal Procuratore generale e dalla legge federale sulle registrazioni (che impongono agli enti federali statunitensi, compresi gli enti di sicurezza nazionale, di stabilire periodi di conservazione delle loro registrazioni che devono essere approvati dalla NARA).

([299]) Articolo 2, lettera c), punto iii), lettera A), punto 1), lettera a) e articolo 5, lettera d), del decreto presidenziale 14086, in combinato disposto con l'articolo 2.3 del decreto presidenziale 12333.

([300]) Articolo 2, lettera c), punto iii), lettera A), punto 1), lettere b) ed e), del decreto presidenziale 14086.

organismi del governo statunitense può avvenire soltanto se una persona autorizzata e formata ha la ragionevole certezza che il destinatario necessita di conoscere le informazioni ([301]) e le proteggerà adeguatamente ([302]). Al fine di stabilire se i dati personali possono essere divulgati a destinatari esterni agli organismi del governo statunitense (compreso un governo straniero o un'organizzazione internazionale), occorre tener conto della finalità di tale divulgazione, della natura e della portata dei dati diffusi e del potenziale impatto negativo sulla persona o sulle persone interessate ([303]).

(159) Infine, anche per facilitare la vigilanza in merito al rispetto dei requisiti giuridici applicabili e di mezzi di ricorso efficaci, ogni ente di intelligence è tenuto, ai sensi del decreto presidenziale 14086, a conservare una documentazione adeguata sulla raccolta di intelligence dei segnali. I requisiti in materia di documentazione riguardano elementi quali la base fattuale per la valutazione della necessità di una specifica attività di raccolta per far progredire una priorità convalidata dell'intelligence ([304]).

(160) Oltre alle suddette garanzie di cui al decreto presidenziale 14086 per l'uso delle informazioni raccolte attraverso l'intelligence dei segnali, tutti gli enti di intelligence statunitensi sono soggetti a requisiti più generali in materia di limitazione delle finalità, minimizzazione dei dati, accuratezza, sicurezza, conservazione e diffusione dei dati, in particolare a norma della circolare n. A-130 dell'OMB, della legge sull'e-Government, della legge federale sulle registrazioni (cfr. considerando da 101 a 106) e degli orientamenti del comitato sui sistemi di sicurezza nazionale (CNSS) ([305]).

3.2.2 *Vigilanza*

(161) Le attività degli enti di intelligence statunitensi sono soggette al controllo da parte di organismi diversi.

(162) Innanzitutto il decreto presidenziale 14086 impone a ciascun ente di intelligence di disporre di funzionari di alto livello competenti in materie giuridiche, di vigilanza e di conformità al fine di garantire il rispetto del diritto statunitense applicabile ([306]). In particolare tali funzionari devono svolgere una vigilanza periodica delle attività di intelligence dei segnali e garantire che sia posto rimedio a eventuali non conformità. Gli enti di intelligence devono fornire a tali funzionari l'accesso a tutte le informazioni pertinenti per svolgere le loro funzioni di vigilanza e non possono intraprendere azioni volte ad ostacolare o influenzare indebitamente le loro attività di vigilanza ([307]). Inoltre, qualsiasi caso significativo di non conformità ([308]), individuato da un funzionario incaricato della vigilanza o da qualsiasi altro dipendente deve essere prontamente segnalato al capo dell'ente di intelligence e al direttore dell'intelligence nazionale, i quali devono garantire che siano adottate tutte le misure necessarie per porre rimedio alla circostanza in questione ed evitare il ripetersi del caso significativo di non conformità ([309]).

(163) Questa funzione di vigilanza è svolta da addetti aventi un ruolo designato in materia di conformità, nonché da funzionari e ispettori generali competenti per la tutela della vita privata e delle libertà civili ([310]).

([301]) Cfr. ad esempio il documento AGG-DOM il quale prevede ad esempio che l'FBI possa diffondere informazioni soltanto se il destinatario ha la necessità di sapere per svolgere la propria missione o per proteggere il pubblico.

([302]) Articolo 2, lettera c), punto iii), lettera A), punto 1), lettera c), del decreto presidenziale 14086. Gli enti di intelligence possono ad esempio diffondere informazioni in circostanze pertinenti a un'indagine penale o relative a un reato anche, ad esempio, diffondendo avvertimenti relativi a minacce di uccisione, lesioni personali gravi o rapimenti; diffondendo informazioni in merito a minacce informatiche, incidenti informatici o risposte ad intrusioni; e inviando notifiche alle vittime o avvertendo potenziali vittime di reati.

([303]) Articolo 2, lettera c), punto iii), lettera A), punto 1), lettera d), del decreto presidenziale 14086.

([304]) Articolo 2, lettera c), punto iii), lettera E), del decreto presidenziale 14086.

([305]) Cfr. la politica n. 22 del comitato sui sistemi di sicurezza nazionale, la politica di gestione dei rischi di cibersicurezza e l'istruzione 1253 di detto comitato, che forniscono orientamenti dettagliati in merito alle misure di sicurezza da attuare per i sistemi di sicurezza nazionale.

([306]) Articolo 2, lettera d), punto i), lettere A) e B), del decreto presidenziale 14086.

([307]) Articolo 2, lettera d), punto i), lettere B) e C), del decreto presidenziale 14086.

([308]) Ossia un'inosservanza sistemica o intenzionale del diritto statunitense applicabile che potrebbe compromettere la reputazione o l'integrità di un servizio della comunità dell'intelligence o mettere in discussione in altro modo la correttezza di un'attività della comunità dell'intelligence, anche alla luce di qualsiasi impatto significativo sugli interessi della persona o delle persone interessate in materia di vita privata e alle libertà civili (cfr. articolo 5, lettera l), del decreto presidenziale 14086).

([309]) Articolo 2, lettera d), del decreto presidenziale 14086.

([310]) Articolo 2, lettera d), punto i), lettera B), del decreto presidenziale 14086.

(164) Come nel caso delle autorità di contrasto in materia penale, tutti gli enti di intelligence dispongono di addetti alla tutela della vita privata e alle libertà civili ([311]). I poteri di tali addetti prevedono solitamente la vigilanza sulle procedure, per assicurare che il dipartimento/ente tenga adeguatamente conto degli aspetti inerenti alla vita privata e alle libertà civili e abbia predisposto procedure adeguate per trattare i reclami sporti dalle persone che denunciano una violazione della loro vita privata o delle loro libertà civili (in alcuni casi, come presso l'ODNI, gli addetti stessi sono abilitati a esaminare i reclami ([312])). I capi degli enti di intelligence devono garantire che gli addetti alla tutela della vita privata e alle libertà civili dispongano delle risorse necessari per adempiere il loro mandato, abbiano accesso a tutto il materiale e al personale necessari per lo svolgimento delle loro funzioni, siano informati e consultati in merito alle modifiche politiche proposte ([313]). 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, fornendo una sintesi del trattamento loro riservato, delle verifiche effettuate e delle indagini condotte, nonché degli effetti delle attività svolte dall'addetto stesso ([314]).

(165) In secondo luogo, ciascun ente di intelligence dispone di un ispettore generale indipendente, incaricato, tra l'altro, di vigilare sulle attività di intelligence esterna. L'articolazione del sistema comprende, presso l'ODNI, un Ufficio dell'ispettore generale della comunità dell'intelligence 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 ([315]). Come nel caso delle autorità di contrasto in materia penale (cfr. il considerando 109), tali ispettori generali sono indipendenti per legge ([316]) e responsabili dei controlli e delle indagini riguardanti i programmi e le operazioni condotte dall'ente in questione per finalità di intelligence nazionale, anche in relazione a casi di abuso o violazione della legge ([317]). Sono autorizzati ad accedere a tutti i dati, le relazioni, le verifiche, gli esami, i documenti, le carte, le

([311]) Cfr. codice degli Stati Uniti, titolo 42, articolo 2000ee-1. È il caso, ad esempio, del Dipartimento di Stato, del Dipartimento della Giustizia, del Dipartimento della Sicurezza interna, del Dipartimento della Difesa, dell'NSA, della *Central Intelligence Agency* (CIA, agenzia centrale di intelligence), dell'FBI e dell'ODNI.

([312]) Cfr. articolo 3, lettera c), del decreto presidenziale 14086.

([313]) Codice degli Stati Uniti, titolo 42, articolo 2000ee-1, lettera d).

([314]) Cfr. codice degli Stati Uniti, titolo 42, articolo 2000ee-1, lettera f), punti da 1) a 2). Ad esempio, dalla relazione dell'Ufficio per le libertà civili, la vita privata e la trasparenza dell'NSA relativa al periodo da gennaio 2021 a giugno 2021 emerge che l'NSA ha effettuato 591 riesami in merito a impatti sulle libertà civili e sulla vita privata in vari contesti, ad esempio per quanto concerne le attività di raccolta, gli accordi e le decisioni di condivisione di informazioni, le decisioni in materia di conservazione dei dati, ecc., tenendo conto di fattori diversi, quali la quantità e il tipo di informazioni associate all'attività, le persone coinvolte, la finalità e l'uso previsto dei dati, le garanzie esistenti per attenuare i potenziali rischi per la vita privata, ecc. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Analogamente dalle relazioni dell'Ufficio per la tutela della vita privata e le libertà civili della CIA per il periodo da gennaio a giugno 2019 si possono desumere informazioni sulle attività di vigilanza dell'Ufficio, ad esempio un riesame della conformità rispetto agli orientamenti emanati dal Procuratore generale ai sensi del decreto presidenziale 12333 per quanto concerne la conservazione e la diffusione di informazioni, orientamenti sull'attuazione della direttiva presidenziale 28 e requisiti per individuare e affrontare violazioni dei dati, nonché un riesame dell'uso e del trattamento di informazioni personali (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) L'ispettore generale è nominato dal presidente e confermato dal Senato e può essere destituito soltanto dal presidente.

([316]) Gli ispettori generali sono nominati a tempo indeterminato e possono essere rimossi 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 la legge sugli ispettori generali del 1978, articolo 8 (per il Dipartimento della Difesa); articolo 8E (per il Dipartimento della Giustizia), articolo 8G, lettera d), punto 2), lettere A) e B) (per l'NSA); il codice degli Stati Uniti, titolo 50, articolo 403q, lettera b) (per la CIA); la legge autorizzativa dell'intelligence per l'esercizio finanziario 2010, articolo 405, lettera f) (per la comunità dell'intelligence).

([317]) Legge sugli ispettori generali del 1978 come modificata, Pub. L. 117-108 dell'8 aprile 2022. Ad esempio, come spiegato nelle sue relazioni semestrali al Congresso relative al periodo dal 1º aprile 2021 al 31 marzo 2022, l'ispettore generale dell'NSA ha effettuato valutazioni sul trattamento delle informazioni di persone statunitensi raccolte ai sensi del decreto presidenziale 12333, sul processo di selezione dei dati di intelligence dei segnali, su uno strumento automatizzato di individuazione degli obiettivi utilizzato dall'NSA e sul rispetto della documentazione e delle norme di interrogazione in relazione alla raccolta di informazioni a norma dell'articolo 702 FISA, e ha formulato diverse raccomandazioni in tale contesto (cfr. https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, pagg. 5-8 e https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, pagg. 10-13). Cfr. anche le verifiche e le indagini recenti svolte dall'ispettore generale della comunità dell'intelligence in relazione alla sicurezza delle informazioni e alle divulgazioni non autorizzate di informazioni classificate in materia di sicurezza nazionale (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, pagg. 8, 11 e https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, pagg. 19-20).

raccomandazioni o altro materiale pertinente, se necessario mediante l'emanazione di una citazione, e possono assumere testimonianze ([318]). Gli ispettori generali segnalano i casi di presunte violazioni in materia penale ai fini dell'azione penale e formulano raccomandazioni per azioni correttive rivolte ai capi degli enti in questione ([319]). Sebbene le loro raccomandazioni non siano vincolanti, le relazioni che redigono, anche sugli interventi con cui vi si è dato seguito (o sull'assenza di tali interventi) ([320]), sono in genere rese pubbliche e trasmesse al Congresso, che su tale base può esercitare la sua funzione di vigilanza (cfr. considerando 168 e 169) ([321]).

(166) In terzo luogo l'Autorità di vigilanza sull'intelligence (IOB), istituita nell'ambito del Comitato presidenziale consultivo sull'intelligence (PIAB), vigila sul rispetto della costituzione statunitense e di tutte le norme applicabili da parte delle autorità di intelligence degli Stati Uniti ([322]). Il Comitato presidenziale consultivo sull'intelligence è un organo consultivo in seno all'Ufficio esecutivo del presidente, composto da 16 membri nominati dal presidente scelti all'esterno degli organismi del governo statunitense. L'Autorità di vigilanza sull'intelligence è costituita da un massimo di cinque membri designati dal presidente tra i membri del Comitato presidenziale consultivo sull'intelligence. Conformemente al decreto presidenziale 12333 ([323]), i capi di tutti gli enti di intelligence sono tenuti a segnalare all'Autorità di vigilanza sull'intelligence qualsiasi attività di intelligence per la quale vi sia motivo di credere che possa essere illegale o contraria a un decreto presidenziale o a una direttiva presidenziale. Al fine di assicurare che l'Autorità di vigilanza sull'intelligence abbia accesso alle informazioni necessarie per svolgere le sue funzioni, il decreto presidenziale 13462 incarica il direttore dell'intelligence nazionale e i capi degli enti di intelligence di fornire tutte le informazioni e tutta l'assistenza ritenute necessarie da tale autorità per lo svolgimento delle sue funzioni, nella misura consentita dalla legge ([324]). L'Autorità di vigilanza sull'intelligence è a sua volta tenuta a informare il presidente in merito alle attività di intelligence che ritiene possano violare il diritto degli Stati Uniti (compresi i decreti presidenziali) e non sono adeguatamente affrontate dal Procuratore generale, dal direttore dell'intelligence nazionale o dal capo di un ente di intelligence ([325]). Inoltre l'Autorità di vigilanza sull'intelligence è tenuta a informare il Procuratore generale in merito a possibili violazioni del diritto penale.

(167) In quarto luogo, gli enti di intelligence sono soggetti a controllo da parte della PCLOB. Ai sensi della legge che istituisce tale ente, alla PCLOB sono attribuite competenze nel settore delle politiche antiterrorismo e della loro attuazione, al fine di tutelare la vita privata e le libertà civili. Per controllare le attività degli enti di intelligence ha facoltà di accedere a tutti i dati, le relazioni, le verifiche, i documenti, le carte e le raccomandazioni dell'ente interessato, comprese le informazioni classificate, di procedere a interrogatori e di assumere testimonianze ([326]). Riceve le relazioni trasmesse dagli addetti alla tutela della vita privata e alle libertà civili di vari dipartimenti/enti federali ([327]), può rivolgere raccomandazioni al governo e agli enti di intelligence e riferisce periodicamente alle commissioni del Congresso e al presidente ([328]). Le relazioni della PCLOB, comprese quelle presentate al Congresso, devono essere messe a disposizione del pubblico nella misura più ampia possibile ([329]). La PCLOB ha pubblicato diverse relazioni di vigilanza e di seguito, tra cui un'analisi dei programmi attuati sulla base dell'articolo 702 FISA e della tutela della vita privata in tale contesto, nonché l'attuazione della direttiva presidenziale 28 e del decreto presidenziale 12333 ([330]). La PCLOB ha altresì il compito di svolgere funzioni di vigilanza specifiche per quanto

([318]) Cfr. legge sugli ispettori generali del 1978, articolo 6.
([319]) Cfr. ibidem articoli 4, 6-5.
([320]) Per quanto riguarda il seguito dato alle relazioni e alle raccomandazioni degli ispettori generali, cfr. ad esempio la risposta a un rapporto dell'ispettore generale del Dipartimento della Giustizia nel quale è stato constatato che l'FBI non era stata sufficientemente trasparente nei confronti della Corte FISA in relazione alle domande dal 2014 al 2019, una circostanza questa che ha portato a riforme volte a migliorare la conformità, la vigilanza e la responsabilizzazione presso l'FBI (ad esempio, il direttore dell'FBI ha ordinato oltre 40 azioni correttive, tra cui 12 specifiche per il processo FISA relativo alla documentazione, alla supervisione, alla manutenzione dei fascicoli, alla formazione e alle verifiche) (cfr. https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance e https://oig.justice.gov/reports/2019/o20012.pdf). Cfr. ad esempio anche la verifica dell'Ufficio dell'FBI da parte dell'ispettore generale del Dipartimento della Giustizia sui ruoli e sulle responsabilità del giureconsulto nel vigilare sul rispetto delle leggi, delle politiche e delle procedure applicabili in relazione alle attività di sicurezza nazionale dell'FBI e l'appendice 2, che comprende una lettera dell'FBI che accetta tutte le raccomandazioni. A tale riguardo, l'appendice 3 fornisce una panoramica delle azioni di seguito e delle informazioni richieste all'ispettore generale dall'FBI per poter chiudere le sue raccomandazioni (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).
([321]) Cfr. legge sugli ispettori generali del 1978, articolo 4, paragrafo 5, e articolo 5.
([322]) Cfr. del decreto presidenziale 13462.
([323]) Articolo 1.6, lettera c), del decreto presidenziale 12333.
([324]) Articolo 8, lettera a), del decreto presidenziale 13462.
([325]) Articolo 6, lettera b), del decreto presidenziale 13462.
([326]) Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera g).
([327]) Cfr. codice degli Stati Uniti, titolo 42, articolo 2000ee-1, lettera f), punto 1), lettera A), punto iii). Tra questi figurano almeno il Dipartimento della Giustizia, il Dipartimento della Difesa, il Dipartimento della Sicurezza interna, il Direttore dell'intelligence nazionale e la CIA, cui si aggiungono tutti gli altri dipartimenti, enti o servizi dell'esecutivo che la PCLOB ha ritenuto opportuno contemplare.
([328]) Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera e).
([329]) Codice degli Stati Uniti, titolo 42, articolo 2000ee, lettera f).
([330]) Disponibile all'indirizzo https://www.pclob.gov/Oversight.

concerne l'attuazione del decreto presidenziale 14086, in particolare riesaminando se le procedure dell'ente siano coerenti con tale decreto presidenziale (cfr. considerando 126) e valutando il funzionamento della riparazione del meccanismo di ricorso (cfr. considerando 194).

(168) In quinto luogo, oltre ai citati meccanismi di vigilanza inquadrati nell'esecutivo, commissioni specifiche in seno al Congresso degli Stati Uniti (le commissioni Giustizia e Intelligence della Camera dei rappresentanti e del Senato), hanno competenze di vigilanza sulle attività d'intelligence esterna condotte dagli USA. I membri di tali commissioni hanno accesso alle informazioni classificate e ai metodi e programmi d'intelligence ([331]). Dette commissioni esercitano le loro funzioni di vigilanza in modi diversi, in particolare attraverso audizioni, indagini, riesami e relazioni ([332]).

(169) Le commissioni del Congresso ricevono relazioni periodiche sulle attività di intelligence, anche dal Procuratore generale, dal direttore dell'intelligence nazionale, dagli enti di intelligence e da altri organismi di vigilanza (ad esempio gli ispettori generali) (cfr. considerando 164 e 165). In particolare, 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 ([333]). 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 ([334]).

(170) Inoltre ulteriori obblighi di informativa derivano da leggi specifiche. In particolare la FISA impone 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 ([335]). Chiede inoltre al governo di trasmettere alle commissioni del Congresso copia di ogni decisione, ordinanza o parere pronunciati dalla Corte FISA o dalla FISCR, in cui è riportata una spiegazione o interpretazione rilevante di una disposizione della FISA. Per quanto concerne in particolare la sorveglianza a norma dell'articolo 702 FISA, la vigilanza parlamentare 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 FISA, corredata di documenti giustificativi, tra i quali le relazioni sulla conformità del Dipartimento della Giustizia e dell'ODNI e la descrizione dei casi di inosservanza ([336]), 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 ([337]).

([331]) Codice degli Stati Uniti, titolo 50, articolo 3091.

([332]) Ad esempio le commissioni organizzano audizioni tematiche (cfr. ad esempio un'audizione recente della commissione Giustizia della Camera dei rappresentanti sulle "retate digitali", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 e un'audizione della Commissione Intelligence della Camera dei rappresentanti in merito all'uso dell'intelligenza artificiale da parte della comunità dell'intelligence, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), nonché audizioni periodiche di vigilanza, ad esempio della divisione della sicurezza nazionale dell'FBI e del Dipartimento della Giustizia, cfr. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 e https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Come esempio di indagine, cfr. l'indagine della commissione Intelligence del Senato sull'ingerenza russa nelle elezioni statunitensi del 2016, cfr. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Per quanto riguarda le relazioni, cfr. ad esempio la panoramica delle attività (di vigilanza) della commissione di cui alla relazione della commissione Intelligence del Senato per il periodo dal 4 gennaio 2019 al 3 gennaio 2021, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Cfr. codice degli Stati Uniti, titolo 50, articolo 3091, lettera a), punto 1). Questa disposizione prevede i requisiti generali in materia di vigilanza del Congresso nel settore della sicurezza nazionale.

([334]) Cfr. codice degli Stati Uniti, titolo 50, articolo 3091, lettera b).

([335]) Cfr. codice degli Stati Uniti, titolo 50, articoli 1808, 1846, 1862, 1871, 1881f.

([336]) Cfr. codice degli Stati Uniti, titolo 50, articolo 1881f.

([337]) Cfr. codice degli Stati Uniti, titolo 50, articolo 1881a, lettera l), punto 1).

(171) Inoltre la FISA impone al governo statunitense di comunicare ogni anno al Congresso (e al pubblico) il numero delle ordinanze 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 ([338]). Tale legge impone altre comunicazioni pubbliche circa il numero di National Security Letter 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 National Security Letter, di pubblicare, a determinate condizioni, relazioni sulla trasparenza) ([339]).

(172) Più in generale la comunità dell'intelligence statunitense si adopera in vari modi per garantire la trasparenza delle sue attività di intelligence (esterna). Ad esempio nel 2015 l'ODNI ha adottato i principi di trasparenza dell'intelligence e un piano di attuazione per la trasparenza e ha ordinato a ciascun ente di intelligence di designare un responsabile della trasparenza dell'intelligence al fine di promuovere la trasparenza e guidare le iniziative in materia di trasparenza ([340]). Nell'ambito di tali sforzi, la comunità dell'intelligence ha reso e continua a rendere pubbliche parti declassificate di politiche, procedure, relazioni di vigilanza, relazioni sulle attività di cui all'articolo 702 FISA e al decreto presidenziale 12333, decisioni della Corte FISA e altri materiali, anche su una pagina web dedicata "IC on the Record", gestita dall'ODNI ([341]).

(173) Infine la raccolta di dati personali ai sensi dell'articolo 702 FISA, oltre alla vigilanza da parte degli organi di vigilanza di cui ai considerando da 162 a 168, è soggetta a vigilanza da parte della Corte FISA ([342]). Conformemente alla norma 13 del regolamento di procedura della Corte FISA, i responsabili della conformità presso gli enti di intelligence statunitensi sono tenuti a segnalare al Dipartimento della Giustizia e all'ODNI qualsiasi violazione delle procedure in materia di individuazione degli obiettivi, minimizzazione e interrogazione di cui all'articolo 702 FISA, i quali a loro volta le segnalano alla Corte FISA. Inoltre il Dipartimento della Giustizia e l'ODNI presentano alla Corte FISA relazioni semestrali di valutazione congiunta della vigilanza, che individuano le tendenze in materia di conformità delle procedure di individuazione degli obiettivi; forniscono dati statistici; descrivono le categorie dei casi di non conformità; descrivono in maniera dettagliata i motivi per cui si sono verificati taluni casi di non conformità rispetto alle procedure di individuazione degli obiettivi, così come le misure adottate dagli enti di intelligence per evitare il ripetersi di tali casi ([343]).

(174) Se necessario (ad esempio qualora vengano individuate violazioni delle procedure di individuazione degli obiettivi), la Corte può ordinare all'ente di intelligence pertinente di adottare misure correttive ([344]). Le misure correttive in questione potranno spaziare da misure individuali a misure strutturali, ad esempio dalla cessazione dell'acquisizione di dati e dalla cancellazione di dati ottenuti illecitamente fino alla modifica delle pratiche di raccolta, anche per quanto riguarda gli orientamenti e la formazione del personale ([345]). Inoltre, durante il riesame annuale delle

([338]) Codice degli Stati Uniti, titolo 50, articolo 1873, lettera b). 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, lettera 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.

([339]) Codice degli Stati Uniti, titolo 50, articolo 1873, lettera b), punto 7) e articolo 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Cfr. "IC on the Record", disponibile all'indirizzo https://icontherecord.tumblr.com/.

([342]) In passato la Corte FISA ha concluso che la Corte ha l'impressione che gli enti di attuazione, nonché l'ODNI e la divisione per la sicurezza nazionale del Dipartimento della Giustizia, destinano risorse considerevoli alle loro responsabilità in materia di conformità e vigilanza ai sensi dell'articolo 702. Come regola generale, i casi di non conformità sono individuati tempestivamente e sono adottate misure correttive adeguate, tra cui l'eliminazione delle informazioni ottenute in modo improprio o altrimenti soggette a prescrizioni in materia di distruzione secondo le procedure applicabili. Corte FISA, *Memorandum Opinion and Order* (2014), disponibile all'indirizzo https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) *Cfr. ad esempio* Relazione del Dipartimento della Giustizia/dell'ODNI alla Corte FISA in materia di conformità rispetto all'articolo 702 FISA, per il periodo da giugno 2018 a novembre 2018, pagg. 21-65.

([344]) Codice degli Stati Uniti, titolo 50, articolo 1803, lettera h). Cfr. anche PCLOB, Relazione relativa all'articolo 702, pag. 76. Inoltre, cfr. il documento *Memorandum Opinion and Order*, del 3 ottobre 2011, della Corte FISA come esempio di ordinanza sulle carenze nel contesto della quale al governo è stato ingiunto di porre rimedio alle carenze individuate entro 30 giorni. Disponibile all'indirizzo https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Cfr. lettera di Walton, sezione 4, pagg. 10-11. Cfr. anche il parere della Corte FISA del 18 ottobre 2018, disponibile all'indirizzo https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, come confermato dalla FISCR nel suo parere del 12 luglio 2019, disponibile all'indirizzo https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, nel quale Corte FISA ha tra l'altro ordinato al governo di conformarsi a determinati obblighi di notifica, documentazione e rendicontazione nei confronti della Corte FISA.

([345]) Cfr. ad esempio Corte FISA, *Memorandum Opinion and Order*, pag. 76 (6 dicembre 2019) (pubblicazione autorizzata il 4 settembre 2020), documento nel contesto del quale la Corte FISA ha ingiunto al governo di presentare entro il 28 febbraio 2020 una relazione scritta sulle misure che il governo stava adottando al fine di migliorare i processi per l'individuazione e la rimozione di relazioni derivate da informazioni di cui all'articolo 702 FISA richiamate per motivi di conformità, nonché per altre questioni. Cfr. anche allegato VII.

certificazioni a norma dell'articolo 702, la Corte FISA prende in considerazione i casi di non conformità per stabilire se le certificazioni presentate sono conformi ai requisiti della FISA. Analogamente se la Corte FISA ritiene che le certificazioni del governo non siano state sufficienti, anche in ragione di particolari casi di inadempienza, può emettere una cosiddetta "ordinanza sulle carenze" che impone al governo di porre rimedio alla violazione entro 30 giorni o impone al governo di cessare o non iniziare ad attuare la certificazione a norma dell'articolo 702 in questione. Infine la Corte FISA valuta le tendenze rilevate in materia di conformità e può imporre modifiche delle procedure o ulteriori attività di vigilanza e comunicazione per affrontare le tendenze in materia di conformità ([346]).

3.2.3 ***Mezzi di ricorso***

(175) Come spiegato più dettagliatamente nella presente sezione, negli Stati Uniti gli interessati dispongono di svariate vie di ricorso che consentono loro la possibilità di promuovere un'azione legale dinanzi a un organo giurisdizionale indipendente e imparziale dotato di poteri vincolanti. Congiuntamente tali mezzi consentono alle persone fisiche di avere accesso ai propri dati personali, di ottenere un riesame della legittimità dell'accesso ai propri dati da parte di pubbliche amministrazioni e, qualora si accerti una violazione, di porvi rimedio, anche attraverso la rettifica o la cancellazione dei dati personali in questione.

(176) Innanzitutto è istituito un meccanismo di ricorso specifico, ai sensi del decreto presidenziale 14086, integrato dal regolamento del Procuratore generale, che istituisce il Tribunale del riesame in materia di protezione dei dati (DPRC), al fine di gestire e risolvere i reclami di persone riguardanti le attività statunitensi di intelligence dei segnali. Chiunque nell'UE ha il diritto di presentare un reclamo rivolgendosi al meccanismo di ricorso in merito a una presunta violazione del diritto statunitense che disciplina le attività di intelligence dei segnali (ad esempio il decreto presidenziale 14086, l'articolo 702 FISA, il decreto presidenziale 12333) che lede gli interessi della persona in questione in materia di tutela della vita privata e libertà civili ([347]). Tale meccanismo di ricorso è a disposizione di persone provenienti da paesi od organizzazioni regionali di integrazione economica che sono stati designati dal Procuratore generale degli Stati Uniti come "Stati qualificati" ([348]). Il 30 giugno 2023 l'Unione europea e i tre paesi dell'Associazione europea di libero scambio, che assieme costituiscono lo Spazio economico europeo, sono stati designati dal Procuratore generale ai sensi dell'articolo 3, lettera f), del decreto presidenziale 14086 come "Stati qualificati" ([349]). Tale designazione lascia impregiudicato l'articolo 4, paragrafo 2, del trattato sull'Unione europea.

(177) Un interessato dell'Unione che intenda promuovere un reclamo deve presentarlo a un'autorità di controllo di uno Stato membro dell'UE competente per la vigilanza in merito al trattamento di dati personali da parte di autorità pubbliche (un'autorità di protezione dei dati) ([350]). Ciò garantisce un facile accesso al meccanismo di ricorso consentendo alle persone di rivolgersi a un'autorità "vicina a casa" con la quale possono comunicare nella propria lingua. Una volta verificati i requisiti per la presentazione di un reclamo di cui al considerando 178, l'autorità di protezione dei dati competente trasmette il reclamo al meccanismo di ricorso tramite il segretariato del comitato europeo per la protezione dei dati.

(178) La promozione di un reclamo presso il meccanismo di ricorso è soggetta a requisiti di ammissibilità ridotti, in quanto le persone non devono dimostrare che i loro dati sono stati effettivamente oggetto di attività di intelligence dei segnali negli Stati Uniti ([351]). Al tempo stesso, per fornire un punto di partenza per lo svolgimento del riesame da parte del meccanismo di ricorso, occorre che gli interessati forniscano talune informazioni di base, ad esempio in merito ai dati personali che si ritiene ragionevolmente siano stati trasferiti negli Stati Uniti e ai mezzi con cui si ritiene che tale trasferimento sia avvenuto; l'identità degli enti pubblici statunitensi che si ritiene siano coinvolti nella presunta violazione (laddove nota); la base per sostenere che si è verificata una violazione del diritto statunitense (anche se anche in questo caso non è necessario dimostrare che i dati personali sono stati effettivamente raccolti da enti di intelligence statunitensi) e la natura del provvedimento richiesto.

([346]) Cfr. allegato VII.

([347]) Cfr. articolo 4, lettera k), punto iv), del decreto presidenziale 14086, secondo cui un reclamo promosso presso il meccanismo di ricorso deve essere presentato da un reclamante che agisce per proprio conto (ossia non in qualità di rappresentante di un governo, di un'organizzazione non governativa o intergovernativa). Il concetto di "soggetto i cui interessi sono stati lesi" non impone al denunciante di rispettare una determinata soglia per avere accesso al meccanismo di ricorso (cfr. considerando 178 a tale riguardo). Esso chiarisce piuttosto che l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e il DPRC hanno il potere di porre rimedio a violazioni del diritto statunitense che disciplina le attività di intelligence dei segnali che ledono gli interessi individuali del denunciante in materia di tutela della vita privata e libertà civili. Di contro le violazioni degli obblighi previsti dal diritto statunitense applicabile che non sono concepiti per tutelare le persone (ad esempio requisiti di bilancio) non rientrerebbero nella competenza giurisdizionale dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e del DPRC.

([348]) Articolo 3, lettera f), del decreto presidenziale 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Articolo 4, lettera d), punto v), del decreto presidenziale 14086.

([351]) Cfr. articolo 4, lettera k), punti i)-iv), del decreto presidenziale 14086.

(179) L'indagine iniziale sui reclami presentati a questo meccanismo di ricorso è svolta dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI, il cui ruolo e i cui poteri statutari sono stati ampliati per le azioni specifiche intraprese a norma del decreto presidenziale 14086 ([352]). All'interno della comunità dell'intelligence, l'addetto alla tutela della vita privata e alle libertà civili ha il compito, tra l'altro, di garantire che la tutela delle libertà civili e della vita privata sia adeguatamente integrata nelle politiche e procedure dell'ODNI e degli enti di intelligence; di vigilare sul rispetto, da parte dell'ODNI, dei requisiti applicabili in materia di libertà civili e tutela della vita privata; e di svolgere valutazioni dell'impatto sulla vita privata ([353]). L'addetto alla tutela della vita privata e alle libertà civili dell'ODNI può essere revocato dal direttore dell'intelligence nazionale soltanto per giusta causa, ossia in caso di condotta illecita, concussione, violazione della sicurezza, negligenza o incapacità ([354]).

(180) Nell'effettuare il riesame, l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI ha accesso alle informazioni per la sua valutazione e può avvalersi dell'assistenza obbligatoria degli addetti alla tutela della vita privata e alle libertà civili attivi in seno ai diversi enti di intelligence ([355]). Agli enti di intelligence è fatto divieto di ostacolare o influenzare indebitamente i riesami svolti dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI. Rientra in tale contesto anche il direttore dell'intelligence nazionale, che non deve interferire con il riesame ([356]). In sede di esame di un reclamo, l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI deve applicare la legge "in modo imparziale", tenendo conto sia degli interessi di sicurezza nazionale nelle attività di intelligence dei segnali che delle tutele della vita privata ([357]).

(181) Nel contesto del suo esame, l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI stabilisce se si è verificata una violazione del diritto statunitense applicabile e, in tal caso, si pronuncia in merito a una riparazione adeguata ([358]). Quest'ultima fa riferimento a misure che pongono pienamente rimedio a una violazione individuata, quali la cessazione dell'acquisizione illecita di dati, la cancellazione dei dati raccolti illecitamente, la cancellazione dei risultati di interrogazioni condotte in modo inadeguato su dati altrimenti raccolti lecitamente, la limitazione dell'accesso ai dati raccolti legalmente a personale adeguatamente formato o il richiamo di relazioni di intelligence contenenti dati acquisiti senza legittima autorizzazione o diffusi illecitamente ([359]). Le decisioni dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI sui singoli reclami (compresa la riparazione) sono vincolanti per gli enti di intelligence interessati ([360]).

(182) L'addetto alla tutela della vita privata e alle libertà civili dell'ODNI deve conservare la documentazione del suo riesame e produrre una decisione classificata che spieghi la base delle sue constatazioni fattuali, la determinazione dell'esistenza di una violazione contemplata e la determinazione della riparazione adeguata ([361]). Se dall'esame condotto dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI emerge una violazione di un'autorità soggetta a vigilanza da parte della Corte FISA, tale addetto alla tutela della vita privata e alle libertà civili deve fornire altresì una relazione classificata al Procuratore generale aggiunto per la sicurezza nazionale, il quale a sua volta è tenuto a segnalare la non conformità alla Corte FISA, che può adottare ulteriori azioni coercitive (conformemente alla procedura illustrata ai considerando 173 e 174) ([362]).

(183) Una volta completato l'esame, l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI informa il reclamante, tramite l'autorità nazionale, in merito al fatto che l'esame non ha individuato alcuna violazione contemplata o l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI ha emesso una decisione che richiede una riparazione adeguata ([363]). Ciò consente di tutelare la riservatezza delle attività svolte a tutela della sicurezza nazionale, fornendo nel contempo alle persone una decisione che confermi che il loro reclamo è stato debitamente esaminato e giudicato. Tale decisione può inoltre essere impugnata dalla persona. A tal fine, la persona in questione viene informata della possibilità di presentare ricorso adendo il DPRC per ottenere un riesame delle decisioni dell'addetto alla tutela della vita privata e alle libertà civili (cfr. considerando 184 e successivi) così come del fatto che, qualora tale Corte sia adita, viene selezionato un avvocato speciale per sostenere gli interessi del reclamante ([364]).

([352]) Articolo 3, lettera c), punto iv), del decreto presidenziale 14086. Cfr. anche la legge sulla sicurezza nazionale del 1947, il codice degli Stati Uniti, titolo 50, articolo 403-3d e l'articolo 103D relativo al ruolo dell'addetto alla tutela della vita privata e alle libertà civili in seno all'ODNI.
([353]) Codice degli Stati Uniti, titolo 50, articolo 3029, lettera b).
([354]) Articolo 3, lettera c), punto iv), del decreto presidenziale 14086.
([355]) Articolo 3, lettera c), punto iii), del decreto presidenziale 14086.
([356]) Articolo 3, lettera c), punto iv), del decreto presidenziale 14086.
([357]) Articolo 3, lettera c), punto i), lettera B), punti i) e iii), del decreto presidenziale 14086.
([358]) Articolo 3, lettera c), punto i), del decreto presidenziale 14086.
([359]) Articolo 4, lettera a), del decreto presidenziale 14086.
([360]) Articolo 3, lettere c) e d), del decreto presidenziale 14086.
([361]) Articolo 3, lettera c), punto i), lettere F) e G), del decreto presidenziale 14086.
([362]) Cfr. anche articolo 3, lettera c), punto i), lettera D), del decreto presidenziale 14086.
([363]) Articolo 3, lettera c), punto i), lettera E), punto 1), del decreto presidenziale 14086.
([364]) Articolo 3, lettera c), punto i), lettera E), punti da 2) a 3), del decreto presidenziale 14086.

(184) Qualsiasi reclamante, nonché ciascun servizio della comunità dell'intelligence, può chiedere il riesame della decisione dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI dinanzi al DPRC. Tali domande di riesame devono essere presentate entro 60 giorni dal ricevimento della notifica da parte dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI che informa che l'esame è stato completato e devono comprendere tutte le informazioni che la persona desidera fornire al DPRC (ad esempio argomentazioni su questioni di diritto o sull'applicazione del diritto ai fatti del caso) ([365]). Anche in questo caso gli interessati dell'Unione possono presentare la loro domanda all'autorità di protezione dei dati competente (cfr. considerando 177).

(185) Il DPRC è un tribunale indipendente istituito dal Procuratore generale sulla base del decreto presidenziale 14086 ([366]). È composto da almeno sei giudici, nominati dal Procuratore generale in consultazione con la PCLOB, il Segretario al Commercio e il direttore dell'intelligence nazionale per un mandato rinnovabile di quattro anni ([367]). La nomina dei giudici da parte del Procuratore generale si basa sui criteri utilizzati dal potere esecutivo per valutare i candidati alla magistratura federale, tenendo conto di eventuali precedenti esperienze giudiziarie ([368]). Inoltre i giudici devono essere operatori della giustizia (ossia membri attivi in regola dell'ordine forense e debitamente abilitati a esercitare la professione legale) e avere un'esperienza adeguata in relazione al diritto in materia di tutela della vita privata e di sicurezza nazionale. Il Procuratore generale deve adoperarsi per garantire che almeno la metà dei giudici in un dato momento disponga di un'esperienza giudiziaria precedente e che tutti i giudici siano in possesso di un nulla osta di sicurezza per poter accedere a informazioni classificate in materia di sicurezza nazionale ([369]).

(186) Possono essere nominate a far parte del DPRC soltanto le persone che soddisfano le qualifiche di cui al considerando 185 e che non sono dipendenti del ramo esecutivo al momento della loro nomina o che non lo sono state nei due anni antecedenti. Analogamente, durante il loro mandato presso il DPRC, i giudici non possono svolgere funzioni o impieghi ufficiali all'interno del governo statunitense (se non in qualità di giudici presso il DPRC) ([370]).

(187) L'indipendenza del processo di pronuncia del giudizio è conseguita mediante una serie di garanzie. In particolare al potere esecutivo (il Procuratore generale e gli enti di intelligence) è vietato interferire con il riesame del DPRC o influenzare indebitamente tale processo ([371]). Il DPRC stesso è tenuto a giudicare le cause in modo imparziale ([372]) e opera secondo un proprio regolamento interno (adottato a maggioranza dei voti). Inoltre l'incarico dei giudici del DPRC può essere revocato esclusivamente dal Procuratore generale e soltanto per giusta causa (ad esempio condotta illecita, concussione, violazione della sicurezza, negligenza o incapacità), dopo aver tenuto debitamente conto delle norme applicabili ai giudici federali stabilite nelle norme per i procedimenti in materia di condotta della magistratura e di disabilità della magistratura ([373]).

([365]) Articolo 201.6, lettere a) e b), del regolamento del Procuratore generale.

([366]) Articolo 3, lettera d), punto i) e regolamento del Procuratore generale. La Corte Suprema degli Stati Uniti ha riconosciuto la possibilità per il Procuratore generale di istituire organi indipendenti con potere decisionale, incaricati anche di pronunciarsi in merito a singoli casi, cfr. in particolare *Stati Uniti ex rel. Accardi/Shaughnessy,* 347 U.S. 260 (1954) e *United States/Nixon,* 418 U.S. 683, 695 (1974). Il rispetto dei diversi requisiti di cui al decreto presidenziale 14086, ad esempio i criteri e la procedura per la nomina e la revoca dell'incarico dei giudici del DPRC, è soggetto in particolare alla supervisione dell'ispettore generale del Dipartimento di giustizia (cfr. anche il considerando 109 sull'autorità statutaria degli ispettori generali).

([367]) Articolo 3, lettera d), punto i), lettera A), del decreto presidenziale 14086 e articolo 201.3, lettera a), del regolamento del Procuratore generale.

([368]) Articolo 201.3, lettera b), del regolamento del Procuratore generale.

([369]) Articolo 3, lettera d), punto i), lettera B), del decreto presidenziale 14086.

([370]) Articolo 3, lettera d), punto i), lettera A), del decreto presidenziale 14086 e articolo 201.3, lettere a) e c), del regolamento del Procuratore generale. Le persone nominate a far parte del DPRC possono partecipare ad attività extragiudiziarie, tra cui attività commerciali, attività finanziarie, attività di raccolta fondi senza scopo di lucro, attività fiduciarie e all'esercizio della professione forense, a condizione che tali attività non interferiscano con l'esercizio imparziale delle loro funzioni o con l'efficacia o l'indipendenza del DPRC (articolo 201.7, lettera c), del regolamento del Procuratore generale).

([371]) Articolo 3, lettera d), punti da iii) a iv), del decreto presidenziale 14086 e articolo 201.7, lettera d), del regolamento del Procuratore generale.

([372]) Articolo 3, lettera d), punto i), lettera D), del decreto presidenziale 14086 e articolo 201.9, del regolamento del Procuratore generale.

([373]) Articolo 3, lettera d), punto iv), del decreto presidenziale 14086 e articolo 201.7, lettera d), del regolamento del Procuratore generale. Cfr. anche la sentenza *Bumap/United States,* 252 U.S. 512, 515 (1920), che ha confermato il principio di lunga data vigente nel diritto statunitense secondo cui il potere di revoca dell'incarico è connesso a quello di nomina (come ricordato anche dall'Ufficio del Giureconsulto del Dipartimento della Giustizia nel documento *The Constitutional Separation of Powers Between the President and Congress,* 20 Op. O.L.C. 124, 166 (1996)).

(188) Le domande presentate al DPRC sono esaminate da collegi di tre giudici, tra cui un presidente, che devono agire conformemente al codice di condotta per i giudici statunitensi ([374]). Ciascun collegio è assistito da un avvocato speciale ([375]), il quale ha accesso a tutte le informazioni relative alla causa, comprese quelle classificate ([376]). Il ruolo dell'avvocato speciale consiste nel garantire che gli interessi del reclamante siano rappresentati e che il collegio del DPRC sia ben informato su tutte le questioni di diritto e di fatto pertinenti ([377]). Al fine di informare ulteriormente la propria posizione in merito a una domanda di riesame presentata da una persona al DPRC, l'avvocato speciale può chiedere informazioni al reclamante mediante la formulazione di domande scritte ([378]).

(189) Il DPRC esamina le decisioni adottate dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI (sia in relazione all'eventualità che si sia verificata una violazione del diritto statunitense applicabile, sia per quanto riguarda la riparazione adeguata) sulla base, come minimo, delle registrazioni dell'indagine condotta da tale addetto dell'ODNI, nonché di tutte le informazioni e le osservazioni fornite dal reclamante, dall'avvocato speciale o da un ente di intelligence ([379]). Un collegio del DPRC ha accesso a tutte le informazioni necessarie per effettuare un riesame, che può ottenere tramite l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI (ad esempio il collegio può chiedere a tale addetto di integrare le proprie registrazioni con informazioni supplementari o conclusioni fattuali, se necessario per effettuare il riesame) ([380]).

(190) Al momento di concludere il suo riesame, il DPRC può: 1) decidere che non vi sono prove indicanti che sono state svolte attività di intelligence dei segnali riguardanti dati personali del reclamante; 2) decidere che le decisioni dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI erano giuridicamente corrette e suffragate da prove sostanziali; oppure 3) qualora il DPRC non concordi con le conclusioni dell'addetto dell'ODNI (qualora si sia verificata una violazione del diritto statunitense applicabile o sia da definire una riparazione adeguata), emettere decisioni proprie in merito alla questione ([381]).

([374]) Articolo 3, lettera d), punto i), lettera B), del decreto presidenziale 14086 e articolo 201.7, lettere da a) a c), del regolamento del Procuratore generale. L'Ufficio per la tutela della vita privata e le libertà civili del Dipartimento di giustizia, competente per la fornitura di sostegno amministrativo al DPRC e agli avvocati speciali (cfr. articolo 201.5 del regolamento del Procuratore generale), seleziona un collegio di tre persone a rotazione, al fine di garantire che ciascun collegio disponga di almeno un giudice avente esperienza giudiziaria antecedente (qualora nessuno dei giudici del collegio disponga di tale esperienza, il presidente sarà il giudice scelto per primo da tale Ufficio).

([375]) Articolo 201.4, del regolamento del Procuratore generale. Almeno due avvocati speciali sono nominati dal Procuratore generale, in consultazione con il Segretario al Commercio, il direttore dell'intelligence nazionale e la PCLOB, per due mandati rinnovabili. Gli avvocati speciali devono disporre di un'esperienza adeguata nel settore della tutela della vita privata e del diritto in materia di sicurezza nazionale, essere avvocati esperti, membri attivi in regola dell'ordine forense ed essere debitamente abilitati a esercitare la professione legale. Inoltre, al momento della nomina iniziale, non devono essere stati dipendenti del potere esecutivo nei due anni antecedenti. Per ogni riesame di una domanda, il presidente sceglie un avvocato speciale incaricato di fornire assistenza al collegio (cfr. articolo 201.8, lettera a), del regolamento del Procuratore generale).

([376]) Articolo 201.8, lettera c) e articolo 201.11, del regolamento del Procuratore generale.

([377]) Articolo 3, lettera d), punto i), lettera C), del decreto presidenziale 14086 e articolo 201.8, lettera e), del regolamento del Procuratore generale. L'avvocato speciale non agisce in qualità di agente né ha un rapporto avvocato/cliente con il reclamante.

([378]) Cfr. articolo 201.8, lettere d) ed e), del regolamento del Procuratore generale. Tali questioni sono esaminate innanzitutto dall'Ufficio per la tutela della vita privata e le libertà civili, in consultazione con il pertinente servizio della comunità dell'intelligence, al fine di individuare ed escludere qualsiasi informazione classificata o privilegiata o protetta prima della trasmissione al reclamante. Ulteriori informazioni ricevute dall'avvocato speciale in risposta a tali domande sono incluse nelle osservazioni dell'avvocato speciale al DPRC.

([379]) Articolo 3, lettera d), punto i), lettera D), del decreto presidenziale 14086.

([380]) Articolo 3, lettera d), punto iii), del decreto presidenziale 14086 e articolo 201.9, lettera b), del regolamento del Procuratore generale.

([381]) Articolo 3, lettera d), punto i), lettera E), del decreto presidenziale 14086 e articolo 201.9, lettere da c) ad e), del regolamento del Procuratore generale. Secondo la definizione di "riparazione adeguata" di cui all'articolo 4, lettera a), del decreto presidenziale 14086, il DPRC deve tenere conto delle modalità con cui una violazione del tipo individuato è stata affrontata abitualmente nel momento in cui si pronuncia in merito a una misura di riparazione volta ad affrontare pienamente una violazione; ciò significa che il DPRC considererà, tra gli altri fattori, il modo in cui in passato si è posto rimedio a questioni analoghe di conformità al fine di garantire che il rimedio in questione sia efficace e adeguato.

(191) In tutti i casi il DPRC adotta una decisione scritta a maggioranza dei voti. Nel caso in cui dal riesame emerga una violazione delle norme applicabili, la decisione specificherà un'eventuale riparazione, che contempla la cancellazione dei dati raccolti illecitamente, la cancellazione dei risultati di interrogazioni condotte in modo inadeguato, la limitazione dell'accesso ai dati raccolti legalmente a personale adeguatamente formato o il richiamo di relazioni di intelligence contenenti dati acquisiti senza legittima autorizzazione o diffusi illecitamente ([382]). La decisione del DPRC è vincolante e definitiva per quanto concerne il reclamo promosso presso lo stesso ([383]). Inoltre, se dall'esame condotto emerge una violazione di un'autorità soggetta a vigilanza da parte della Corte FISA, il DPRC deve fornire altresì una relazione classificata al Procuratore generale aggiunto per la sicurezza nazionale, il quale a sua volta è tenuto a segnalare la non conformità alla Corte FISA, che può adottare ulteriori azioni coercitive (conformemente alla procedura illustrata ai considerando 173 e 174) ([384]).

(192) Ogni decisione di un collegio del DPRC è trasmessa all'addetto alla tutela della vita privata e alle libertà civili dell'ODNI ([385]). Nei casi in cui il riesame effettuato dal DPRC è stato avviato a seguito di una domanda presentata dal reclamante, il reclamante è informato tramite l'autorità nazionale del fatto che il DPRC ha completato il riesame e che il riesame non ha individuato alcuna violazione contemplata o il DPRC ha emesso una decisione che richiede una riparazione adeguata ([386]). L'Ufficio per la tutela della vita privata e le libertà civili del Dipartimento della Giustizia tiene un registro di tutte le informazioni esaminate dal DPRC e di tutte le decisioni adottate, che sono messe a disposizione per essere prese in considerazione come precedenti non vincolanti da parte dei futuri collegi del DPRC ([387]).

(193) Il Dipartimento del Commercio è inoltre tenuto a tenere registrazioni in merito a ciascun reclamante che ha presentato un reclamo ([388]). Al fine di migliorare la trasparenza, almeno ogni cinque anni, il Dipartimento del Commercio deve contattare gli enti di intelligence pertinenti al fine di verificare se le informazioni relative a un riesame da parte del DPRC sono state declassificate ([389]). In tal caso l'interessato viene informato del fatto che tali informazioni possono essere disponibili ai sensi del diritto applicabile (ossia che può chiedere l'accesso alle stesse ai sensi della legge sulla libertà d'informazione, cfr. considerando 199).

(194) Infine il corretto funzionamento di questo meccanismo di ricorso sarà soggetto a una valutazione periodica e indipendente. Più specificamente, ai sensi del decreto presidenziale 14086, il funzionamento del meccanismo di ricorso è soggetto a riesame annuale da parte della PCLOB, un organismo indipendente (cfr. considerando 110) ([390]). Nel contesto di tale riesame, la PCLOB valuta tra l'altro se l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e il DPRC hanno trattato i reclami in modo tempestivo; se hanno ottenuto pieno accesso alle informazioni necessarie; se le garanzie sostanziali di cui al decreto presidenziale 14086 sono state adeguatamente prese in considerazione nel processo di riesame; e se la comunità dell'intelligence si sia pienamente conformata a quanto stabilito dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e dal DPRC. La PCLOB elabora una relazione sull'esito del suo riesame che presenta al presidente, al Procuratore generale, al direttore dell'intelligence nazionale, al capo degli enti di intelligence, all'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e alle commissioni in materia di intelligence del Congresso; tale relazione sarà altresì resa pubblica in una versione non classificata, e alimenterà a sua volta il riesame periodico del funzionamento della presente decisione che sarà condotto dalla Commissione. Il Procuratore generale, il direttore dell'intelligence nazionale, l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e i capi degli enti di intelligence sono tenuti ad attuare o a trattare in altro modo tutte le raccomandazioni incluse in tali relazioni. Inoltre la PCLOB emetterà una certificazione pubblica annuale attestante se il meccanismo di ricorso stia trattando o meno i reclami in linea con i requisiti di cui al decreto presidenziale 14086.

([382]) Articolo 4, lettera a), del decreto presidenziale 14086.

([383]) Articolo 3, lettera d), punto ii), del decreto presidenziale 14086 e articolo 201.9, lettera g), del regolamento del Procuratore generale. Dato che la decisione del DPRC è definitiva e vincolante, nessun'altra istituzione esecutiva o amministrativa né alcun altro ente esecutivo o amministrativo (compreso il presidente degli Stati Uniti) può annullare una decisione del DPRC. Ciò è stato confermato anche dalla giurisprudenza della Corte suprema, la quale ha chiarito che, delegando l'autorità unica del Procuratore generale all'interno del ramo esecutivo ai fini dell'adozione di decisioni vincolanti a un organismo indipendente, il Procuratore generale si nega la capacità di dettare in alcun modo la decisione da parte di tale organismo (cfr. *United States ex rel. Accardi/Shaughnessy,* 347 U.S. 260 (1954).

([384]) Articolo 3, lettera d), punto i), lettera F), del decreto presidenziale 14086 e articolo 201.9, lettera i), del regolamento del Procuratore generale.

([385]) Articolo 201.9, lettera h), del regolamento del Procuratore generale.

([386]) Articolo 3, lettera d), punto i), lettera H), del decreto presidenziale 14086 e articolo 201.9, lettera h), del regolamento del Procuratore generale. Per quanto concerne la natura della notifica, cfr. articolo 201.9, lettera h), punto 3, del regolamento del Procuratore generale.

([387]) Articolo 201.9, lettera j), del regolamento del Procuratore generale.

([388]) Articolo 3, lettera d), punto v), lettera A), del decreto presidenziale 14086.

([389]) Articolo 3, lettera d), punto v), del decreto presidenziale 14086.

([390]) Articolo 3, lettera e), del decreto presidenziale 14086. Cfr. anche https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Oltre al meccanismo di ricorso specifico istituito a norma del decreto presidenziale 14086, tutte le persone (indipendentemente dalla loro cittadinanza o dal loro luogo di residenza) dispongono di vie di ricorso dinanzi agli organi giurisdizionali ordinari statunitensi ([391]).

(196) In particolare la FISA e una legge correlata offrono alle persone la possibilità: di avviare una causa civile contro gli USA per ottenere un risarcimento pecuniario quando le informazioni che le riguardano sono state usate o divulgate illecitamente e con dolo ([392]); di adire le vie legali contro agenti del governo statunitense che agiscono nella loro capacità personale per ottenere un risarcimento pecuniario ([393]); 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 USA ([394]). Più in generale, se il governo intende utilizzare le informazioni ottenute nel corso di operazioni di intelligence contro un indiziato nel contesto di un procedimento penale, i requisiti costituzionali e statutari ([395]) impongono l'obbligo di divulgare determinate informazioni, affinché l'indiziato possa contestare la legittimità della raccolta e dell'uso delle prove da parte del governo.

(197) Inoltre vi è una serie di ulteriori possibilità per adire le vie legali contro agenti del governo in caso di 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 ([396]), la legge sulla privacy nelle comunicazioni elettroniche ([397]) e la legge sul diritto alla privacy finanziaria ([398]). Tutte queste azioni legali riguardano dati, obiettivi e/o tipi di accesso specifici (ad es. accesso remoto a un computer via internet) e sono disponibili a determinate condizioni (ad esempio condotta intenzionale/dolosa, abuso di potere, danno).

(198) Una possibilità di ricorso più generale è offerta dalla legge sulle procedure amministrative ([399]), 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 ([400]), 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 ([401]). Ad esempio nel 2015 un organo giurisdizionale di appello federale si è pronunciato in merito a un'istanza in merito alla legge sulle procedure amministrative secondo cui la raccolta in blocco di metadati telefonici da parte del governo statunitense non era autorizzata dall'articolo 501 FISA ([402]).

([391]) L'accesso a tali vie di ricorso è subordinato alla dimostrazione della "legittimazione ad agire". Tale norma, che si applica a qualsiasi persona indipendentemente dalla cittadinanza, deriva dal requisito del "caso o controversia" stabilito dall'articolo III della costituzione degli Stati Uniti. Secondo la Corte suprema, ciò richiede che 1) la persona abbia subito un "pregiudizio a livello fattuale" (ossia un pregiudizio di un interesse giuridicamente tutelato che è concreto e dettagliato e reale o imminente); 2) vi sia un nesso causale tra il pregiudizio e il comportamento contestato dinanzi all'organo giurisdizionale; e 3) sia probabile, piuttosto che speculativo, che una decisione favorevole del giudice affronti il pregiudizio (cfr. *Lujan/Defenders of Wildlife*, 504 U.S. 555 (1992)).

([392]) Codice degli Stati Uniti, titolo 18, articolo 2712.

([393]) Codice degli Stati Uniti, titolo 50, articolo 1810.

([394]) Codice degli Stati Uniti, titolo 50, articolo 1806.

([395]) *Cfr.*, rispettivamente, la sentenza *Brady/Maryland*, 373 U.S. 83 (1963), la legge Jencks e il codice degli Stati Uniti, titolo 18, articolo 3500.

([396]) Codice degli Stati Uniti, titolo 18, articolo 1030.

([397]) Codice degli Stati Uniti, titolo 18, articoli 2701-2712.

([398]) Codice degli Stati Uniti, titolo 12, articolo 3417.

([399]) Codice degli Stati Uniti, titolo 5, articolo 702.

([400]) 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, titolo 5, articolo 704).

([401]) Codice degli Stati Uniti, titolo 5, articolo 706, punto 2), lettera A).

([402]) *American Civil Liberties Union/Clapper*, 785 F.3d 787 (2d Cir. 2015). Il programma di raccolta in blocco di dati di telefonia contestato in tale causa è stato cessato nel 2015 con la legge USA FREEDOM.

(199) Infine, oltre ai mezzi di ricorso di cui ai considerando da 176 a 198, chiunque ha il diritto di chiedere l'accesso alle registrazioni esistenti degli enti federali ai sensi della legge sulla libertà d'informazione, anche se queste contengono dati personali ([403]). L'ottenimento di tale accesso può facilitare altresì l'avvio di procedimenti dinanzi agli organi giurisdizionali ordinari, anche a sostegno della legittimazione ad agire. Gli enti possono non divulgare informazioni che rientrano in determinate eccezioni elencate, compreso l'accesso alle informazioni classificate in materia di sicurezza nazionale e alle informazioni relative alle indagini di autorità di contrasto ([404]), ma i reclamanti che non sono soddisfatti della risposta hanno la possibilità di contestarla chiedendo un controllo amministrativo e, successivamente, giurisdizionale (dinanzi agli organi giurisdizionali federali) ([405]).

(200) Ne consegue che quando le autorità degli Stati Uniti preposte all'attività di contrasto e alla sicurezza nazionale accedono a dati personali che rientrano nell'ambito di applicazione della presente decisione, tale accesso è disciplinato da un quadro giuridico che stabilisce le condizioni alle quali può avvenire l'accesso e assicurano che l'accesso e l'ulteriore uso dei dati siano limitati a quanto necessario e proporzionati all'obiettivo di interesse pubblico perseguito. Tali garanzie possono essere invocate da persone che godono di diritti di ricorso effettivi.

4. **CONCLUSIONI**

(201) La Commissione ritiene che gli Stati Uniti, attraverso i principi emanati dal Dipartimento del Commercio degli Stati Uniti, garantiscano un livello di protezione dei dati personali trasferiti dall'Unione alle organizzazioni certificate negli Stati Uniti nell'ambito del quadro UE-USA per la protezione dei dati personali sostanzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

(202) Inoltre la Commissione ritiene che l'effettiva applicazione dei principi sia garantita dagli obblighi di trasparenza e dall'amministrazione del DPF da parte della Dipartimento del Commercio. Nel complesso i meccanismi di vigilanza e i mezzi di ricorso previsti dal diritto statunitense consentono altresì di individuare e punire nella pratica eventuali violazioni delle norme in materia di protezione dei dati e offrono all'interessato mezzi di ricorso per ottenere l'accesso ai dati personali che lo riguardano e, in ultima analisi, la rettifica o la cancellazione di tali dati.

(203) Infine, sulla base delle informazioni disponibili sull'ordinamento giuridico statunitense, comprese le informazioni figuranti negli allegati VI e VII, la Commissione ritiene che qualsiasi ingerenza attuata nell'interesse pubblico, in particolare per finalità di contrasto penale e di sicurezza nazionale, da parte di autorità pubbliche statunitensi in relazione ai diritti fondamentali delle persone i cui dati personali sono trasferiti dall'Unione agli Stati Uniti nell'ambito del quadro UE-USA per la protezione dei dati personali, sarà limitata a quanto strettamente necessario a conseguire l'obiettivo legittimo in questione, e che contro tali ingerenze esista una tutela giuridica efficace. Pertanto, alla luce delle conclusioni di cui sopra, è opportuno decidere che gli Stati Uniti garantiscono un livello di protezione adeguato ai sensi dell'articolo 45 del regolamento (UE) 2016/679, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea, per i dati personali trasferiti dall'Unione europea a organizzazioni certificate ai sensi del quadro UE-USA per la protezione dei dati personali.

(204) Dato che le limitazioni, le garanzie e il meccanismo di ricorso istituiti dal decreto presidenziale 14086 sono elementi essenziali del quadro giuridico statunitense su cui si basa la valutazione della Commissione, l'adozione della presente decisione si fonda in particolare sull'adozione di politiche e procedure aggiornate per l'attuazione del decreto presidenziale 14086 da parte di tutti gli enti di intelligence statunitensi e sulla designazione dell'Unione quale organizzazione qualificata ai fini del meccanismo di ricorso che hanno avuto luogo rispettivamente il 3 luglio 2023 (cfr. considerando 126) e il 30 giugno 2023 (cfr. considerando 176).

([403]) Codice degli Stati Uniti, titolo 5, articolo 552. Leggi analoghe vigono a livello di Stati federati.

([404]) 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)). I criteri e la durata della classificazione sono stabiliti nel decreto presidenziale 13526, il quale prevede, in linea di principio, che si debba stabilire una data o un evento per la declassificazione in base alla durata della sensibilità delle informazioni sotto il profilo della sicurezza nazionale, che corrisponde al momento in cui le informazioni devono essere automaticamente declassificate (cfr. articolo 1.5 del decreto presidenziale 13526).

([405]) Il giudice emette una decisione nuova in merito all'eventualità o meno che le registrazioni siano legittimamente trattenute e può costringere il governo a fornire l'accesso alle registrazioni in questione (codice degli Stati Uniti, titolo 5, articolo 552, lettera a), punto 4), lettera B)).

5. EFFETTI DELLA PRESENTE DECISIONE E AZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI

(205) Gli Stati membri e i loro organi sono tenuti ad adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, che si presumono 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.

(206) Di conseguenza, una decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 è vincolante per tutti gli organi degli Stati membri che ne sono i destinatari, comprese le autorità di controllo indipendenti. In particolare i trasferimenti da un titolare del trattamento o un responsabile del trattamento nell'Unione verso organizzazioni certificate negli Stati Uniti possono avvenire senza la necessità di ottenere ulteriori autorizzazioni.

(207) È opportuno ricordare che, ai sensi dell'articolo 58, paragrafo 5, del regolamento (UE) 2016/679, e come spiegato dalla Corte di giustizia nella sentenza *Schrems* ([406]), quando un'autorità nazionale di protezione dei dati mette in dubbio, anche in seguito a un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona fisica concernenti la tutela della vita privata e la protezione dei dati, il diritto nazionale deve prevedere mezzi di ricorso per l'affermazione di tali obiezioni dinanzi un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia ([407]).

6. MONITORAGGIO E RIESAME DELLA PRESENTE DECISIONE

(208) Secondo la giurisprudenza della Corte di giustizia ([408]), e come riconosciuto dall'articolo 45, paragrafo 4, del regolamento (UE) 2016/679, la Commissione dovrebbe monitorare costantemente gli sviluppi nel paese terzo registrati dopo l'adozione di una decisione di adeguatezza, al fine di valutare se il paese terzo continui a garantire un livello di protezione sostanzialmente equivalente. Tale verifica è in ogni caso obbligatoria quando la Commissione riceve informazioni che fanno sorgere un dubbio giustificato al riguardo.

(209) La Commissione dovrebbe pertanto controllare su base continuativa la situazione negli Stati Uniti per quanto riguarda il quadro giuridico e la prassi effettiva del trattamento dei dati personali valutati dalla presente decisione. Per agevolare tale processo, le autorità degli Stati Uniti dovrebbero informare tempestivamente la Commissione in merito a sviluppi sostanziali dell'ordinamento giuridico degli Stati Uniti che abbiano un impatto sul quadro giuridico oggetto della presente decisione, nonché di qualsiasi evoluzione delle pratiche relative al trattamento dei dati personali oggetto della presente decisione, per quanto riguarda sia il trattamento di dati personali da parte di organizzazioni certificate negli Stati Uniti, sia le limitazioni e le garanzie applicabili all'accesso ai dati personali da parte delle autorità pubbliche.

(210) Inoltre, al fine di consentire alla Commissione di svolgere in modo efficace la propria funzione di monitoraggio, gli Stati membri dovrebbero informarla delle eventuali azioni intraprese dalle autorità nazionali di protezione dei dati, in particolare per quanto riguarda eventuali domande o reclami presentati da interessati dell'Unione relativamente al trasferimento di dati personali dall'Unione verso organizzazioni certificate negli Stati Uniti. La Commissione dovrebbe inoltre essere informata di eventuali indicazioni del fatto che le azioni delle autorità pubbliche degli Stati Uniti responsabili della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati ovvero della sicurezza nazionale, compresi gli organismi di vigilanza, non garantiscono il necessario livello di protezione.

([406]) *Schrems*, punto 65.

([407]) *Schrems*, punto 65: a tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione.

([408]) *Schrems*, punto 76.

(211) In applicazione dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 ([409]), la Commissione, in seguito all'adozione della presente decisione, dovrebbe riesaminare periodicamente se le conclusioni relative all'adeguatezza del livello di protezione garantito dagli Stati Uniti nell'ambito del DPF UE-USA continuino ad essere giustificate sotto il profilo fattuale e giuridico. Poiché in particolare il decreto presidenziale 14086 e il regolamento del Procuratore generale richiedono la creazione di meccanismi nuovi e l'attuazione di garanzie nuove, la presente decisione dovrebbe essere oggetto di un primo riesame entro un anno dalla sua entrata in vigore, al fine di verificare se tutti gli elementi pertinenti siano stati pienamente attuati e funzionino efficacemente nella pratica. A seguito del primo riesame, e tenuto conto del suo esito, la Commissione deciderà, in stretta consultazione con il comitato istituito a norma dell'articolo 93, paragrafo 1, del regolamento (UE) 2016/679, la frequenza dei riesami futuri ([410]).

(212) Al fine di effettuare i riesami, la Commissione dovrebbe incontrare il Dipartimento del Commercio, l'FTC e il DOT accompagnati, se del caso, da altri dipartimenti ed enti coinvolti nell'attuazione del DPF UE-USA, nonché, per le questioni relative all'accesso ai dati da parte di pubbliche amministrazioni, rappresentanti del Dipartimento della Giustizia, dell'ODNI (compreso l'addetto alla tutela della vita privata e alle libertà civili), di altri servizi della comunità dell'intelligence, del DPRC e degli avvocati speciali. Alla riunione dovrebbero poter partecipare i rappresentanti dei membri del comitato europeo per la protezione dei dati.

(213) I riesami in questione dovrebbero riguardare tutti gli aspetti del funzionamento della presente decisione per quanto concerne il trattamento di dati personali negli Stati Uniti, in particolare: l'applicazione e l'attuazione dei principi, con particolare riguardo alle tutele offerte in caso di trasferimenti successivi; gli sviluppi pertinenti della giurisprudenza; l'efficacia dell'esercizio dei diritti individuali; il controllo e l'applicazione del rispetto dei principi; nonché le limitazioni e le garanzie per quanto concerne l'accesso da parte di pubbliche amministrazioni, in particolare in relazione all'attuazione e all'applicazione delle garanzie introdotte dal decreto presidenziale 14086, anche attraverso politiche e procedure sviluppate dagli enti di intelligence; l'interazione tra il decreto presidenziale 14086 e l'articolo 702 FISA e il decreto presidenziale 12333; e l'efficacia dei meccanismi di vigilanza e delle vie di ricorso (compreso il funzionamento del nuovo meccanismo di ricorso istituito a norma del decreto presidenziale 14086). Nel contesto di tali riesami si presterà attenzione anche alla cooperazione tra le autorità di protezione dei dati e le autorità competenti degli Stati Uniti, anche tramite lo sviluppo di orientamenti e di altri strumenti interpretativi sull'applicazione dei principi nonché su altri aspetti del funzionamento del quadro in questione.

(214) La Commissione dovrebbe elaborare, sulla base del riesame, una relazione pubblica da presentare al Parlamento europeo e al Consiglio.

7. SOSPENSIONE, ABROGAZIONE O MODIFICA DELLA PRESENTE DECISIONE

(215) Se dalle informazioni disponibili, in particolare da quelle risultanti dal monitoraggio della presente decisione o fornite dalle autorità statunitensi o degli Stati membri, risulta che il livello di protezione offerto ai dati trasferiti nell'ambito della presente decisione potrebbe non essere più adeguato, la Commissione dovrebbe informare prontamente le autorità statunitensi competenti e richiedere che adottino misure adeguate entro un periodo di tempo specificato e ragionevole.

(216) Laddove alla scadenza di tale periodo di tempo specificato le autorità statunitensi competenti non abbiano adottato tali misure o non dimostrino altrimenti in modo soddisfacente che la presente decisione continua ad essere basata su un livello di protezione adeguato, la Commissione avvierà la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679 al fine di sospendere o abrogare parzialmente o completamente la presente decisione.

(217) In alternativa, la Commissione avvierà tale procedura al fine di modificare la presente decisione, in particolare imponendo ulteriori condizioni per i trasferimenti di dati o limitando il riconoscimento dell'adeguatezza soltanto ai trasferimenti di dati per cui continua ad essere garantito un livello di protezione adeguato.

([409]) Conformemente all'articolo 45, paragrafo 3, del regolamento (UE) 2016/679, "[l]'atto di esecuzione prevede un meccanismo di riesame periodico, [...] che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale".

([410]) L'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 dispone che il riesame periodico abbia luogo almeno ogni quattro anni. Cfr. anche comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01.

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

(a) indicazioni del fatto che le organizzazioni che hanno ricevuto dati personali dall'Unione a norma della presente decisione non rispettano i principi e che tale inadempienza non è affrontata in modo efficace dai competenti organismi di vigilanza e di applicazione;

(b) indicazioni del fatto che le autorità statunitensi non rispettano le condizioni e le limitazioni applicabili all'accesso da parte delle autorità pubbliche statunitensi per finalità di contrasto e di sicurezza nazionale ai dati personali trasferiti nell'ambito del DPF UE-USA; oppure

(c) mancata risposta efficace ai reclami degli interessati dell'Unione, anche da parte dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e/o del DPRC.

(219) La Commissione dovrebbe inoltre valutare l'opportunità di avviare la procedura di modifica, sospensione o abrogazione della presente decisione se le autorità statunitensi competenti non forniscano le informazioni o i chiarimenti necessari alla valutazione del livello di protezione offerto ai dati personali trasferiti dall'Unione agli Stati Uniti o per quanto concerne la conformità alla presente decisione. A tale riguardo, la Commissione dovrebbe tener conto della misura in cui le informazioni pertinenti possono essere ottenute da altre fonti.

(220) In ragione di motivi imperativi d'urgenza debitamente giustificati, ad esempio se il decreto presidenziale 14086 o il regolamento del Procuratore generale fossero modificati in modo tale da compromettere il livello di protezione descritto nella presente decisione o se la designazione del Procuratore generale dell'Unione in qualità di organizzazione qualificata ai fini del meccanismi di ricorso viene revocata, la Commissione farà ricorso alla possibilità di adottare, conformemente alla procedura di cui all'articolo 93, paragrafo 3, del regolamento (UE) 2016/679, atti di esecuzione immediatamente applicabili destinati a sospendere, abrogare o modificare la presente decisione.

8. **CONSIDERAZIONI FINALI**

(221) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ([411]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(222) Il Parlamento europeo ha adottato una risoluzione sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati ([412]).

(223) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93, paragrafo 1, del regolamento (UE) 2016/679,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 45 del regolamento (UE) 2016/679, gli Stati Uniti d'America garantiscono un livello di protezione adeguato dei dati personali trasferiti dall'Unione alle organizzazioni presenti negli Stati Uniti che figurano nell'elenco degli aderenti al quadro per la protezione dei dati personali, tenuto e pubblicato dal Dipartimento del Commercio degli Stati Uniti in conformità dell'allegato I, parte I, punto 3.

Articolo 2

Quando, al fine di proteggere le persone con riguardo al trattamento dei loro dati personali, le autorità competenti degli Stati membri esercitano i poteri di cui all'articolo 58 del regolamento (UE) 2016/ 679 in relazione ai trasferimenti di cui all'articolo 1 della presente decisione, lo Stato membro interessato ne informa senza ritardo la Commissione.

([411]) Parere 5/2023 relativo al progetto di decisione di esecuzione della Commissione europea per quanto riguarda la protezione adeguata dei dati personali nel contesto del quadro per la protezione dei dati UE-USA del 28 febbraio 2023.

([412]) Risoluzione del Parlamento europeo dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati (2023/2501(RSP)).

Articolo 3

1. La Commissione monitora costantemente l'applicazione del quadro giuridico oggetto della presente decisione, comprese le condizioni in cui sono effettuati i trasferimenti successivi, sono esercitati i diritti individuali e le autorità pubbliche degli Stati Uniti hanno accesso ai dati trasferiti sulla base della presente decisione, al fine di valutare se gli Stati Uniti continuino a garantire un livello di protezione adeguato ai sensi dell'articolo 1.

2. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui risulta che gli organi degli Stati Uniti cui la legge conferisce il potere di far rispettare i principi enunciati nell'allegato I non mettono a disposizione meccanismi efficaci di rilevamento e di vigilanza che consentano d'individuare le violazioni dei principi di cui all'allegato I 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 loro dati personali, compiute dalle autorità pubbliche statunitensi competenti della sicurezza nazionale, dell'applicazione della legge o di altro interesse pubblico, vadano oltre quanto necessario e proporzionato e/o che contro le ingerenze di tale natura non esista una tutela giuridica efficace.

4. Dopo un anno dalla data di notifica della presente decisione agli Stati membri, e successivamente secondo una cadenza che sarà decisa in stretta consultazione con il comitato costituito a norma dell'articolo 93, paragrafo 1, del regolamento (UE) 2016/679 e con il comitato europeo per la protezione dei dati, la Commissione verifica la constatazione enunciata all'articolo 1, paragrafo 1, in base a tutte le informazioni disponibili, comprese quelle ottenute tramite il riesame effettuato congiuntamente con le autorità competenti degli Stati Uniti.

5. Qualora abbia indicazioni del fatto che non è più garantito un livello di protezione adeguato, la Commissione ne informa le autorità statunitensi competenti. Se necessario, essa decide di sospendere, modificare o abrogare la presente decisione o di limitarne l'ambito di applicazione, conformemente all'articolo 45, paragrafo 5, del regolamento (UE) 2016/679. La Commissione può inoltre adottare una tale decisione se la mancanza di cooperazione del governo statunitense le impedisce di stabilire se gli Stati Uniti continuino a garantire un livello di protezione adeguato.

Articolo 4

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 10 luglio 2023

Per la Commissione
Didier REYNDERS
Membro della Commissione

ALLEGATO I

PRINCIPI DEL QUADRO UE-USA PER LA PROTEZIONE DEI DATI PERSONALI EMANANTI DAL DIPARTIMENTO DEL COMMERCIO DEGLI STATI UNITI D'AMERICA

I. CONSIDERAZIONI GENERALI

1. Sebbene gli Stati Uniti d'America ("Stati Uniti") e l'Unione europea ("UE") condividano l'impegno a rafforzare la tutela della vita privata, lo Stato di diritto e il riconoscimento dell'importanza dei flussi transatlantici di dati per i cittadini, le economie e le società dei rispettivi paesi, gli Stati Uniti adottano un approccio diverso in materia di tutela della vita privata rispetto a quello dell'UE. Gli Stati Uniti si basano su un approccio settoriale costituito da una combinazione di legislazione, regolamentazione e autoregolamentazione. Il Dipartimento del Commercio degli Stati Uniti ("il Dipartimento") emette i principi del quadro UE-USA per la protezione dei dati personali, compresi i principi supplementari (collettivamente "i principi") e l'allegato I dei principi ("allegato I"), in virtù della propria autorità statutaria di favorire, promuovere e sviluppare il commercio internazionale (codice degli Stati Uniti, titolo 15, articolo 1512). I principi sono stati messi a punto in consultazione con la Commissione europea ("la Commissione"), con l'industria e con altri portatori di interessi per facilitare gli scambi commerciali fra gli Stati Uniti e l'UE. I principi, che costituiscono una componente fondamentale del quadro UE-USA per la protezione dei dati personali ("DPF UE-USA"), dotano le organizzazioni presenti negli Stati Uniti di un meccanismo affidabile per il trasferimento di dati personali dall'UE agli Stati Uniti, garantendo nel contempo che gli interessati dell'UE continuino 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. I principi sono destinati unicamente alle organizzazioni ammissibili presenti negli Stati Uniti che ricevono dati personali dall'UE, al fine di permettere loro di conformarsi ai requisiti del DPF UE-USA e, quindi, di ottenere i benefici della decisione di adeguatezza della Commissione ([1]). I principi lasciano impregiudicata l'applicazione del regolamento (UE) 2016/679 ("il regolamento generale sulla protezione dei dati" o "GDPR") ([2]) applicabile al trattamento dei dati personali negli Stati membri dell'UE. I principi non determinano limiti agli obblighi in materia di privacy altrimenti applicabili in forza della legge statunitense.

2. Per ricevere dati personali trasferiti dall'UE in virtù del DPF UE-USA, un'organizzazione deve autocertificare l'adesione ai principi presso il Dipartimento o un'altra persona (fisica o giuridica) da esso designata. Sebbene la decisione di un'organizzazione di aderire in questo modo al DPF UE-USA 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 al DPF UE-USA un'organizzazione deve: a) essere sottoposta all'autorità d'indagine e di controllo della Commissione federale del Commercio (FTC), del Dipartimento dei Trasporti (DOT) degli Stati Uniti 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; e d) dare loro attuazione integrale ([3]). L'inosservanza da parte dell'organizzazione è perseguibile da parte del FTC ai sensi dell'articolo 5 della legge sulla Commissione federale del Commercio, che proibisce gli atti sleali o ingannevoli nel commercio o aventi ripercussioni sul commercio (codice degli Stati Uniti, titolo 15, articolo 45), da parte del DOT ai sensi del codice degli Stati Uniti, titolo 49, articolo 41712, che vieta al vettore o al rivenditore che fa servizio di biglietteria, nell'attività di trasporto aereo o di vendita di trasporto aereo, qualsiasi pratica sleale o ingannevole, o a norma di altre leggi o regolamenti che vietano tali atti.

([1]) Se la decisione della Commissione sull'adeguatezza della protezione offerta dal DPF UE-USA si applicherà anche a Islanda, Liechtenstein e Norvegia, tale DPF riguarderà anche tali tre paesi oltre all'UE. In tal caso, i riferimenti all'UE e ai suoi Stati membri si intendono quindi comprensivi di Islanda, Liechtenstein e Norvegia.

([2]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

([3]) I principi dello scudo UE-USA per la privacy sono stati modificati e costituiscono ora i "principi del quadro UE-USA per la protezione dei dati personali" (principi del DPF UE-USA). (*Cfr.* il principio supplementare sull'autocertificazione).

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 in questione ("elenco degli aderenti al DPF" o "elenco"). I benefici derivanti dall'adesione al DPF UE-USA sono attivati a partire dalla data in cui il Dipartimento inserisce l'organizzazione nell'elenco. Il Dipartimento depenna dall'elenco le organizzazioni che abbandonano volontariamente il DPF UE-USA o che non completano la loro ricertificazione annuale presso il Dipartimento; tali organizzazioni devono continuare ad applicare i principi alle informazioni personali ricevute nell'ambito del DPF UE-USA e rinnovare ogni anno presso il Dipartimento l'impegno in tal senso (ossia fintantoché conservano tali informazioni), fornire una protezione "adeguata" delle informazioni con altri mezzi autorizzati (ad esempio utilizzando un contratto che rispecchi pienamente i requisiti delle pertinenti clausole contrattuali tipo adottate dalla Commissione), oppure restituire o cancellare le informazioni. Il Dipartimento depenna dall'elenco anche le organizzazioni che hanno commesso reiterate inosservanze dei principi e tali organizzazioni devono restituire o cancellare le informazioni personali ricevute nell'ambito del DPF UE-USA. L'organizzazione depennata dall'elenco non è più ammissibile a beneficiare della decisione di adeguatezza della Commissione che le consente di ricevere informazioni personali dall'UE.

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 al DPF UE-USA; che il depennamento dall'elenco implica che l'organizzazione non può dichiararsi conforme al DPF UE-USA 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 di ricevere informazioni personali dall'UE. L'FTC, il DOT o altre autorità preposte all'applicazione della legge possono avviare un'azione coercitiva nei confronti dell'organizzazione che, depennata dall'elenco, continua a millantare l'adesione al DPF UE-USA o a lasciare altrimenti intendere che vi partecipa.

5. L'adesione a tali principi può essere limitata: a) alla misura necessaria per ottemperare all'ordinanza di un organo giurisdizionale o per soddisfare esigenze di interesse pubblico, di contrasto o di sicurezza nazionale, anche nel caso in cui le disposizioni legislative o regolamentari creino obblighi contrastanti; b) da disposizioni legislative, ordinanze di un organo giurisdizionale o regolamentari che comportano 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 il GDPR rende possibili eccezioni o deroghe, secondo condizioni stabilite in tale atto, a patto che tali eccezioni o deroghe si applichino in contesti comparabili. In tale contesto le garanzie previste dalla legge statunitense per tutelare la vita privata e le libertà civili comprendono quelle richieste dal decreto presidenziale 14086 ([4]) alle condizioni ivi stabilite (compresi i requisiti di necessità e proporzionalità). 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, sforzandosi di indicare nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno applicate le eccezioni ammesse dal punto 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 al DPF UE-USA, 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 del DPF UE-USA 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.

([4]) Decreto presidenziale del 7 ottobre 2022, "Enhancing Safeguards for United States Signals Intelligence Activities".

7. Alle questioni riguardanti l'interpretazione e il rispetto dei principi e alle relative politiche della privacy delle organizzazioni aderenti al DPF UE-USA si applica la normativa statunitense, eccetto nel caso in cui l'organizzazione si sia impegnata a cooperare con le autorità europee di protezione dei dati. Salvo disposizioni contrarie, tutte le disposizioni di cui ai principi 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 il GDPR, che un'organizzazione presente negli Stati Uniti riceve dall'UE 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 e dell'allegato I dei principi è la data di entrata in vigore della decisione di adeguatezza della Commissione europea.

II. PRINCIPI

1. Informativa

a. L'organizzazione deve informare le persone:

   i. della sua adesione al DPF UE-USA, fornendo un collegamento ipertestuale o l'indirizzo internet in cui è reperibile l'elenco degli aderenti al DPF;

   ii. dei tipi di dati personali raccolti e, se del caso, dei soggetti o delle filiali statunitensi 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 del DPF UE-USA;

   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 DOT o di altro ente competente per legge autorizzato negli USA;

   xi. della possibilità di chiedere, a determinate condizioni, un arbitrato vincolante ([5]);

   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; e

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

([5]) Cfr. ad esempio lettera c) del principio su ricorso, controllo e responsabilità.

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 (ossia la 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 TRASFERIMENTO SUCCESSIVO**

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; e 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 ([6]). 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 ([7]) 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 DPF UE-USA. 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.

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; e

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 al DPF UE-USA. 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 cooperare 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.

([6]) 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.

([7]) 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.

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 trasferimento successivo, l'organizzazione aderente è responsabile del trattamento dei dati personali ricevuti nell'ambito del DPF UE-USA e inoltrati a un terzo che agisce come suo procuratore. In base ai principi l'organizzazione aderente 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 un'organizzazione è oggetto dell'ordinanza di un organo giurisdizionale che si fonda su una mancata conformità o dell'ordinanza di un ente statunitense competente per legge (ad esempio, FTC o DOT) elencato nei principi o in un futuro allegato dei principi che si fonda su una mancata conformità, l'organizzazione in questione rende pubbliche tutte le pertinenti sezioni relative al DPF UE-USA di qualsiasi relazione di conformità o di valutazione presentata all'organo giurisdizionale o all'ente statunitense competente per legge nella misura 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. L'FTC e il DOT trattano in via prioritaria i casi d'inosservanza dei principi ad essa sottoposti dal Dipartimento e dalle autorità degli Stati membri dell'UE e condividono 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 (ossia facoltà di accettazione) per i dati sensibili se il trattamento è:

i. nel vitale interesse del diretto 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, 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 di cui ai principi 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, i prestatori 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. Il DPF UE-USA 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, 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 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 cooperare con le autorità di protezione dei dati secondo le modalità esposte qui di seguito. Nell'ambito del DPF UE-USA 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; e 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 cooperazione con le autorità di protezione dei dati.

b. Per affermare l'impegno a cooperare con le autorità di protezione dei dati, nell'autocertificazione inerente al DPF UE-USA presentata al Dipartimento (*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 cooperare con le autorità di protezione dei dati;

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

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, 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 cooperazione 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 UE, 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 DPF UE-USA. Il parere mira a garantire che i principi 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 cooperare con le autorità di protezione dei dati per le finalità del DPF UE-USA, 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 della 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 all'FTC, al DOT 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 cooperazione, il quale è quindi da considerarsi nullo e privo di effetti. In quest'ultimo caso il comitato informa il Dipartimento affinché modifichi di conseguenza l'elenco degli aderenti al DPF. La mancanza all'impegno di cooperare con le autorità di protezione dei dati o l'inosservanza dei principi sono perseguibili in quanto pratica ingannevole a norma dell'articolo 5 della legge sull'FTC (codice degli Stati Uniti, titolo 15, articolo 45), del codice degli Stati Uniti, titolo 49, articolo 41712 o di altra analoga disposizione di legge.

d. L'organizzazione che vuole far rientrare nel regime del DPF UE-USA i dati sulle risorse umane trasferiti dall'UE nell'ambito di un rapporto di lavoro deve impegnarsi a cooperare 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. Tale organizzazione 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. L'ammontare della quota è determinato dal Dipartimento previa consultazione della Commissione. La riscossione del canone può essere effettuata da un terzo scelto dal Dipartimento per fungere da depositario dei fondi raccolti per tale finalità. Il Dipartimento coopera strettamente con la Commissione e le autorità di protezione dei dati al fine di stabilire procedure adeguate per la distribuzione dei fondi riscossi tramite la quota, nonché altri aspetti procedurali e amministrativi del comitato. Il Dipartimento e la Commissione possono decidere di modificare la frequenza di riscossione della quota.

6. **Autocertificazione**

a. I benefici derivanti dall'adesione al DPF UE-USA sono attivati a partire dalla data in cui il Dipartimento inserisce l'organizzazione nell'elenco degli aderenti al DPF. Il dipartimento inserisce un'organizzazione nell'elenco soltanto dopo aver accertato che la domanda di autocertificazione iniziale dell'organizzazione è completa e depenna detta organizzazione dall'elenco qualora l'organizzazione revochi la sua adesione volontariamente, non completi la sua ricertificazione annuale o persista nel non rispettare i principi (*cfr.* principio supplementare su composizione delle controversie e controllo dell'applicazione).

b. Ai fini dell'autocertificazione iniziale o della ricertificazione successiva dell'aderenza al DPF UE-USA, un'organizzazione deve presentare ogni volta al Dipartimento un documento emesso da un dipendente dell'organizzazione per conto di quest'ultima attestante che l'organizzazione intende autocertificare o ricertificare (a seconda dei casi) la propria adesione ai principi ([8]), contenente quanto meno le informazioni seguenti:

([8]) Tale presentazione deve essere effettuata tramite il sito web del Dipartimento dedicato al DPF da una persona che opera all'interno dell'organizzazione autorizzata a rilasciare dichiarazioni per conto dell'organizzazione e di qualsiasi entità interessata in merito alla sua adesione ai principi.

i. il nome dell'organizzazione statunitense che si autocertifica o si ricertifica, nonché il nome o i nomi di tutti i soggetti o di tutte le filiali statunitensi di tale organizzazione che aderiscono anch'essi/e ai principi che l'organizzazione intende rispettare;

ii. una descrizione delle attività svolte dall'organizzazione in rapporto alle informazioni personali che proverrebbero dall'UE nell'ambito del DPF UE-USA;

iii. una descrizione della politica o delle politiche pertinenti della privacy seguite 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; e

2. la data effettiva di attuazione della politica;

iv. l'ufficio referente all'interno dell'organizzazione per il trattamento dei reclami, le richieste di accesso e qualsiasi altra questione che può porsi in relazione ai principi ([9]), compresi:

1. il nome, la mansione (a seconda dei casi), l'indirizzo di posta elettronica e il numero di telefono della persona o delle persone interessate o dell'ufficio o degli uffici referenti pertinenti all'interno dell'organizzazione; e

2. l'indirizzo postale statunitense pertinente per l'organizzazione;

v. 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);

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

vii. il metodo di verifica (ossia l'autovalutazione; o le verifiche esterne della conformità, compresi i terzi che effettuano tali riesami) ([10]); e

viii. il meccanismo o i meccanismi di ricorso indipendente pertinenti disponibili per le indagini in merito a reclami irrisolti relativi ai principi ([11]).

c. L'organizzazione che lo desidera può far rientrare nel regime del DPF UE-USA 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. Inoltre l'organizzazione deve dichiarare l'intenzione in tal senso nell'autocertificazione iniziale, così come in qualsiasi ricertificazione, impegnandosi a cooperare 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.

([9]) Il "contatto principale dell'organizzazione" o il "dipendente dell'organizzazione" non può essere una persona esterna all'organizzazione (ad esempio, un consulente esterno).

([10]) *Cfr.* il principio supplementare sulla verifica.

([11]) *Cfr.* il principio supplementare su composizione delle controversie e controllo dell'applicazione.

d. Il Dipartimento tiene e mette a disposizione del pubblico l'elenco degli aderenti al DPF contenente le organizzazioni che hanno presentato autocertificazioni iniziali complete e aggiorna tale elenco sulla base delle ricertificazioni annuali complete, nonché delle notifiche ricevute ai sensi del principio supplementare sulla composizione delle controversie e sul controllo dell'applicazione. La ricertificazione deve essere presentata con cadenza almeno annuale; in caso contrario, l'organizzazione è depennata dall'elenco e non può più godere dei vantaggi derivanti dall'adesione al DPF UE-USA. Tutte le organizzazioni che il dipartimento inserisce nell'elenco degli aderenti al DPF devono disporre di politiche della privacy pertinenti conformi al principio dell'informativa e dichiarare in tali politiche che rispettano i principi ([12]). Se consultabile in rete, la politica della privacy dell'organizzazione deve contenere un collegamento ipertestuale al sito web del Dipartimento dedicato al DPF 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 relativi ai principi a titolo gratuito per la persona.

e. I principi si applicano immediatamente alla data dell'autocertificazione. Le organizzazioni aderenti che si sono precedentemente autocertificate in base ai principi dello scudo UE-USA per la privacy dovranno aggiornare le loro politiche della privacy affinché facciano invece riferimento ai "principi del quadro UE-USA per la protezione dei dati personali". Tali organizzazioni inseriscono detto riferimento quanto prima, e in ogni caso entro tre mesi dalla data di entrata in vigore dei principi del DPF UE-USA.

f. Un'organizzazione deve attenersi ai principi per tutti i dati personali ricevuti dall'UE in virtù del DPF UE-USA. Per i dati personali ricevuti nel periodo in cui l'organizzazione gode dei vantaggi del DPF UE-USA, 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. Un'organizzazione che desideri abbandonare il DPF UE-USA deve notificarlo preventivamente al Dipartimento. Tale notifica deve indicare altresì cosa farà l'organizzazione con i dati personali ricevuti ai sensi del DPF UE-USA (ossia conservazione, restituzione o cancellazione dei dati e, in caso di conservazione, occorre indicare i mezzi autorizzati tramite i quali fornirà protezione a tali dati). L'organizzazione che, pur abbandonando il DPF UE-USA, 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); in caso contrario, l'organizzazione deve restituire o cancellare le informazioni ([13]). Un'organizzazione che abbandona il DPF UE-USA elimina dalla sua politica della privacy qualsiasi riferimento al DPF che lasci intendere che continua ad aderirvi e a godere dei benefici che ne derivano.

([12]) Un'organizzazione che si autocertifica per la prima volta non può asserire l'adesione al DPF UE-USA nella sua politica della privacy finale fino a quando il Dipartimento non le notifichi la possibilità di procedere in tal senso. Al momento della presentazione dell'autocertificazione iniziale, l'organizzazione deve fornire al Dipartimento un progetto di politica della privacy conforme ai principi. Dopo che il Dipartimento ha accertato che l'autocertificazione iniziale dell'organizzazione è altrimenti completa, il Dipartimento notifica all'organizzazione che dovrebbe finalizzare (ad esempio, se del caso, pubblicare) la propria politica della privacy coerente con il DPF UE-USA. L'organizzazione deve notificare tempestivamente al Dipartimento la finalizzazione della politica della privacy pertinente e in quel momento il Dipartimento inserisce l'organizzazione nell'elenco degli aderenti al DPF.

([13]) Se, al momento dell'abbandono del DPF UE-USA, un'organizzazione sceglie di conservare i dati personali ricevuti ai sensi del DPF e dichiara annualmente al Dipartimento di continuare ad applicare loro i principi, l'organizzazione deve verificare presso il Dipartimento una volta l'anno dopo l'abbandono (ossia, a meno che e finché l'organizzazione fornisca una protezione "adeguata" per tali dati con altri mezzi autorizzati o restituisca o cancelli tutti questi dati e notifichi tale azione al Dipartimento) quello che ha fatto con tali dati personali, cosa farà con i singoli dati personali che continua a conservare e chi fungerà da punto di contatto permanente per le domande relative a principi.

g. Un'organizzazione che cessa di esistere come persona giuridica distinta in ragione di una variazione della forma societaria, quale l'esito di una fusione, un'acquisizione, un fallimento o uno scioglimento, deve notificarlo preventivamente al Dipartimento. La notifica dovrebbe inoltre indicare se il soggetto risultante dal cambiamento della forma societaria: i) continuerà ad aderire al DPF UE-USA attraverso un'autocertificazione esistente; ii) si autocertificherà in qualità di nuovo aderente al DPF UE-USA (ad esempio, se il nuovo soggetto o il soggetto superstite non dispone già di un'autocertificazione attraverso la quale potrebbe aderire al DPF UE-USA); oppure iii) metterà in atto altre garanzie, ad esempio un accordo scritto che garantisca la continuità dell'applicazione dei principi a tutti i dati personali ricevuti dall'organizzazione nell'ambito del DPF UE-USA e conservati. Se non si applica alcuno dei punti i), ii) e iii), i dati personali acquisiti nell'ambito del DPF UE-USA devono essere immediatamente restituiti o cancellati.

h. L'organizzazione che, per qualsivoglia motivo, abbandoni il DPF UE-USA deve eliminare qualsiasi dichiarazione che lasci intendere che continua ad aderirvi o ad avere diritto a godere dei relativi benefici. Se usato, dev'essere eliminato anche il marchio di certificazione del DPF UE-USA. L'FTC, il DOT o un altro ente pubblico competente possono perseguire l'organizzazione per qualsiasi dichiarazione pubblica con cui millanti l'adesione ai principi. L'adesione millantata nei confronti del Dipartimento può essere perseguibile in forza della legge sulle false dichiarazioni (codice degli Stati Uniti, 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 del DPF UE-USA.

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 conformità.

c. Qualora l'organizzazione abbia optato per l'autovalutazione, tale verifica deve dimostrare che la sua politica della privacy per quanto concerne le informazioni personali ricevute dall'UE è accurata, completa, prontamente disponibile, conforme ai principi ed è pienamente attuata (ossia è rispettata). Deve indicare inoltre che le persone siano informate del meccanismo interno di trattamento dei reclami e del meccanismo o dei meccanismi di ricorso 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 il completamento dell'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. Qualora l'organizzazione abbia optato per una verifica esterna della conformità, tale verifica deve dimostrare che la sua politica della privacy per quanto concerne le informazioni personali ricevute dall'UE è accurata, completa, prontamente disponibile, conforme ai principi ed è pienamente attuata (ossia è rispettata). Deve indicare inoltre che le persone sono informate del meccanismo o dei meccanismi attraverso i quali possono proporre reclami. 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 conformità, 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 del DPF UE-USA e, nell'ambito delle indagini o dei reclami per mancato soddisfacimento dei requisiti, metterle a disposizione, a richiesta, dell'organo indipendente di composizione delle controversie 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 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 ([14]);

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

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.

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.

([14]) 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. 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 dal GDPR, 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'ingerenza 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

i. 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

i. 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

i. 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 da parte del DPF UE-USA

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 al DPF UE-USA, 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 limitazioni applicabili al loro trasferimento in forza di detta legge.

ii. I principi 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 del DPF UE-USA 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

i. Il principio supplementare sull'accesso fornisce indicazioni sui motivi che possono giustificare il rifiuto o la limitazione dell'accesso richiesto in tema di risorse umane. Nell'UE il datore di lavoro deve ovviamente rispettare la normativa locale e garantire al dipendente dell'UE 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. Il DPF UE-USA impone all'organizzazione che tratta tali dati negli Stati Uniti di cooperare, 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. 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 il DPF UE-USA si applichi ai dati UE sulle risorse umane trasferiti dall'Unione europea nel contesto di un rapporto di lavoro, l'organizzazione statunitense aderente al DPF UE-USA che li usa deve pertanto impegnarsi a cooperare 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 trasferimento successivo

i. Per le esigenze operative occasionali di natura occupazionale cui l'organizzazione aderente al DPF UE-USA 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 trasferimento successivo, a condizione che l'organizzazione abbia rispettato i principi sull'informativa e sulla scelta.

10. **Contratti obbligatori per il trasferimento successivo**

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 al DPF UE-USA.

ii. Nell'UE 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 al DPF UE-USA. 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 il trasferimento successivo; e

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 dei principi.

iii. Poiché le organizzazioni aderenti forniscono una protezione adeguata, i contratti conclusi con tali organizzazioni a fini esclusivi di trattamento non sono subordinati ad autorizzazione preliminare.

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

i. In base al principio sulla responsabilità in caso di trasferimento successivo, 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 rimane responsabile dell'osservanza dei relativi principi.

c. Trasferimenti fra titolari del trattamento

i. Per i trasferimenti fra titolari del trattamento il destinatario non deve necessariamente essere un'organizzazione aderente o disporre di un meccanismo di ricorso indipendente. L'organizzazione aderente deve concludere con il terzo titolare del trattamento che riceve i dati un contratto che preveda lo stesso livello di protezione fornito dal DPF UE-USA, senza imporgli di aderire a quest'ultimo regime 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 del DPF UE-USA. 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 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 cooperare con le autorità di protezione dei dati ubicate nell'UE 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. Si noti che 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 sull'FTC (codice degli Stati Uniti, titolo 15, articolo 45) il quale proibisce gli atti sleali o ingannevoli, del codice degli Stati Uniti, titolo 49, articolo 41712, che vieta al vettore o al rivenditore che fa servizio di biglietteria, nell'attività di trasporto aereo o di vendita di trasporto aereo, qualsiasi pratica sleale o ingannevole, oppure di altra legge o regolamento che vieti tali atti.

c. Per contribuire al rispetto degli impegni assunti con l'adesione al DPF UE-USA 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 al DPF UE-USA. 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. Meccanismi di ricorso

i. Le persone dovrebbero essere incoraggiate a sporgere reclamo all'organizzazione prima di rivolgersi al meccanismo di ricorso indipendente. Le organizzazioni devono rispondere a una persona 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 indipendente 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 essere rispettati dall'organo indipendente di composizione delle controversie, che devono però essere trasparenti e giustificati (ad esempio, esclusione dei reclami che esulano dall'ambito di 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. Per semplificare il processo di risoluzione dei casi di reclamo, il meccanismo dovrebbe altresì cooperare 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 e ai servizi che presta nell'ambito del DPF UE-USA. Le informazioni devono comprendere: 1) informazioni sugli obblighi che i principi impongono ai meccanismi di ricorso indipendenti oppure un collegamento ipertestuale agli stessi; 2) un collegamento ipertestuale al sito web del Dipartimento dedicato al DPF; 3) l'indicazione che i servizi di composizione delle controversie prestati nell'ambito del DPF UE-USA sono gratuiti per la persona; 4) la spiegazione del modo in cui presentare un reclamo in virtù dei principi; 5) i tempi di trattamento dei reclami presentati in virtù dei principi; e 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 dei principi 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; e 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 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 ([15]) o per le denunce vertenti sull'adeguatezza del DPF UE-USA. In questo contesto il "collegio arbitrale del DPF UE-USA" (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 possono sottoporre la decisione arbitrale al riesame e all'esecuzione in sede giudiziaria previsti dalla legge statunitense ai sensi della legge federale sull'arbitrato.

e. Riparazioni e sanzioni

i. La riparazione ottenuta tramite l'organo indipendente 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 dei 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

([15]) I principi, panoramica, punto 5.

conformità e, in determinate situazioni, l'obbligo di cancellare i dati ([16]). 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 non si attiene alla decisione pronunciata, l'organo indipendente 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

i. 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 vi è stata una violazione dell'articolo 5, 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 una violazione anche quando l'organizzazione millanta l'adesione ai principi o la partecipazione al DPF UE-USA pur non figurando più nell'elenco degli aderenti al DPF o non essendosi mai autocertificata come tale presso il Dipartimento. L'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 dell'ordinanza di un organo giurisdizionale federale. L'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.

g. Inosservanze reiterate

i. L'organizzazione per cui si riscontrano reiterate inosservanze dei principi perde i benefici derivanti dal DPF UE-USA: 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, incluso il Dipartimento, constata che l'organizzazione viola i principi con tale frequenza da togliere qualsiasi credibilità alla sua dichiarazione formale di rispetto. Nei casi in cui tale constatazione sia formulata da un ente od organo diverso dal Dipartimento, l'organizzazione deve informare tempestivamente il Dipartimento di tali fatti. La mancata notifica può essere perseguibile in forza della legge sulle false dichiarazioni (codice degli Stati Uniti, 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. Il Dipartimento depenna un'organizzazione dall'elenco degli aderenti al DPF per inosservanza reiterata, anche in risposta a una notifica dell'inosservanza trasmessa dall'organizzazione stessa, da un organo di autoregolamentazione del settore privato o da un altro organo indipendente di composizione delle controversie, oppure da un ente pubblico, ma non prima di aver concesso all'organizzazione un preavviso di 30 giorni e la possibilità di replica ([17]). L'elenco degli aderenti al DPF 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 al DPF UE-USA è tenuta a presentargli tutte le informazioni relative alla precedente adesione al regime.

([16]) L'organo indipendente 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.

([17]) Il Dipartimento indica nella notifica il termine, necessariamente inferiore a 30 giorni, entro il quale l'organizzazione deve rispondere alla notifica.

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. 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. Ai sensi del GDPR, in mancanza di una decisione di adeguatezza, i dati personali possono essere trasferiti a un paese terzo se sono previste garanzie adeguate in materia di protezione dei dati ai sensi dell'articolo 46 GDPR o, in situazioni specifiche, se è soddisfatta una delle condizioni di cui all'articolo 49 GDPR (ad esempio, se l'interessato ha esplicitamente acconsentito al trasferimento). Le organizzazioni statunitensi che aderiscono al DPF UE-USA forniscono un'adeguata protezione dei dati personali e possono pertanto ricevere trasferimenti di dati dall'UE sulla base dell'articolo 45 GDPR, senza dover predisporre uno strumento di trasferimento a norma dell'articolo 46 GDPR o soddisfare le condizioni di cui all'articolo 49 GDPR. Poiché il regime del DPF UE-USA 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 alle organizzazioni aderenti. 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 dell'UE/dello Stato membro dell'UE o dei principi

i. La normativa dello Stato membro dell'UE si applica alla raccolta dei dati personali e al relativo trattamento prima del trasferimento negli Stati Uniti. I principi 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 in campi specifici della ricerca medica o farmaceutica svolgono spesso un ruolo importante in future ricerche scientifiche. Se i dati personali raccolti per una determinata ricerca sono trasferiti a un'organizzazione statunitense nell'ambito del DPF UE-USA, 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

i. 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

i. 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

i. Nella misura in cui l'osservanza dei principi interferisca con l'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 trasferimento successivo e accesso, ad 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

i. 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, ossia dati personali dell'UE ai sensi del diritto dell'Unione, rientrerebbe nell'ambito di applicazione dei principi.

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

a. L'organizzazione deve applicare ai dati personali ricavati da fonti di pubblico dominio i principi 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 trasferimento successivo 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 trasferimento successivo alle informazioni di pubblico dominio, a meno che il trasferente europeo indichi che le informazioni sono soggette a limitazioni 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 del DPF UE-USA.

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 od 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 può pubblicare di propria iniziativa relazioni periodiche 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 ad altri dati, le informazioni comunicate dalle organizzazioni aderenti in detti relazioni possono essere usate per informare il riesame congiunto periodico del funzionamento del DPF UE-USA 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 al DPF UE-USA 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 DPF UE-USA. 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 meccanismi previsti dal DPF UE-USA.

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 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 del DPF UE-USA.

B. **Forme di riparazione disponibili**

In questo contesto il "collegio arbitrale del DPF UE-USA" (il collegio arbitrale 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 del DPF UE-USA in tema di riparazioni. Nel valutare le riparazioni possibili, il collegio arbitrale del DPF UE-USA è tenuto a tenere conto delle altre riparazioni già disposte da altri meccanismi nell'ambito di tale regime. 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 lettera d), punto i), del principio supplementare su composizione delle controversie e controllo dell'applicazione; 2) rivolgersi al meccanismo di ricorso indipendente previsto dai principi, procedura che è gratuita per la persona; 3) per il tramite della propria autorità di protezione dei dati, sottoporre la questione al Dipartimento dandogli la possibilità di adoperarsi per risolverla nei tempi indicati nella lettera dell'Amministrazione del commercio internazionale del Dipartimento, 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 1) è competente ai sensi del principio supplementare sul ruolo delle autorità di protezione dei dati o del principio supplementare sui dati sulle risorse umane, 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]) I principi, panoramica, punto 5.

E. **Riesame ed esecuzione**

Ai sensi della legge federale sull'arbitrato, la persona e l'organizzazione aderente possono sottoporre la decisione arbitrale al riesame e all'esecuzione in sede giudiziaria previsti dalla legge statunitense ([2]). 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 al regime.

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 per il collegio arbitrale del DPF UE-USA all'elenco di arbitri descritto di seguito.

In linea con la normativa vigente, il Dipartimento e la Commissione stilano un elenco di almeno dieci 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 da parte del Dipartimento per ulteriori termini di 3 anni, previa notifica preventiva alla Commissione;

2) non riceve istruzioni da nessuna delle parti, da nessuna organizzazione aderente né dagli Stati Uniti, 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; e

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

([2]) 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, 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. (ibidem). 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 (ibidem, articolo 207). Sempre a norma del capo 2, i giudici distrettuali degli Stati Uniti sono competenti dell'azione o del procedimento avviato in virtù della convenzione di New York, a prescindere dall'importo oggetto della controversia (ibidem, 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 (ibidem, 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 od 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 (ibidem, 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 (ibidem, articolo 9).

G. **Procedure arbitrali**

Il Dipartimento e la Commissione hanno concordato, conformemente al diritto applicabile, l'adozione di norme arbitrali che disciplinano i procedimenti dinanzi al collegio arbitrale del DPF UE-USA ([3]). Qualora le norme che disciplinano il procedimento dovessero essere modificate, il Dipartimento e la Commissione concordano di modificarle o di adottare una serie diversa di procedure arbitrali statunitensi esistenti e consolidate, a seconda dei casi, fatte salve le seguenti considerazioni:

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;

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 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; 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 arbitrale del DPF UE-USA 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.

([3]) L'*International Centre for Dispute Resolution* (ICDR, Centro internazionale per la composizione delle controversie), la divisione internazionale dell'*American Arbitration Association* (AAA, Associazione americana per l'arbitrato) (collettivamente "ICDR-AAA"), è stato selezionato dal Dipartimento per gestire gli arbitrati e il fondo arbitrale di cui all'allegato I dei principi. Il 15 settembre 2017 il Dipartimento e la Commissione hanno approvato l'adozione di una serie di norme arbitrali destinate a disciplinare i procedimenti arbitrali vincolanti di cui all'allegato I dei principi, nonché di un codice di condotta per gli arbitri che sia conforme alle norme etiche generalmente accettate per gli arbitri commerciali e all'allegato I dei principi. Il Dipartimento e la Commissione hanno convenuto di adeguare le norme arbitrali e il codice di condotta per tenere conto degli aggiornamenti nell'ambito del DPF UE-USA e collaboreranno con l'ICDR-AAA per effettuare tali aggiornamenti.

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 agevola il mantenimento di un fondo, destinato a coprire le spese arbitrali, compresi gli onorari degli arbitri, cui ciascuna organizzazione aderente è tenuta a contribuire in base alla sua dimensione fino a concorrenza di importi massimi ("massimali"). Il fondo sarà gestito da un terzo, che riferisce periodicamente al Dipartimento sul suo funzionamento. Il Dipartimento collabora periodicamente con tale terzo per esaminare il funzionamento del fondo, compresa la necessità di adeguare le quote o i massimali per le spese arbitrali, e considera 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. Il Dipartimento notifica alla Commissione l'esito di tali esami con detto terzo e le trasmette una notifica preventiva di eventuali adeguamenti dell'importo dei contributi. Gli onorari degli avvocati non sono contemplati dalla presente disposizione né da nessun fondo costituito in virtù della presente disposizione.

ALLEGATO II

DIPARTIMENTO DEL COMMERCIO DEGLI STATI UNITI D'AMERICA
Segretaria al commercio
Washington, D.C. 20230

6 luglio 2023

Didier Reynders
Commissario per la Giustizia
Commissione europea
Rue de la Loi/ Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissario Reynders,

a nome degli Stati Uniti, sono lieta di trasmettere con la presente un pacchetto di materiali relativi al quadro UE-USA per la protezione dei dati personali che, in combinazione con il decreto presidenziale 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" e il *Code of Federal Regulations* (CFR, codice dei regolamenti federali), titolo 28, parte 201, che modifica i regolamenti del ministero della Giustizia al fine di istituire il "Data Protection Review Court" (DPRC, tribunale del riesame in materia di protezione dei dati), rispecchia importanti e dettagliati negoziati volti a rafforzare la tutela della vita privata e delle libertà civili. Tali negoziati hanno portato alla definizione di nuove garanzie per assicurare che le attività statunitensi di intelligence dei segnali siano necessarie e proporzionate al perseguimento di determinati obiettivi di sicurezza nazionale così come di un nuovo meccanismo che consenta alle persone dell'Unione europea ("UE") di presentare ricorso qualora ritengano di essere oggetto illecitamente di attività di intelligence dei segnali, che congiuntamente garantiranno la protezione dei dati personali dell'UE. Il quadro UE-USA per la protezione dei dati personali sosterrà un'economia digitale inclusiva e competitiva. Dovremmo entrambi essere orgogliosi dei miglioramenti che si rispecchiano in tale quadro, che rafforzerà la tutela della vita privata in tutto il mondo. Assieme al decreto presidenziale, ai regolamenti e ad altri materiali accessibili da fonti pubbliche, la documentazione acclusa getta una solida base per un nuovo accertamento di adeguatezza da parte della Commissione europea ([1]).

Si allega la documentazione seguente:

— i principi del quadro UE-USA per la protezione dei dati personali, compresi i principi supplementari (collettivamente "i principi") e l'allegato I dei principi (ossia, un allegato che stabilisce le condizioni in base alle quali le organizzazioni aderenti al quadro per la protezione dei dati personali sono tenute a sottoporre ad arbitrato determinate rivendicazioni residue in relazione ai dati personali contemplati dai principi);

— una lettera dell'Amministrazione del commercio internazionale del Dipartimento che gestisce il programma relativo al quadro per la protezione dei dati personali, che descrive gli impegni assunti dal nostro Dipartimento per garantire l'efficace funzionamento del quadro UE-USA per la protezione dei dati personali;

— una lettera in cui la Commissione federale del Commercio descrive le proprie modalità di esecuzione dei principi;

— una lettera in cui il Dipartimento dei Trasporti descrive le proprie modalità di esecuzione dei principi;

— una lettera dell'Ufficio del direttore dell'intelligence nazionale sulle garanzie e limitazioni applicabili alle autorità di sicurezza nazionale degli USA; e

— una 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.

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

Il pacchetto completo relativo al quadro UE-USA per la protezione dei dati personali sarà pubblicato sul sito web del Dipartimento dedicato al quadro per la protezione dei dati personali e i principi e l'allegato I dei principi entreranno in vigore alla data di entrata in vigore della decisione di adeguatezza della Commissione europea.

Mi preme sottolineare la serietà con cui gli Stati Uniti tengono conto di questi impegni. Il Dipartimento del Commercio attende con interesse di collaborare con la Commissione europea quando il quadro UE-USA per la protezione dei dati personali sarà attuato e quando, insieme, passeremo alla fase successiva di questo processo.

La prego di accogliere, signor Commissario, i sensi della mia più alta stima.

Gina M. RAIMONDO

ALLEGATO III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 dicembre 2022

Didier Reynders
Commissario per la Giustizia
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissario Reynders,

a nome dell'Amministrazione del commercio internazionale (*International Trade Administration*, ITA), sono lieta di descrivere gli impegni assunti dal Dipartimento del Commercio ("il Dipartimento") al fine di garantire la protezione dei dati personali attraverso l'amministrazione e la supervisione da parte dello stesso del programma relativo al quadro per la protezione dei dati personali. La messa a punto del quadro UE-USA per la protezione dei dati personali ("DPF UE-USA") costituisce un risultato importante per la tutela della vita privata e per le imprese su entrambe le sponde dell'Atlantico, in quanto offrirà ai cittadini dell'UE fiducia nella protezione dei loro dati e nella disponibilità di mezzi di ricorso per affrontare le preoccupazioni relative ai loro dati, e consentirà a migliaia di imprese di continuare a investire e a impegnarsi altrimenti in attività di commercio attraverso l'Atlantico a vantaggio delle nostre rispettive economie e dei nostri rispettivi cittadini. Il DPF UE-USA rispecchia anni di intenso lavoro e profonda collaborazione con Lei e i Suoi colleghi della Commissione europea ("la Commissione"), con la quale attendiamo con interesse di continuare la collaborazione per assicurare che questo sforzo collaborativo funzioni in maniera efficace.

Il DPF UE-USA offrirà benefici rilevanti alle persone e alle imprese. In primo luogo, alle persone dell'UE offre un insieme importante di tutele circa la privacy dei dati trasferiti negli Stati Uniti. 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 del quadro UE-USA per la protezione dei dati personali", compresi i principi supplementari (collettivamente "i principi"), e l'allegato I dei principi (ossia, un allegato che stabilisce le condizioni in base alle quali le organizzazioni aderenti al DPF UE-USA sono tenute a sottoporre ad arbitrato determinate rivendicazioni residue in relazione ai dati personali contemplati dai principi), in modo che l'impegno assunto sia azionabile in virtù della legge statunitense ([1]); 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 di indagine e di controllo di un ente statunitense competente per legge elencato nei principi (ad esempio, la Commissione federale del Commercio (FTC), il Dipartimento dei Trasporti (DOT)) o di un altro ente statunitense competente per legge elencato in un futuro allegato dei principi. Sebbene la decisione di un'organizzazione di autocertificarsi sia volontaria, se un'organizzazione si impegna pubblicamente a rispettare il DPF UE-USA, tale impegno può essere fatto valere, in virtù della legge statunitense, dall'FTC, dal DOT o da un altro ente statunitense competente per legge a seconda di quale soggetto

([1]) Le organizzazioni che autocertificano il loro impegno a rispettare i principi del DPF UE-USA e desiderano beneficiare dei vantaggi derivanti dall'adesione a tale regime devono rispettare i "principi del quadro UE-USA per la protezione dei dati personali". Tale impegno a rispettare i "principi del quadro UE-USA per la protezione dei dati personali" si rispecchia nelle politiche della privacy di tali organizzazioni aderenti quanto prima, e in ogni caso entro non oltre tre mesi dalla data di entrata in vigore di tali principi. (*Cfr.* lettera e) del principio supplementare sull'autocertificazione).

abbia competenza giurisdizionale sull'organizzazione aderente. In secondo luogo, il DPF UE-USA permetterà alle imprese negli Stati Uniti, e alle filiali di imprese europee situate negli Stati Uniti, di ricevere dati personali dall'Unione europea, facilitando i flussi di dati a sostegno del commercio transatlantico. I flussi di dati tra gli Stati Uniti e l'Unione europea sono i più ampi al mondo e sono alla base delle relazioni economiche tra Stati Uniti e UE, che rappresentano 7,1 miliardi di USD e sostengono 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. 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.

Il Dipartimento si impegna a collaborare strettamente e in modo produttivo con le controparti dell'UE al fine di gestire e supervisionare in maniera efficace il programma relativo al quadro per la protezione dei dati personali. Tale impegno si riflette nello sviluppo e nel continuo perfezionamento da parte del Dipartimento di una serie di risorse destinate a fornire assistenza alle organizzazioni nel processo di autocertificazione, nella creazione di un sito web per fornire informazioni mirate ai portatori di interessi, nella collaborazione con la Commissione e le autorità europee di protezione dei dati ("autorità di protezione dei dati") al fine di elaborare orientamenti che chiariscano elementi importanti del DPF UE-USA, nella sensibilizzazione volta a facilitare una maggiore comprensione degli obblighi delle organizzazioni in materia di protezione dei dati, così come nella vigilanza e nel monitoraggio del rispetto dei requisiti del programma da parte delle organizzazioni.

La nostra cooperazione costante con le preziose controparti dell'UE consentirà al Dipartimento di garantire il funzionamento efficace del DPF UE-USA. Il governo degli Stati Uniti vanta una tradizione di lunga data in termini di collaborazione con la Commissione al fine di promuovere principi condivisi in materia di protezione dei dati, colmando le differenze nei nostri rispettivi approcci giuridici e promuovendo nel contempo il commercio e la crescita economica nell'Unione europea e negli Stati Uniti. Riteniamo che il DPF UE-USA, che è un esempio di tale cooperazione, consentirà alla Commissione di adottare una nuova decisione di adeguatezza che permetterà alle organizzazioni di utilizzare tale regime per trasferire dati personali dall'Unione europea agli Stati Uniti nel rispetto del diritto dell'Unione.

Gestione e supervisione del programma "Quadro per la protezione dei dati personali" (DPF) da parte del Dipartimento del Commercio

Il Dipartimento è fermamente impegnato a favore di una gestione e di una supervisione efficaci del programma relativo al quadro per la protezione dei dati personali e intende intraprendere sforzi adeguati e destinare risorse adeguate per garantire il conseguimento di tale risultato. Il Dipartimento tiene e mette a disposizione del pubblico un elenco ufficiale di organizzazioni statunitensi che si sono autocertificate presso il Dipartimento e hanno dichiarato il loro impegno ad aderire ai principi ("elenco degli aderenti al DPF"), che aggiornerà sulla base delle ricertificazioni annuali presentate dalle organizzazioni aderenti, depennando altresì le organizzazioni che abbandonano volontariamente il regime, non completano la ricertificazione annuale secondo le procedure del Dipartimento o risultano costantemente inadempienti. Il Dipartimento tiene e mette a disposizione del pubblico anche un elenco ufficiale delle organizzazioni statunitensi depennate dall'elenco e indicherà per ciascuna il motivo dell'esclusione. L'elenco delle organizzazioni aderenti e quello di quelle depennate resta a disposizione del pubblico sul sito web del Dipartimento dedicato al quadro per la protezione dei dati personali. Il sito web dedicato al quadro per la protezione dei dati personali contiene una spiegazione ben visibile indicante che qualsiasi organizzazione depennata dall'elenco deve cessare di dichiarare di aderire al DPF UE-USA o di rispettare tale regime e di poter ricevere informazioni personali ai sensi del DPF UE-USA. Una tale organizzazione deve tuttavia continuare ad applicare i principi alle informazioni personali ricevute durante l'adesione al DPF UE-USA fintantoché conserva tali informazioni. In linea con il suo impegno generale e costante a favore di una gestione e supervisione efficaci del programma relativo al quadro per la protezione dei dati personali, il Dipartimento si impegna in particolare ad attuare quanto segue.

Verifica del soddisfacimento dei requisiti per l'autocertificazione

— Prima della finalizzazione dell'autocertificazione iniziale o della ricertificazione annuale di un'organizzazione (collettivamente "autocertificazione") e prima di inserire o mantenere un'organizzazione nell'elenco degli aderenti al quadro per la protezione dei dati personali, il Dipartimento verifica che l'organizzazione soddisfi, come minimo, i requisiti pertinenti stabiliti nel principio supplementare sull'autocertificazione in relazione alle informazioni che un'organizzazione deve fornire nella sua autocertificazione presentata al Dipartimento e che detta organizzazione abbia fornito, in tempo utile, una politica della privacy che informi le persone in merito a tutti i 13 elementi elencati nel principio sull'informativa. Il Dipartimento verifica che l'organizzazione:

— abbia individuato l'organizzazione che presenta la propria autocertificazione, nonché i soggetti e le filiali statunitensi dell'organizzazione che si autocertifica che aderiscono anch'essi ai principi che l'organizzazione intende includere nella propria autocertificazione;

— abbia fornito le informazioni richieste di contatto dell'organizzazione (ad esempio informazioni di contatto per persone e/o uffici specifici all'interno dell'organizzazione che si autocertifica competenti per la gestione di reclami, richieste di accesso e qualsiasi altra questione sollevata nel contesto del DPF UE-USA);

— abbia descritto le finalità per le quali l'organizzazione intende raccogliere e utilizzare le informazioni personali ricevute dall'Unione europea;

— abbia indicato quali informazioni personali riceverebbe dall'Unione europea ai sensi del DPF UE-USA che rientrerebbero pertanto nella sua autocertificazione;

— qualora disponga un sito web pubblico, abbia fornito l'indirizzo web dove la pertinente politica della privacy è prontamente disponibile su tale sito oppure, qualora l'organizzazione non disponga di un sito web pubblico, abbia fornito al Dipartimento una copia della pertinente politica della privacy e indicazione del luogo presso il quale è disponibile per la consultazione da parte delle persone interessate (ossia, i dipendenti interessati se la pertinente politica della privacy riguarda le risorse umane o il pubblico se la pertinente politica della privacy non riguarda le risorse umane);

— abbia incluso nella sua politica della privacy, al momento opportuno (ossia, inizialmente, soltanto in un progetto di politica della privacy fornito unitamente alla documentazione presentata inizialmente se si tratta di un'autocertificazione iniziale; altrimenti, in una politica sulla privacy definitiva e, se del caso, pubblicata), una dichiarazione attestante l'adesione ai principi e un collegamento ipertestuale o l'indirizzo web del sito web del Dipartimento dedicato al quadro per la protezione dei dati personali (ad esempio, la homepage o la pagina web dell'elenco degli aderenti al DPF);

— abbia incluso nella sua politica della privacy pertinente, al momento opportuno, tutti gli altri 12 elementi elencati nel principio sull'informativa (ad esempio la possibilità, a determinate condizioni, per la persona interessata dell'UE di invocare un arbitrato vincolante; l'obbligo di divulgare informazioni personali in risposta a legittime richieste da parte di autorità pubbliche, tra l'altro per soddisfare obblighi in materia di sicurezza nazionale o di applicazione della legge; e la responsabilità che le incombe in caso di trasferimento successivo dei dati a terzi);

— 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);

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

— abbia individuato se il metodo pertinente (ossia le procedure di controllo che deve attuare) per verificare la propria conformità ai principi è l'"autovalutazione" (ossia una verifica interna) o una "verifica esterna della conformità" (ossia una verifica da parte di terzi) e, qualora abbia optato per la verifica esterna della conformità come metodo pertinente, abbia individuato altresì il terzo che ha completato tale verifica;

— abbia individuato l'adeguato meccanismo di ricorso indipendente disponibile per trattare i reclami presentati ai sensi dei principi e fornire un ricorso adeguato e gratuito alla persona interessata.

— Se ha optato per un meccanismo di ricorso indipendente messo a disposizione da un organo di composizione alternativa delle controversie del settore privato, l'organizzazione deve aver incluso nella propria politica della privacy un collegamento ipertestuale o l'indirizzo del sito web pertinente o del modulo di presentazione dei reclami nel contesto del meccanismo disponibile per indagare in merito a reclami non risolti presentati ai sensi dei principi;

— se l'organizzazione è tenuta (ad esempio per quanto riguarda i dati relativi alle risorse umane trasferiti dall'Unione europea nel contesto di un rapporto di lavoro) oppure ha scelto di cooperare con le competenti autorità di protezione dei dati nell'indagine e nella risoluzione dei reclami presentati ai sensi dei principi, detta organizzazione deve aver dichiarato il proprio impegno a favore di tale cooperazione con le autorità di protezione dei dati e il rispetto del relativo parere di intraprendere azioni specifiche per conformarsi ai principi;

— il Dipartimento verifica inoltre che l'autocertificazione presentata dall'organizzazione sia coerente con la sua o le sue politiche della privacy. Se un'organizzazione che si autocertifica intende includere qualsiasi suo soggetto o qualsiasi sua filiale statunitense che dispone di politiche della privacy distinte, il Dipartimento verifica anche le pertinenti politiche della privacy di tali soggetti inclusi o filiali incluse al fine di garantire che tali politiche comprendano tutti gli elementi richiesti stabiliti nel principio sull'informativa;

— il Dipartimento collaborerà con gli enti competenti per legge (ad esempio l'FTC e il DOT) al fine di verificare che le organizzazioni siano soggette alla competenza giurisdizionale dell'ente competente pertinente individuato nelle loro autocertificazioni, qualora il Dipartimento abbia motivo di dubitare che le organizzazioni siano soggette a tale competenza giurisdizionale;

— il Dipartimento collaborerà con gli organi di composizione alternativa delle controversie del settore privato al fine di verificare che le organizzazioni siano attivamente registrate per il meccanismo di ricorso indipendente individuato nelle loro autocertificazioni; e collaborerà con tali organi al fine di verificare che le organizzazioni siano attivamente registrate per la verifica esterna della conformità indicata nelle loro autocertificazioni, qualora tali organi possano offrire entrambi i tipi di servizi;

— il Dipartimento collaborerà con il terzo da esso designato per fungere da depositario dei fondi riscossi per i contributi spese del comitato delle autorità di protezione dei dati (ossia il contributo spese annuo destinato a coprire i costi di esercizio di tale comitato) al fine di verificare che le organizzazioni abbiano corrisposto tale contributo per l'anno in questione, qualora le organizzazioni abbiano individuato le autorità di protezione dei dati come il meccanismo di ricorso indipendente pertinente;

— il Dipartimento collaborerà con il terzo da esso designato per gestire gli arbitrati e il fondo arbitrale di cui all'allegato I dei principi al fine di verificare che le organizzazioni abbiano contribuito a tale fondo arbitrale;

— qualora il Dipartimento rilevi eventuali questioni da risolvere nel corso dell'esame delle autocertificazioni delle organizzazioni, informa queste ultime della necessità che provvedano ad affrontare tutte le questioni rilevate entro i termini stabiliti dal Dipartimento stesso ([2]). Il Dipartimento informa tali organizzazioni altresì del fatto che la mancata risposta entro i termini da esso indicati o il mancato completamento dell'autocertificazione secondo le procedure del Dipartimento imporrà a quest'ultimo di considerare abbandonate le autocertificazioni in questione, così come del fatto che qualsiasi falsa dichiarazione in merito all'adesione al DPF UE-USA o alla conformità di un'organizzazione rispetto a tale regime può essere oggetto di un'azione coercitiva da parte dell'FTC, del DOT o di altro ente pubblico competente. Il Dipartimento informa le organizzazioni attraverso i mezzi di contatto che le organizzazioni hanno fornito al Dipartimento.

Facilitazione della cooperazione con gli organi di composizione alternativa delle controversie che forniscono servizi connessi ai principi

— Il Dipartimento collabora con gli organi di composizione alternativa delle controversie del settore privato che forniscono meccanismi di ricorso indipendenti, disponibili per indagare in merito a reclami irrisolti presentati ai sensi dei principi, al fine di verificare che soddisfino quanto meno i requisiti stabiliti nel principio supplementare su composizione delle controversie e controllo dell'applicazione. Il Dipartimento verifica che tali organi:

  — includano nei loro siti web pubblici informazioni sui principi e sui servizi che forniscono nell'ambito del DPF UE-USA, che devono comprendere: 1) informazioni sugli obblighi che i principi impongono ai meccanismi di ricorso indipendenti oppure un collegamento ipertestuale agli stessi; 2) un collegamento ipertestuale al sito web del Dipartimento dedicato al quadro per la protezione dei dati personali; 3) l'indicazione che i servizi di composizione delle controversie prestati nell'ambito del DPF UE-USA sono gratuiti per la persona; 4) la spiegazione del modo in cui presentare un reclamo in virtù dei principi; 5) i tempi di trattamento dei reclami presentati in virtù dei principi; e 6) la descrizione della gamma delle possibili riparazioni. Il Dipartimento informa tempestivamente gli organi in merito alle modifiche sostanziali alla gestione e alla supervisione svolte dallo stesso in relazione al programma del quadro per la protezione dei dati personali, qualora tali modifiche siano imminenti o siano già state apportate e tali modifiche siano pertinenti al ruolo svolto dagli organi nell'ambito del DPF UE-USA;

([2]) Ad esempio, per quanto concerne la ricertificazione, ci si aspetterebbe che le organizzazioni affrontino tutti questi problemi entro 45 giorni; fatta salva la designazione da parte del Dipartimento di un termine diverso e adeguato.

— pubblichino una relazione annuale che fornisca statistiche aggregate in merito ai loro servizi di risoluzione delle controversie, la quale deve contemplare: 1) il numero complessivo dei reclami in virtù dei principi 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; e 4) l'esito dei reclami ricevuti, in particolare il numero e il tipo delle riparazioni o delle sanzioni decretate. Il Dipartimento fornisce agli organi orientamenti specifici e complementari in merito a quali informazioni dovrebbero fornire nelle relazioni annuali che elaborano in merito a tali requisiti (ad esempio elencazione dei criteri specifici che un reclamo deve soddisfare per essere considerato un reclamo relativo ai principi ai fini della relazione annuale), individuando altresì altri tipi di informazioni che gli organi in questione dovrebbero fornire (ad esempio se l'organo fornisce anche un servizio di verifica relativo ai principi, l'organo in questione deve fornire una descrizione del modo in cui evita conflitti di interesse effettivi o potenziali in situazioni nelle quali fornisce a un'organizzazione tanto servizi di verifica quanto servizi di risoluzione delle controversie). Gli orientamenti aggiuntivi forniti dal Dipartimento specificano inoltre la data entro la quale le relazioni annuali degli organi dovrebbero essere pubblicate per il periodo di riferimento pertinente.

Seguito in relazione alle organizzazioni che desiderano essere o che sono state depennate dall'elenco degli aderenti al DPF

— Se un'organizzazione desidera abbandonare il DPF UE-USA, il Dipartimento le chiede di eliminare da qualsiasi pertinente politica della privacy qualsiasi riferimento al DPF UE-USA che implichi che essa continui ad aderire a tale regime e che possa ricevere dati personali a norma di tale regime (*cfr.* descrizione dell'impegno del Dipartimento a reperire i casi di millantata adesione). Il Dipartimento imporrà inoltre alle organizzazioni in questione di compilare e presentargli un apposito questionario destinato a verificare:

  — la volontà dell'organizzazione di abbandonare il regime;

  — per quale delle possibilità seguenti opta in relazione ai dati personali che ha ricevuto nel contesto del DPF UE-USA durante la sua adesione a tale regime: a) conservazione di tali dati, prosecuzione dell'applicazione dei principi a tali dati e conferma al Dipartimento, su base annuale, del proprio impegno ad applicare i principi a tali dati; b) conservazione di tali dati e fornitura di una protezione "adeguata" di tali dati con altri mezzi autorizzati; o c) restituzione o cancellazione di tutti i dati pertinenti entro una data specificata; e

  — chi, all'interno dell'organizzazione, fungerà da punto di contatto permanente per le domande relative ai principi;

— nel caso in cui un'organizzazione abbia optato per l'opzione a) di cui sopra, il Dipartimento le chiede inoltre di completare e presentargli ogni anno dopo il suo abbandono del regime (ossia entro il primo anniversario dall'abbandono, nonché entro ogni anniversario successivo, a meno che e fintantoché l'organizzazione fornisca una protezione "adeguata" di tali dati con altri mezzi autorizzati oppure restituisca o cancelli tutti i dati e ne informi il Dipartimento), un questionario adeguato per verificare ciò che l'organizzazione ha fatto con tali dati personali, cosa farà con i singoli dati che continua a conservare e chi, all'interno dell'organizzazione, fungerà da punto di contatto permanente per le domande relative ai principi;

— se un'organizzazione ha lasciato scadere la propria autocertificazione (ossia se non ha completato la ricertificazione annuale della sua adesione ai principi né è stata depennata dall'elenco degli aderenti al DPF per altri motivi, quali un suo abbandono del regime), il Dipartimento le ingiunge di compilare e presentargli un questionario adeguato per verificare se desidera abbandonare il regime oppure ricertificarsi:

  — e, qualora intenda abbandonare il regime, per verificare ulteriormente cosa farà con i dati personali che ha ricevuto ai sensi del DPF UE-USA durante l'adesione dell'organizzazione al regime (*cfr.* descrizione precedente in merito a ciò che un'organizzazione deve verificare se desidera abbandonare il regime);

  — e qualora intenda ricertificarsi, per verificare ulteriormente che, durante la scadenza del suo status di certificazione, abbia applicato i principi ai dati personali ricevuti nell'ambito del DPF UE-USA e per chiarire quali misure intende adottare per affrontare le questioni in sospeso che hanno ritardato la ricertificazione;

— se un'organizzazione è depennata dall'elenco degli aderenti al DPF per uno dei seguenti motivi: a) abbandono del DPF UE-USA; b) mancato completamento della ricertificazione annuale della sua adesione ai principi (ossia, l'organizzazione ha avviato il processo annuale di ricertificazione ma non lo ha completato in modo tempestivo o non ha neppure avviato detto processo); o c) "inosservanza reiterata", il Dipartimento invia una notifica al contatto o ai contatti individuati nell'autocertificazione dell'organizzazione specificando il motivo del depennamento e spiegando che deve cessare di formulare dichiarazioni esplicite o implicite di adesione al DPF UE-USA o di rispetto di tale regime e di ricevere dati personali a norma di tale regime. La notifica, che può comprendere altresì altri contenuti adattati al motivo del depennamento, indica che le organizzazioni che millantano l'adesione al DPF UE-USA o la loro conformità rispetto a tale regime, compreso il caso in cui dichiarino di aderire al DPF UE-USA dopo essere state depennate dall'elenco degli aderenti al DPF, possono essere oggetto di azioni coercitive da parte dell'FTC, del DOT o di un altro ente pubblico competente.

Reperimento dei casi di millantata adesione e loro soluzione

— Su base continuativa, quando un'organizzazione: a) abbandona il DPF UE-USA; b) non completa la ricertificazione annuale della sua adesione ai principi (ossia, l'organizzazione ha avviato il processo annuale di ricertificazione ma non lo ha completato in modo tempestivo o non ha neppure avviato detto processo); c) è depennata dall'elenco degli aderenti al DPF UE-USA, in particolare per "inosservanza reiterata"; o d) non ha completato un'autocertificazione iniziale della sua adesione ai principi (ossia ha avviato il processo di autocertificazione iniziale ma non lo ha completato in modo tempestivo), il Dipartimento si impegna, *ex officio*, a verificare che la pertinente politica della privacy pubblicata dall'organizzazione non contenga riferimenti al DPF UE-USA che implichino che l'organizzazione aderisce al regime e che possa ricevere dati personali a norma di tale regime. Se accerta la presenza di tali riferimenti, il Dipartimento informa l'organizzazione del fatto che, se continuerà a millantare l'adesione al DPF UE-USA, la questione sarà sottoposta all'ente competente per un'eventuale azione coercitiva. Il Dipartimento informa l'organizzazione attraverso i mezzi di contatto forniti da quest'ultima al Dipartimento o, se necessario, ricorrendo ad altri mezzi. Se l'organizzazione non elimina i riferimenti né si autocertifica conforme al DPF UE-USA in linea con le procedure previste dal Dipartimento, quest'ultimo investe d'ufficio della questione l'FTC, il DOT o un altro ente competente oppure intraprende le azioni adeguate per garantire il rispetto dell'uso opportuno del marchio di certificazione legato al DPF UE-USA;

— il Dipartimento intraprende altri sforzi per individuare i casi di millantata adesione al DPF UE-USA e di uso improprio del marchio di certificazione di tale regime, anche da parte di organizzazioni che, a differenza delle organizzazioni di cui sopra, non hanno mai avviato il processo di autocertificazione (ad esempio effettuando ricerche adeguate su internet per individuare riferimenti al DPF UE-USA nelle politiche della privacy delle organizzazioni). Se, attraverso tali sforzi rileva casi di millantata adesione al DPF UE-USA o di uso improprio del marchio di certificazione di tale regime, il Dipartimento informa l'organizzazione del fatto che, se continuerà a millantare l'adesione al DPF UE-USA, la questione sarà sottoposta all'ente competente per un'eventuale azione coercitiva. Il Dipartimento informa l'organizzazione attraverso i mezzi di contatto forniti da quest'ultima al Dipartimento, se presenti, o, se necessario, ricorrendo ad altri mezzi. Se l'organizzazione non elimina i riferimenti né si autocertifica conforme al DPF UE-USA in linea con le procedure previste dal Dipartimento, quest'ultimo investe d'ufficio della questione l'FTC, il DOT o un altro ente competente oppure intraprende le azioni adeguate per garantire il rispetto dell'uso opportuno del marchio di certificazione legato al DPF UE-USA;

— il Dipartimento esamina tempestivamente e tratta reclami specifici e non futili ricevuti in merito a casi di millantata adesione al DPF UE-USA (ad esempio reclami ricevuti da autorità di protezione dei dati, meccanismi di ricorso indipendenti messi a disposizione da organi di composizione alternativa delle controversie del settore privato, interessati, imprese dell'UE e degli Stati Uniti e altri tipi di terzi); e

— il dipartimento potrà adottare altre misure correttive adeguate. L'adesione millantata nei confronti del Dipartimento può essere perseguibile in forza della legge sulle false dichiarazioni (codice degli Stati Uniti, titolo 18, articolo 1001).

Svolgimento di controlli periodici d'ufficio della conformità e valutazioni del programma del DPF

— Su base continuativa, il Dipartimento si adopera per monitorare l'effettiva conformità da parte delle organizzazioni aderenti al DPF UE-USA al fine di individuare questioni che possono giustificare un'azione di seguito. In particolare, il Dipartimento effettua, d'ufficio, controlli periodici a campione di organizzazioni aderenti al DPF UE-USA selezionate casualmente, nonché controlli a campione ad hoc di specifiche organizzazioni aderenti al DPF UE-USA qualora siano individuate potenziali carenze di conformità (ad esempio potenziali carenze di conformità portate all'attenzione del Dipartimento da terzi) al fine di verificare: a) l'effettiva disponibilità del punto o dei punti di contatto competenti per la gestione dei reclami, delle richieste di accesso e di altre questioni sollevate nell'ambito del DPF UE-USA; b) se del caso, che la politica pubblica della privacy dell'organizzazione sia prontamente accessibile per la consultazione da parte del pubblico tanto sul sito web pubblico dell'organizzazione quanto attraverso un collegamento ipertestuale nell'elenco degli aderenti al DPF; c) che la politica della privacy dell'organizzazione continui a rispettare i requisiti di autocertificazione descritti nei principi; e d) che il meccanismo di ricorso indipendente individuato dall'organizzazione sia disponibile per trattare i reclami presentati nell'ambito del DPF UE-USA. Il Dipartimento monitora inoltre attivamente le segnalazioni che forniscono prove credibili di non conformità da parte di organizzazioni aderenti al DPF UE-USA;

— nel contesto del riesame della conformità, il Dipartimento impone a un'organizzazione del DPF UE-USA di compilare e presentargli un questionario dettagliato 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 sul DPF UE-USA; oppure c) prove credibili indicano che l'organizzazione non rispetta gli impegni assunti con tale regime. Se ha inviato un tale questionario dettagliato a un'organizzazione e quest'ultima non risponde in modo soddisfacente al questionario, il Dipartimento informa l'organizzazione che, se del caso, rinvierà la questione all'organo competente affinché siano adottate eventuali azioni coercitive qualora il Dipartimento non riceva una risposta tempestiva e soddisfacente da parte dell'organizzazione. Il Dipartimento informa l'organizzazione attraverso i mezzi di contatto forniti da quest'ultima al Dipartimento o, se necessario, ricorrendo ad altri mezzi. Se l'organizzazione non fornisce una risposta tempestiva e soddisfacente, il dipartimento rinvia d'ufficio la questione all'FTC, al DOT o ad un altro ente competente, o adotta altre misure appropriate per garantire la conformità. Ove opportuno, il Dipartimento consulta le competenti autorità di protezione dei dati circa tali controlli della conformità; e

— il Dipartimento valuta periodicamente la gestione e la supervisione del programma del quadro per la protezione dei dati personali al fine di garantire che i suoi sforzi di monitoraggio, compresi quelli intrapresi mediante l'uso di strumenti di ricerca (ad esempio, per verificare la presenza di collegamenti interrotti con le politiche della privacy di organizzazioni aderenti al DPF UE-USA), siano adeguati per affrontare le questioni esistenti e le eventuali questioni nuove che si presenteranno.

Adattamento del sito web dedicato al quadro per la protezione dei dati personali ai gruppi di destinatari

Il Dipartimento intende adattare il sito web dedicato al quadro per la protezione dei dati personali affinché sia incentrato sui seguenti gruppi di destinatari: cittadini dell'UE, imprese dell'UE, imprese statunitensi e autorità di protezione dei dati. L'inserimento di documentazione mirata direttamente alle persone fisiche e imprese dell'UE favorisce la trasparenza in vari modi. Alle persone fisiche dell'UE il sito web illustra chiaramente: 1) i diritti che il DPF UE-USA conferisce alle persone dell'UE; 2) i meccanismi di ricorso di cui dispongono qualora ritengano che un'organizzazione sia venuta meno all'impegno di attenersi ai principi; e 3) in che modo reperire informazioni sull'autocertificazione con cui l'organizzazione si è vincolata al DPF UE-USA. Alle imprese dell'UE rende più agevole verificare: 1) se un'organizzazione aderisce al DPF UE-USA; 2) il tipo di informazioni contemplate dall'autocertificazione con cui l'organizzazione si è vincolata al DPF UE-USA; 3) la politica della privacy che si applica alle informazioni contemplate; e 4) il metodo con cui l'organizzazione si accerta di rispettare i principi. Alle imprese statunitensi il sito illustra chiaramente: 1) i vantaggi dell'adesione al DPF UE-USA; 2) le modalità di adesione al DPF UE-USA nonché quelle per ricertificarsi e per abbandonare tale regime; e 3) il modo in cui gli Stati Uniti gestiscono e applicano il DPF UE-USA. L'inclusione di materiale destinato direttamente alle autorità di protezione dei dati (ad esempio, informazioni sul punto di contatto specifico del Dipartimento dedicato alle autorità di protezione dei dati e un collegamento ipertestuale ai contenuti relativi ai principi sul sito web dell'FTC) facilita sia la cooperazione che la trasparenza. Il Dipartimento lavorerà inoltre su base ad hoc con la Commissione e il comitato europeo per la protezione dei dati ("EDPB") per sviluppare materiale aggiuntivo su tematiche specifiche (ad esempio risposte alle domande frequenti) da utilizzare sul sito web dedicato al quadro per la protezione dei dati personali, qualora tali informazioni faciliterebbero l'efficienza della gestione e della supervisione del programma del quadro per la protezione dei dati personali.

Agevolazione della cooperazione con le autorità di protezione dei dati

Al fine di aumentare le possibilità di cooperazione con le autorità di protezione dei dati, il Dipartimento mantiene al proprio interno un referente incaricato di agire da punto di collegamento con tali autorità. Se reputa che una data organizzazione aderente al DPF UE-USA 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. Il Dipartimento si impegna al massimo con l'organizzazione aderente al DPF UE-USA per favorire la soluzione del caso di reclamo. Entro 90 giorni dal ricevimento del reclamo, il Dipartimento aggiorna l'autorità di protezione dei dati in merito alla situazione. Il punto di contatto specifico riceve inoltre deferimenti riguardanti le organizzazioni che millantano di aderire al DPF UE-USA. Il referente dedicato tiene traccia di tutti casi sottoposti al Dipartimento dalle autorità di protezione dei dati; nel riesame congiunto illustrato infra, il Dipartimento include un'analisi aggregata dei reclami ricevuti ogni anno. Il referente dedicato assiste le autorità di protezione dei dati che chiedono informazioni sull'autocertificazione o sulla precedente partecipazione di una data organizzazione al DPF UE-USA e risponde alle loro domande circa l'attuazione di specifici obblighi collegati a tale regime. Il Dipartimento coopererà inoltre con la Commissione e l'EDPB in relazione agli aspetti procedurali e amministrativi del comitato di autorità di protezione dei dati, compresa l'istituzione di procedure adeguate per la distribuzione dei fondi riscossi tramite il contributo da versare per tale comitato. Ci risulta che la Commissione collaborerà con il Dipartimento per facilitare la risoluzione di eventuali questioni che dovessero sorgere in relazione a tali procedure. 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 sul DPF UE-USA da caricare sui loro siti web. Grazie alla sensibilizzazione sul DPF UE-USA 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.

Soddisfacimento degli impegni di cui all'allegato I dei principi

Il Dipartimento adempie gli impegni di cui all'allegato I dei principi, anche tenendo un elenco di arbitri scelti con la Commissione sulla base dei criteri di indipendenza, integrità e competenze; e sostenendo, se del caso, il terzo scelto dal Dipartimento per gestire gli arbitrati e il fondo arbitrale di cui all'allegato I dei principi ([3]). Il Dipartimento collabora con il terzo per verificare, tra l'altro, che quest'ultimo mantenga un sito web contenente indicazioni sul procedimento arbitrale, che specifichi tra l'altro: 1) le modalità per avviare tale procedimento e presentare la documentazione; 2) l'elenco degli arbitri tenuto dal Dipartimento e le modalità di selezione degli arbitri da tale elenco; 3) le procedure arbitrali disciplinate e il codice di condotta degli arbitri adottati dal Dipartimento e dalla Commissione ([4]); e 4) la riscossione e il pagamento degli onorari degli arbitri. Inoltre il Dipartimento collabora periodicamente con tale terzo per esaminare il funzionamento del fondo, compresa la necessità di adeguare le quote o i massimali (ossia gli importi massimi) per le spese arbitrali, e considera 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 al DPF UE-USA. Il Dipartimento notifica alla Commissione l'esito di tali esami con detto terzo e le trasmette una notifica preventiva di eventuali adeguamenti dell'importo dei contributi.

Conduzione di riesami congiunti del funzionamento del DPF UE-USA

Il Dipartimento e altri enti, se del caso, tengono riunioni periodiche con la Commissione, le autorità di protezione dei dati interessate e i rappresentanti competenti dell'EDPB, nel contesto delle quali il Dipartimento fornisce aggiornamenti sul DPF UE-USA. Tali riunioni contemplano la discussione di questioni di attualità relative al funzionamento, all'attuazione, alla supervisione e all'applicazione del programma relativo al quadro per la protezione dei dati personali. Le riunioni possono comprendere, se del caso, la discussione di argomenti correlati, quali altri meccanismi di trasferimento dei dati che beneficiano delle garanzie previste dal DPF UE-USA.

([3]) L'*International Centre for Dispute Resolution* (ICDR, Centro internazionale per la composizione delle controversie), la divisione internazionale dell'*American Arbitration Association* (AAA, Associazione americana per l'arbitrato) (collettivamente "ICDR-AAA"), è stato selezionato dal Dipartimento per gestire gli arbitrati e il fondo arbitrale di cui all'allegato I dei principi.

([4]) Il 15 settembre 2017 il Dipartimento e la Commissione hanno approvato l'adozione di una serie di norme arbitrali destinate a disciplinare i procedimenti arbitrali vincolanti di cui all'allegato I dei principi, nonché di un codice di condotta per gli arbitri che sia conforme alle norme etiche generalmente accettate per gli arbitri commerciali e all'allegato I dei principi. Il Dipartimento e la Commissione hanno convenuto di adeguare le norme arbitrali e il codice di condotta per tenere conto degli aggiornamenti nell'ambito del DPF UE-USA e collaboreranno con l'ICDR-AAA per effettuare tali aggiornamenti.

Aggiornamenti normativi

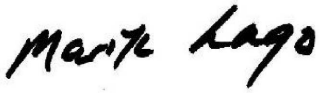
Il Dipartimento si adopera in ogni modo ragionevole per informare la Commissione, se pertinenti ai fini del DPF UE-USA, degli sviluppi rilevanti della normativa statunitense in materia di tutela dei dati personali e di limitazioni e garanzie applicabili all'accesso ai dati personali da parte delle autorità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

Accesso ai dati personali da parte di pubbliche amministrazioni statunitensi

Gli Stati Uniti hanno emanato il decreto presidenziale 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" e il codice dei regolamenti federali, titolo 28, parte 201, che modifica i regolamenti del ministero della Giustizia al fine di istituire il "Data Protection Review Court" (DPRC, tribunale del riesame in materia di protezione dei dati), due atti che offrono una forte protezione dei dati personali per quanto concerne l'accesso agli stessi da parte di pubbliche amministrazioni per finalità di sicurezza nazionale. La protezione fornita comprende: il rafforzamento della tutela della vita privata e delle libertà civili al fine di garantire che le attività statunitensi di intelligence dei segnali siano necessarie e proporzionate al perseguimento di determinati obiettivi di sicurezza nazionale; l'istituzione di un nuovo meccanismo di ricorso con un'autorità indipendente e vincolante; e il rafforzamento della vigilanza rigorosa e a più livelli esistente sulle attività statunitensi di intelligence dei segnali. Grazie a tali tutele, le persone dell'UE possono presentare ricorso presso un nuovo meccanismo di ricorso a più livelli, che comprende un DPRC indipendente composto da persone scelte al di fuori dell'amministrazione statunitense, che avrebbero piena autorità per pronunciarsi in merito alle istanze presentate e per disporre, se necessario, l'adozione di misure correttive. Il Dipartimento tiene un registro delle persone dell'UE che presentano un reclamo qualificato ai sensi del decreto presidenziale 14086 e del codice dei regolamenti federali, titolo 28, parte 201. Cinque anni dopo la data della presente lettera, e successivamente ogni cinque anni, il Dipartimento contatterà gli enti competenti in merito alla declassificazione delle informazioni relative all'esame dei reclami qualificati o all'esame di eventuali domande di riesame presentate al DPRC. Qualora tali informazioni siano state declassificate, il Dipartimento collaborerà con l'autorità di protezione dei dati competente per informare la persona dell'UE. Tali miglioramenti confermano che i dati personali dell'UE trasferiti negli Stati Uniti saranno trattati in modo coerente con gli obblighi giuridici in vigore nell'UE in materia di accesso ai dati da parte delle pubbliche amministrazioni.

Alla luce dei principi, del decreto presidenziale 14086, del codice dei regolamenti federali, titolo 28, parte 201, e delle lettere e della documentazione di accompagnamento, compresi gli impegni assunti dal Dipartimento circa la gestione e la supervisione del programma relativo al quadro per la protezione dei dati personali, il Dipartimento confida che la Commissione giungerà alla conclusione che il DPF UE-USA 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 a tale regime. Il Dipartimento si attende inoltre che i trasferimenti verso le organizzazioni statunitensi effettuati in base alle clausole contrattuali tipo dell'UE o alle norme vincolanti d'impresa dell'UE saranno ulteriormente agevolati dai termini di tali accordi.

La prego di accogliere, signor Commissario, i sensi
della mia più alta stima.



Marisa LAGO

ALLEGATO IV

STATI UNITI D'AMERICA
Commissione federale del commercio
WASHINGTON, D.C. 20580

Ufficio della Presidente

9 giugno 2023

Didier Reynders
Commissario per la Giustizia
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissario Reynders,

la Commissione federale del commercio degli Stati Uniti ("FTC") si pregia di illustrare il proprio ruolo nell'applicazione dei principi del quadro UE-USA per la protezione dei dati personali ("DPF UE-USA"). L'FTC è impegnata da tempo a tutelare i consumatori e la vita privata a livello transfrontaliero e si impegna a far rispettare gli aspetti di tale quadro nel settore commerciale. L'FTC svolge tale ruolo dal 2000, in relazione al quadro UE-USA dell'approdo sicuro, e più recentemente dal 2016, in relazione al quadro dello scudo UE-USA per la privacy ([1]). Il 16 luglio 2020 la Corte di giustizia dell'Unione europea ha annullato la decisione di adeguatezza della Commissione europea basata sul quadro dello scudo UE-USA per la privacy, in ragione di questioni diverse dai principi commerciali applicati dall'FTC. Da allora gli Stati Uniti e la Commissione europea hanno negoziato il quadro UE-USA per la protezione dei dati personali per far fronte a tale sentenza della Corte di giustizia dell'Unione europea.

Le scrivo per confermare l'impegno dell'FTC a far rispettare con vigore i principi del DPF UE-USA. L'FTC s'impegna in particolare su tre aspetti fondamentali: 1) attribuzione di priorità ai casi e indagini; 2) ottenimento e controllo di provvedimenti; e 3) cooperazione esecutiva con le autorità di protezione dei dati.

I. **Introduzione**

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 a una vasta gamma di leggi intese alla tutela della vita privata e alla sicurezza dei consumatori e dei dati che li riguardano. Tra queste la

([1]) Lettera della presidente Edith Ramirez a Věra Jourová, commissaria per la Giustizia, i consumatori e la parità di genere della Commissione europea, che descrive l'applicazione del nuovo quadro dello scudo UE-USA per la privacy da parte della Commissione federale del commercio (29 febbraio 2016), *disponibile all'indirizzo* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. L'FTC si era inoltre impegnata in precedenza ad applicare il programma "approdo sicuro" attuato tra gli Stati Uniti e l'UE. Lettera di Robert Pitofsky, presidente dell'FTC, a John Mogg, direttore della DG Mercato interno, Commissione europea (14 luglio 2000), *disponibile all'indirizzo* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. La presente lettera sostituisce tali impegni precedenti.

principale è la legge sull'FTC stessa, che proibisce gli atti o pratiche "sleali" o "ingannevoli" nel commercio o inerenti al commercio ([2]). 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 ([3]).

Di recente l'FTC ha inoltre portato avanti numerose iniziative volte a rafforzare la sua attività in materia di protezione dei dati. Nell'agosto 2022 l'FTC ha annunciato di stare valutando la possibilità di introdurre norme volte a reprimere la sorveglianza commerciale dannosa e il lassismo nella sicurezza dei dati ([4]). L'obiettivo del progetto è quello di creare un registro pubblico affidabile che informi l'FTC in merito all'opportunità di emanare norme per affrontare le pratiche di sorveglianza commerciale e di sicurezza dei dati e al contenuto eventuale di tali norme. L'FTC ha accolto con favore le osservazioni dei portatori di interessi dell'UE in merito a questa e altre iniziative.

Le conferenze "PrivacyCon" dell'FTC continuano a riunire ricercatori di spicco per discutere in merito alle più recenti ricerche e tendenze relative alla tutela della vita privata e della sicurezza dei dati dei consumatori. L'FTC ha inoltre aumentato la capacità dell'ente di tenere il passo con gli sviluppi tecnologici al centro di gran parte del suo lavoro in materia di tutela della vita privata, creando un gruppo in crescita di tecnici e ricercatori interdisciplinari. Come sapete, l'FTC ha annunciato altresì un dialogo congiunto con Lei e i Suoi colleghi della Commissione europea, che comprende la trattazione di temi relativi alla tutela della vita privata quali i modelli oscuri e i modelli aziendali caratterizzati da una raccolta di dati pervasiva ([5]). Recentemente l'FTC ha inoltre pubblicato una relazione indirizzata al Congresso in merito ai danni associati all'uso dell'intelligenza artificiale ("IA") per affrontare i danni online individuati dal Congresso. Tale relazione ha sollevato preoccupazioni in merito all'imprecisione, alla parzialità, alla discriminazione e al carattere subdolo della sorveglianza commerciale ([6]).

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

Il DPF UE-USA si innesta sul più ampio panorama statunitense della privacy, che offre ai consumatori dell'UE altresì vari tipi di tutele. 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 di cui dispongono i consumatori statunitensi ([7]).

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

([2]) Codice degli Stati Uniti, titolo 15, articolo 45, lettera a). L'FTC non ha competenza giurisdizionale 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, ma ne ha per i soggetti che si presentano come associazioni di beneficenza o altrimenti senza scopo di lucro ma che in effetti 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. 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.

([3]) *Cfr.* FTC, Privacy and Security, https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Cfr.* comunicato stampa, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (11 agosto 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *Cfr.* comunicato stampa congiunto di Didier Reynders, commissario per la Giustizia della Commissione europea, e di Lina Khan, presidente della Commissione federale del commercio degli Stati Uniti (30 marzo 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *Cfr.* comunicato stampa, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (16 giugno 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) Codice degli Stati Uniti, titolo 15, articolo 45, lettera a), punto 4), lettera B). Inoltre, per "atti o pratiche sleali o ingannevoli" si intendono gli atti o le pratiche riguardanti il commercio estero che i) causano o presentano probabilità di causare danni ragionevolmente prevedibili negli USA o ii) implicano un comportamento rilevante tenuto negli Stati Uniti (codice degli Stati Uniti, titolo 15, articolo 45, lettera a), punto 4), lettera 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. Inoltre, 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, violazioni dei dati e di tutela della vita privata.

c. **Attività di applicazione della normativa svolta dall'FTC**

L'FTC ha avviato procedimenti tanto nell'ambito del quadro UE-USA dell'approdo sicuro quanto dello scudo UE-USA per la privacy e ha continuato ad applicare quest'ultimo regime anche dopo l'annullamento da parte della Corte di giustizia dell'Unione europea della decisione di adeguatezza sottostante al quadro dello scudo UE-USA per la privacy ([8]). Numerose delle recenti denunce dell'FTC hanno incluso segnalazioni secondo cui le imprese hanno violato le disposizioni dello scudo UE-USA per la privacy, anche nei procedimenti avviati nei confronti di Twitter ([9]), CafePress ([10]) e Flo ([11]). Nell'azione coercitiva attuata nei confronti di Twitter, l'FTC ha ottenuto 150 milioni di USD da tale impresa in ragione della sua violazione di un precedente provvedimento dell'FTC in relazione a pratiche che hanno interessato più di 140 milioni di clienti, compresa la violazione del principio 5 dello scudo UE-USA per la privacy (integrità dei dati e limitazione della finalità). Inoltre il provvedimento dell'FTC impone a Twitter di consentire agli utenti di utilizzare metodi sicuri di autenticazione a più fattori che non richiedono agli utenti di fornire i loro numeri di telefono.

Nel caso *CafePress*, l'FTC ha affermato che la società non era riuscita a proteggere le informazioni sensibili dei consumatori, aveva insabbiato una grave violazione dei dati e aveva violato i principi 2 (scelta), 4 (sicurezza) e 6 (accesso) dello scudo UE-USA per la privacy. Il provvedimento dell'FTC ha imposto alla società di sostituire le misure di autenticazione inadeguate con un'autenticazione a più fattori, di limitare sostanzialmente la quantità di dati raccolti e conservati, di criptare i numeri di previdenza sociale, di far valutare da terzi i propri programmi di sicurezza delle informazioni e di fornire all'FTC una copia che possa essere pubblicata.

Nel caso *Flo*, l'FTC ha sostenuto che l'applicazione di tracciamento della fertilità aveva divulgato informazioni sulla salute degli utenti a prestatori terzi di analisi dei dati dopo aver assunto impegni a mantenere riservate tali informazioni. La denuncia dell'FTC constata in particolare le interazioni della società con consumatori dell'UE così come il fatto che Flo ha violato i principi dello scudo UE-USA per la privacy 1 (informativa), 2 (scelta), 3 (responsabilità in caso di trasferimento successivo) e 5 (integrità dei dati e limitazione della finalità). Tra le altre cose, il provvedimento dell'FTC ha imposto a Flo di comunicare agli utenti interessati la divulgazione delle loro informazioni personali e di incaricare i terzi che hanno ricevuto le informazioni sanitarie degli utenti di distruggere tali dati. È importante sottolineare che i provvedimenti dell'FTC tutelano i consumatori che, in tutto il mondo, interagiscono con l'impresa statunitense e non soltanto quelli che hanno presentato il reclamo.

Numerosi casi passati di azione coercitiva in relazione al quadro UE-USA dell'approdo sicuro e allo scudo UE-USA per la privacy hanno riguardato organizzazioni che hanno completato un'autocertificazione iniziale tramite il Dipartimento del Commercio, ma non hanno provveduto all'autocertificazione annuale pur continuando a dichiararsi aderenti effettivi al regime in questione. Altri casi hanno riguardato casi di millantata adesione da parte di organizzazioni che non hanno mai completato un'autocertificazione iniziale tramite il Dipartimento del Commercio. In futuro, l'FTC prevede di concentrare i propri sforzi proattivi in materia di applicazione delle norme sui tipi di violazioni sostanziali dei principi del DPF UE-USA asserite nel contesto di casi quali Twitter, CafePress e Flo. Nel frattempo il Dipartimento del Commercio gestirà e supervisionerà il processo di autocertificazione, terrà l'elenco ufficiale degli aderenti al DPF UE-USA e affronterà altre questioni relative alle dichiarazioni di adesione al regime ([12]). È importante sottolineare che le organizzazioni che chiedono di aderire al DPF UE-USA possono essere soggette all'applicazione sostanziale dei principi di tale regime anche se non effettuano o non rinnovano l'autocertificazione tramite il Dipartimento del Commercio.

([8]) *Cfr.* appendice A per un elenco delle questioni relative all'approdo sicuro e allo scudo per la privacy trattate dall'FTC.

([9]) *Cfr.* comunicato stampa, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (25 maggio 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *Cfr.* comunicato stampa, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (15 marzo 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *Cfr.* comunicato stampa, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (22 giugno 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Lettera di Marisa Lago, Sottosegretaria al Commercio, incaricata del commercio internazionale, a Didier Reynders, commissario per la Giustizia, Commissione europea (12 dicembre 2022).

II. **Attribuzione di priorità ai casi e indagini**

Come avvenuto nel contesto del quadro UE-USA dell'approdo sicuro e dello scudo UE-USA per la privacy, l'FTC si impegna a considerare in via prioritaria le segnalazioni relative ai principi del DPF UE-USA formulate dal Dipartimento del Commercio e dagli Stati membri dell'UE. L'FTC intende inoltre dare priorità all'esame di segnalazioni relative al mancato rispetto dei principi del DPF UE-USA da parte di organizzazioni di autoregolamentazione nel settore della privacy e di altri organi indipendenti di composizione delle controversie.

L'FTC ha creato una procedura standard per agevolare gli Stati membri dell'UE nella presentazione dei casi nell'ambito del DPF UE-USA e ha fornito orientamenti indicanti il tipo di informazioni che le saranno più utili ai fini dell'esame del caso sottopostole. In questo contesto l'FTC ha nominato 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 cooperare alle indagini dell'FTC.

Quando investita di un tale caso dal Dipartimento del Commercio, da uno Stato membro dell'UE, da un organo di autoregolamentazione o da altri organi indipendenti di composizione delle controversie, l'FTC può affrontare le questioni sottopostele intervenendo su vari fronti, ad esempio verificando le politiche della privacy seguite dall'organizzazione, ottenendo ulteriori informazioni dall'organizzazione 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 sforzi aggiuntivi per avvertire i partecipanti al mercato e, se del caso, avviando un procedimento coercitivo.

Oltre a dare priorità ai casi deferiti concernenti i principi del DPF UE-USA da parte del Dipartimento del Commercio, degli Stati membri dell'UE e delle organizzazioni di autoregolamentazione nel settore della privacy o di altri organi indipendenti di composizione delle controversie ([13]), l'FTC continuerà, se del caso, a indagare di propria iniziativa in merito a violazioni significative dei principi del DPF UE-USA, utilizzando una serie di strumenti. Nell'ambito del programma di indagine dell'FTC in merito a questioni in materia di tutela della vita privata e sicurezza che coinvolgono organizzazioni commerciali, l'FTC ha esaminato periodicamente se il soggetto in questione stava rilasciando dichiarazioni in merito allo scudo UE-USA per la privacy. In caso affermativo, se dall'indagine risultava una manifesta violazione dei relativi principi, l'FTC ha incluso accuse di violazioni dello scudo UE-USA per la privacy nell'azione coercitiva avviata. L'FTC intende continuare a seguire tale approccio proattivo, ora per quanto riguarda i principi del DPF UE-USA.

III. **Ottenimento e controllo di provvedimenti**

L'FTC s'impegna a ottenere e controllare l'attuazione di provvedimenti coercitivi destinati ad assicurare la conformità rispetto ai principi del DPF UE-USA. L'FTC imporrà tale conformità rispetto ai principi del DPF UE-USA inserendo una serie adeguata di ingiunzioni nei suoi futuri provvedimenti adottati in relazione ai principi del DPF UE-USA. Violare un provvedimento amministrativo disposto dall'FTC può comportare una sanzione civile fino a 50 120 USD per singola violazione oppure, in caso di violazione reiterata ([14]), pari a 50 120 USD al giorno: 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.

L'FTC controlla sistematicamente il rispetto dei provvedimenti esistenti relativi ai principi dello scudo UE-USA per la privacy, come avviene per tutti i suoi provvedimenti, e avvia azioni per farli rispettare, se necessario ([15]). 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 dei principi del DPF UE-USA ([16]).

([13]) 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 relativi al DPF UE-USA 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 presso l'FTC, le persone dell'UE dispongono dello stesso sistema di reclamo offerto ai consumatori statunitensi all'indirizzo https://reportfraud.ftc.gov/. Per il singolo reclamo relativo ai principi del DPF UE-USA, la persona dell'UE potrebbe tuttavia trovare più utile presentarlo all'autorità di protezione dei dati del proprio Stato membro o a un organo indipendente di composizione delle controversie.

([14]) Codice degli Stati Uniti, titolo 15, articolo 45, lettera m); Codice dei regolamenti federali, titolo 16, articolo 1.98. Tale importo è periodicamente adeguato per tenere conto dell'inflazione.

([15]) Lo scorso anno l'FTC ha votato per razionalizzare il processo di indagine in merito ai soggetti che commettono reati reiterati. *Cfr.* comunicato stampa, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (1° luglio 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Cfr.* FTC, Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **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 possono svolgere per la conformità ai principi del DPF UE-USA, l'FTC incoraggia a intensificare la consultazione e la cooperazione esecutiva con esse. In effetti un approccio coordinato alle sfide poste dagli attuali sviluppi del mercato digitale e dai modelli aziendali ad alta intensità di dati è sempre più critico. L'FTC intende 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 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 ([17]). 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.

Oltre a consultare l'autorità di protezione dei dati dell'UE richiedente sulle questioni relative al singolo caso, l'FTC si riunirà periodicamente con i rappresentanti designati del comitato europeo per la protezione dei dati (EDPB) per discutere in generale sul modo di migliorare la cooperazione esecutiva. Parteciperà anche, assieme al Dipartimento del Commercio, alla Commissione europea e ai rappresentanti dell'EDPB, alla valutazione periodica del DPF UE-USA 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. L'FTC è lieta di affermare il proprio impegno a far rispettare gli aspetti del DPF UE-USA nel settore commerciale. Consideriamo il nostro partenariato con i colleghi dell'UE un aspetto fondamentale per garantire la protezione della privacy sia per i nostri cittadini che per i vostri.

La prego di accogliere, signor Commissario, i sensi della mia più alta stima.

Lina M. KHAN
Presidente della Commissione federale del commercio

([17]) 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; 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, titolo 15, articolo 46, lettera j), punto 3)). Questo potere non vale per l'applicazione della normativa sulla concorrenza.

Appendice A

Scudo per la privacy e applicazione dell'approdo sicuro

	Prot./Fascicolo FTC n.	Procedimento	Collegamento
1	Fascicolo FTC n. 2023062 Caso n. 3:22-cv-03070 (N.D. Cal.)	*US v.* **Twitter, Inc.**	Twitter
2	Fascicolo FTC n. 192 3209	*In the Matter of Residual Pumpkin Entity, LLC, formerly d/b/a* **CafePress**, *and PlanetArt, LLC, d/b/a* **CafePress**	CafePress
3	Fascicolo FTC n. 192 3133 Prot. n. C-4747	*In the Matter of* **Flo Health, Inc.**	Flo Health
4	Fascicolo FTC n. 192 3050 Prot. n. C-4723	*In the Matter of* **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	Fascicolo FTC n. 192 3092 Prot. n. C-4709	*In the Matter of* **T&M Protection, LLC**	T&M Protection
6	Fascicolo FTC n. 192 3084 Prot. n. C-4704	*In the Matter of* **TDARX, Inc.**	TDARX
7	Fascicolo FTC n. 192 3093 Prot. n. C-4706	*In the Matter of* **Global Data Vault, LLC**	Global Data
8	Fascicolo FTC n. 192 3078 Prot. n. C-4703	*In the Matter of* **Incentive Services, Inc.**	Incentive Services
9	Fascicolo FTC n. 192 3090 Prot. n. C-4705	*In the Matter of* **Click Labs, Inc.**	Click Labs
10	Fascicolo FTC n. 182 3192 Prot. n. C-4697	*In the Matter of* **Medable, Inc.**	Medable
11	Fascicolo FTC n. 182 3189 Prot. n. 9386	*In the Matter of NTT Global Data Centers Americas, Inc., as successor in interest to* **RagingWire Data Centers, Inc.**	RagingWire
12	Fascicolo FTC n. 182 3196 Prot. n. C-4702	*In the Matter of* **Thru, Inc.**	Thru
13	Fascicolo FTC n. 182 3188 Prot. n. C-4698	*In the Matter of* **DCR Workforce, Inc.**	DCR Workforce
14	Fascicolo FTC n. 182 3194 Prot. n. C-4700	*In the Matter of* **LotaData, Inc.**	LotaData
15	Fascicolo FTC n. 182 3195 Prot. n. C-4701	*In the Matter of* **EmpiriStat, Inc.**	EmpiriStat

16	Fascicolo FTC n. 182 3193 Prot. n. C-4699	*In the Matter of 214 Technologies, Inc., also d/b/a* **Trueface.ai**	Trueface.ai
17	Fascicolo FTC n. 182 3107 Prot. n. 9383	*In the Matter of* **Cambridge Analytica, LLC**	Cambridge Analytica
18	Fascicolo FTC n. 182 3152 Prot. n. C-4685	*In the Matter of* **SecureTest, Inc.**	SecurTest
19	Fascicolo FTC n. 182 3144 Prot. n. C-4664	*In the Matter of* **VenPath, Inc.**	VenPath
20	Fascicolo FTC n. 182 3154 Prot. n. C-4666	*In the Matter of* **SmartStart Employment Screening, Inc.**	SmartStart
21	Fascicolo FTC n. 182 3143 Prot. n. C-4663	*In the Matter of* **mResourceLLC,** *d/b/a Loop Works LLC*	mResource
22	Fascicolo FTC n. 182 3150 Prot. n. C-4665	*In the Matter of* **Idmission LLC**	IDmission
23	Fascicolo FTC n. 182 3100 Prot. n. C-4659	*In the Matter of* **ReadyTech Corporation**	ReadyTech
24	Fascicolo FTC n. 172 3173 Prot. n. C-4630	*In the Matter of* **Decusoft, LLC**	Decusoft
25	Fascicolo FTC n. 172 3171 Prot. n. C-4628	*In the Matter of* **Tru Communication, Inc.**	Tru
26	Fascicolo FTC n. 172 3172 Prot. n. C-4629	*In the Matter of* **Md7, LLC**	Md7
30	Fascicolo FTC n. 152 3198 Prot. n. C-4543	*In the Matter of* **Jhayrmaine Daniels (d/b/a California Skate-Line)**	Jhayrmaine Daniels
31	Fascicolo FTC n. 152 3190 Prot. n. C-4545	*In the Matter of* **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	Fascicolo FTC n. 152 3141 Prot. n. C-4540	*In the Matter of* **Golf Connect, LLC**	Golf Connect
33	Fascicolo FTC n. 152 3202 Prot. n. C-4546	*In the Matter of* **Inbox Group, LLC**	Inbox Group
34	Fascicolo n. 152 3187 Prot. n. C-4542	*In the Matter of* **IOActive, Inc.**	IOActive
35	Fascicolo FTC n. 152 3140 Prot. n. C-4549	*In the Matter of* **Jubilant Clinsys, Inc.**	Jubilant
36	Fascicolo FTC n. 152 3199 Prot. n. C-4547	*In the Matter of* **Just Bagels Manufacturing, Inc.**	Just Bagels

37	Fascicolo FTC n. 152 3138 Prot. n. C-4548	*In the Matter of* **NAICS Association, LLC**	NAICS
38	Fascicolo FTC n. 152 3201 Prot. n. C-4544	*In the Matter of* **One Industries Corp.**	One Industries
39	Fascicolo FTC n. 152 3137 Prot. n. C-4550	*In the Matter of* **Pinger, Inc.**	Pinger
40	Fascicolo FTC n. 152 3193 Prot. n. C-4552	*In the Matter of* **SteriMed Medical Waste Solutions**	SteriMed
41	Fascicolo FTC n. 152 3184 Prot. n. C-4541	*In the Matter of* **Contract Logix, LLC**	Contract Logix
42	Fascicolo FTC n. 152 3185 Prot. n. C-4551	*In the Matter of* **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	Fascicolo FTC n. 152 3051 Prot. n. C-4526	*In the Matter of* **American Int'l Mailing, Inc.**	AIM
44	Fascicolo FTC n. 152 3015 Prot. n. C-4525	*In the Matter of* **TES Franchising, LLC**	TES
45	Fascicolo FTC n. 142 3036 Prot. n. C-4459	*In the Matter of* **American Apparel, Inc.**	American Apparel
46	Fascicolo FTC n. 142 3026 Prot. n. C-4469	*In the Matter of* **Fantage.com, Inc.**	Fantage
47	Fascicolo FTC n. 142 3017 Prot. n. C-4461	*In the Matter of* **Apperian, Inc.**	Apperian
48	Fascicolo FTC n. 142 3018 Prot. n. C-4462	*In the Matter of* **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	Fascicolo FTC n. 142 3019 Prot. n. C-4463	*In the Matter of* **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	Fascicolo FTC n. 142 3020 Prot. n. C-4464	*In the Matter of* **BitTorrent, Inc.**	*BitTorrent*
51	Fascicolo FTC n. 142 3022 Prot. n. C-4465	*In the Matter of* **Charles River Laboratories, Int'l**	Charles River
52	Fascicolo FTC n. 142 3023 Prot. n. C-4466	*In the Matter of* **DataMotion, Inc.**	DataMotion
53	Fascicolo FTC n. 142 3024 Prot. n. C-4467	*In the Matter of* **DDC Laboratories, Inc.**, *d/b/a DNA Diagnostics Center*	DDC
54	Fascicolo FTC n. 142 3028 Prot. n. C-4470	*In the Matter of* **Level 3 Communications, LLC**	Level 3

55	Fascicolo FTC n. 142 3025 Prot. n. C-4468	*In the Matter of* **PDB Sports, Ltd.**, *d/b/a the Denver Broncos Football Club, LLP*	Broncos
56	Fascicolo FTC n. 142 3030 Prot. n. C-4471	*In the Matter of* **Reynolds Consumer Products, Inc.**	Reynolds
57	Fascicolo FTC n. 142 3031 Prot. n. C-4472	*In the Matter of* **Receivable Management Services Corporation**	Receivable Mgmt
58	Fascicolo FTC n. 142 3032 Prot. n. C-4473	*In the Matter of* **Tennessee Football, Inc.**	Tennessee Football
59	Fascicolo FTC n. 102 3058 Prot. n. C-4369	*In the Matter of* **Myspace LLC**	Myspace
60	Fascicolo FTC n. 092 3184 Prot. n. C-4365	*In the Matter of* **Facebook, Inc.**	Facebook
61	Fascicolo FTC n. 092 3081 Azione civile n. 09-CV-5276 (C.D. Cal.)	*FTC v. Javian Karnani, and* **Balls of Kryptonite, LLC**, *d/b/a Bite Size Deals, LLC, and Best Priced Brands, LLC*	Balls of Kryptonite
62	Fascicolo FTC n. 102 3136 Prot. n. C-4336	*In the Matter of* **Google, Inc.**	Google
63	Fascicolo FTC n. 092 3137 Prot. n. C-4282	*In the Matter of* **World Innovators, Inc.**	World Innovators
64	Fascicolo FTC n. 092 3141 Prot. n. C-4271	*In the Matter of* **Progressive Gaitways LLC**	Progressive Gaitways
65	Fascicolo FTC n. 092 3139 Prot. n. C-4270	*In the Matter of* **Onyx Graphics, Inc.**	Onyx Graphics
66	Fascicolo FTC n. 092 3138 Prot. n. C-4269	*In the Matter of* **ExpatEdge Partners, LLC**	ExpatEdge
67	Fascicolo FTC n. 092 3140 Prot. n. C-4281	*In the Matter of* **Directors Desk LLC**	Directors Desk
68	Fascicolo FTC n. 092 3142 Prot. n. C-4272	*In the Matter of* **Collectify LLC**	Collectify

ALLEGATO V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 luglio 2023

Commissario Didier Reynders
Commissione europea
Rue de la Loi/Wetstraat 200
1049 Bruxelles
Belgio

Gentile Commissario Reynders,

il Dipartimento dei Trasporti degli Stati Uniti ("Dipartimento" o "DOT") si pregia di illustrare il proprio ruolo nell'applicazione dei principi del quadro UE-USA per la protezione dei dati personali ("DPF UE-USA"). In un mondo sempre più interconnesso il DPF UE-USA ha un'importanza fondamentale ai fini della tutela dei dati personali comunicati nelle operazioni commerciali. 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.

Il DOT ha espresso per la prima volta pubblicamente il proprio impegno a favore dell'applicazione del quadro UE-USA dell'approdo sicuro in una lettera inviata alla Commissione europea più di 22 anni fa, impegni che sono stati ribaditi e ampliati in una lettera del 2016 relativa al quadro dello scudo UE-USA per la privacy. Il DOT si è impegnato ad applicare con vigore, in tali lettere, i principi del quadro USA-UE dell'approdo sicuro e, successivamente, quelli dello scudo UE-USA per la privacy. Il DOT estende tale impegno ai principi del DPF UE-USA e la presente lettera rievoca e ribadisce tale impegno.

In particolare il DOT conferma l'impegno assunto sui seguenti aspetti fondamentali: 1) attribuzione di priorità all'esame delle presunte violazioni dei principi del DPF UE-USA; 2) adeguato intervento coercitivo nei confronti dei soggetti che millantano l'adesione al DPF UE-USA; e 3) controllo dell'esecuzione e pubblicazione dei provvedimenti coercitivi inerenti a violazioni dei principi del DPF UE-USA. 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 dei principi del DPF UE-USA.

1. **Contesto**

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, titolo 49, articolo 41712, che vieta al vettore o al rivenditore che fa servizio di biglietteria, nell'attività di trasporto aereo o di vendita di trasporto aereo, qualsiasi "pratica sleale o ingannevole". L'articolo 41712 è modellato sull'articolo 5 della legge sulla Commissione federale del Commercio (FTC) (codice degli Stati Uniti, titolo 15, articolo 45).

Di recente il DOT ha emanato regolamenti che definiscono le pratiche sleali e ingannevoli, in linea con i precedenti sia del DOT che dell'FTC (codice dei regolamenti federali, titolo 14, articolo 399.79). In particolare è "sleale" l'atto o la pratica che causa o rischia di causare un danno rilevante, non ragionevolmente evitabile, che non è compensato da un beneficio superiore per i consumatori o per la concorrenza.

Una pratica è "ingannevole" nei confronti dei consumatori quando rischia di fuorviare il consumatore che tiene un comportamento ragionevole in considerazione delle circostanze in relazione a una materia rilevante. Una questione è rilevante se è suscettibile di incidere sul comportamento o sulla decisione del consumatore in relazione a un prodotto o a un servizio. Oltre a questi principi generali, il DOT interpreta specificamente l'articolo 41712 nel senso che vieta alle compagnie aeree o ai rivenditori che fanno servizio di biglietteria: 1) di violare i termini della propria politica della privacy; 2) di violare le norme emanate dal Dipartimento in cui determinate pratiche in materia di privacy sono indicate come sleali o ingannevoli; o 3) di violare la legge sulla tutela della vita privata dei minori online (COPPA) o le norme dell'FTC che la attuano; o 4) di non rispettare, in qualità di aderente al DPF UE-USA, i principi di detto regime ([1]).

Come rilevato sopra, 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 dai rivenditori che fanno 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 del DPF UE-USA, il Dipartimento può quindi esercitare i poteri conferitigli dall'articolo 41712 per farglieli rispettare. Pertanto, se la compagnia aerea o il rivenditore cui il passeggero comunica informazioni si è impegnato a rispettare i principi del DPF UE-USA, il venire meno a quest'impegno costituisce una violazione dell'articolo 41712.

B. Pratiche di applicazione

L'Ufficio per la protezione dei consumatori nel settore del trasporto aereo del Dipartimento ("OACP" o "Ufficio") ([2]) indaga sui casi e avvia azioni al riguardo a norma del codice degli Stati Uniti, 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 ed 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 ([3]).

Se non è conclusa una transazione adeguata e ragionevole, l'OACP ha il potere di avviare un procedimento coercitivo che comporta un incidente probatorio dinanzi a un giudice amministrativo del DOT, 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 37 377 USD per ciascuna violazione della medesima disposizione.

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'OACP 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 del DPF UE-USA. 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 DOT 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 DOT 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Precedentemente noto come Ufficio per l'applicazione della legge e i procedimenti nel trasposto aereo.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

Il DOT è parimenti responsabile, per quanto concerne le compagnie aeree, 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. 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 dei principi del DPF UE-USA**

Se riceve, contro una compagnia aerea o un rivenditore che fa servizio di biglietteria che ha scelto di aderire al DPF UE-USA, un reclamo per presunta violazione dei principi del regime, il Dipartimento lo fa rispettare attivamente e rigorosamente nel modo illustrato qui di seguito.

A. Priorità all'esame della presunta violazione

L'OACP del Dipartimento esamina ciascun reclamo presentato per presunta violazione dei principi del DPF UE-USA (compresi quelli ricevuti dalle autorità di protezione dei dati dell'UE) e, se la violazione è confermata da prove, avvia un'azione coercitiva.

L'OACP coopera inoltre con l'FTC e il Dipartimento del Commercio e conferisce prioritaria ai casi in cui un soggetto regolamentato è accusato di non rispettare gli impegni assunti nell'ambito del DPF UE-USA.

Ricevuta la segnalazione di una presunta violazione dei principi del regime, l'OACP 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 dei principi del DPF UE-USA 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 in relazione ai principi del DPF UE-USA.

B. Soluzione dei casi di millantata adesione al regime

Il Dipartimento resta impegnato a indagare sulle violazioni dei principi del DPF UE-USA, 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 DPF UE-USA 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 del DPF UE-USA, il fatto che l'organizzazione presenti l'autocertificazione o non la rinnovi 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.

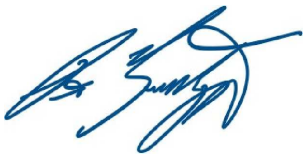
C. Controllo dell'esecuzione e pubblicazione dei provvedimenti coercitivi inerenti a violazioni dei principi del DPF UE-USA

L'OACP del Dipartimento resta parimenti impegnato a controllare l'esecuzione dei provvedimenti coercitivi per quanto necessario ad assicurare il rispetto dei principi del DPF UE-USA. Nello specifico, se emana un provvedimento che diffida la compagnia aerea o il rivenditore che fa servizio di biglietteria dal violare in futuro i principi del DPF UE-USA e l'articolo 41712, l'OACP controlla che questa disposizione inibitoria sia effettivamente rispettata. Provvede inoltre a mettere i provvedimenti emanati nei casi rientranti nei principi del DPF UE-USA a disposizione sul proprio sito web.

Il Dipartimento attende con interesse di continuare a lavorare sulle questioni inerenti al DPF UE-USA assieme ai partner federali e ai portatori di interessi dell'UE.

Nell'auspicare che queste informazioni risultino utili, resto a disposizione per qualsiasi domanda o ulteriore chiarimento.

La prego di accogliere, signor Commissario, i sensi della mia più alta stima.



Pete BUTTIGIEG

ALLEGATO VI

Dipartimento della Giustizia degli Stati Uniti d'America

Sezione penale

Ufficio del Procuratore generale aggiunto Washington, D.C. 20530

23 giugno 2023

Ana Gallego Torres
Direttrice generale della DG Giustizia e consumatori
Commissione europea
Rue Montoyer/Montoyerstraat 59
1049 Bruxelles
Belgio

Gentile Direttrice generale Gallego Torres,

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 scudo 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, 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 (sentenza 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

([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 (codice degli Stati Uniti, titolo 12, articolo 3414, titolo 15, articolo 1681u, titolo 15, articolo 1681v, titolo 18, articolo 2709, titolo 50, articolo 3162), e, per la sorveglianza elettronica, i mandati di perquisizione, i documenti aziendali e la raccolta di altre informazioni a norma della legge relativa alla vigilanza sull'intelligence esterna (codice degli Stati Uniti, titolo 50, articoli 1801 e seguenti).

([2]) La presente lettera verte sui poteri di applicazione della legge e di regolamentazione a livello federale: se la violazione riguarda la legge di uno Stato federato, le indagini sono effettuate dalle autorità di contrasto di 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 o le leggi dello Stato possono prevedere per la procedura giuridica tutele aggiuntive 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.

perquisizione, gli agenti delle autorità di applicazione della legge devono ottenere un mandato dal giudice (cfr. Katz/Stati Uniti, 389 U.S. 347, 357 (1967)). Le norme per l'emissione di un mandato, quali i requisiti relativi all'esistenza di motivi plausibili e alla specificità, si applicano ai mandati per perquisizioni fisiche e sequestri, nonché ai mandati per i contenuti memorizzati di comunicazioni elettroniche emesse ai sensi della *Stored Communications Act* (legge sulle comunicazioni archiviate), come illustrato di seguito. 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 ([3]).

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; 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 pertinenti in relazione alle 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.

Ordinanze di un organo giurisdizionale relative ai dispositivi di 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 dall'organo giurisdizionale competente, certificando che le informazioni sono d'interesse per un'indagine penale in corso, un'ordinanza 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, 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 (ECPA) - L'accesso del governo alle informazioni sugli abbonati, ai dati di traffico e all'archivio dei contenuti delle comunicazioni in possesso dei prestatori di servizi internet, delle società telefoniche e di altri terzi prestatori di servizi è disciplinato da ulteriori norme adottate ai sensi del titolo II dell'ECPA, ossia dalla legge sulle comunicazioni archiviate (SCA) (codice degli Stati Uniti, 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 prestatore di servizi internet. La SCA prevede livelli crescenti di tutela della privacy in funzione dell'intrusività della raccolta dati: per le informazioni

([3]) Per quanto concerne i principi del quarto emendamento sulla tutela della vita privata e degli interessi in materia di sicurezza di cui sopra, i giudici statunitensi applicano regolarmente tali principi ai nuovi tipi di strumenti investigativi di contrasto resi possibili dagli sviluppi tecnologici. Ad esempio nel 2018 la Corte suprema ha stabilito che l'acquisizione da parte di enti governativi, nel contesto di un'indagine di contrasto, di informazioni storiche sull'ubicazione dei siti a livello di cella da una società di telefonia mobile per un periodo di tempo prolungato costituisce una "ricerca" soggetta al requisito del mandato di cui al quarto emendamento (Carpenter/Stati Uniti, 138 S. Ct. 2206 (2018)).

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 ([4]).

Ordinanze di un organo giurisdizionale 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, titolo 18, articoli 2510-2523). L'esercizio di questo potere presuppone l'emissione di un'ordinanza di un organo giurisdizionale nella quale 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 — *Fed. R. Crim. P.* (norme federali di procedura penale), norma 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. Una persona soggetta a perquisizione o i cui beni sono soggetti a perquisizione può chiedere la cancellazione delle prove ottenute o derivate da una perquisizione illegale se tali prove vengono presentate contro tale persona durante un processo penale (cfr. Mapp/Ohio, 367 U.S. 643 (1961)). Quando il titolare dei dati è tenuto a divulgare dati in forza di un mandato, la parte obbligata può contestare l'obbligo di divulgazione in quanto indebitamente gravoso. Cfr. *In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979)* (nella quale si afferma che il giusto processo richiede un'audizione in merito alla questione dell'onerosità prima di obbligare una società telefonica a fornire assistenza in relazione a un mandato di perquisizione); *In re Application of United States, 616 F.2d 1122 (9th Cir. 1980)* (che giunge alla stessa conclusione sulla base dell'autorità di vigilanza dell'organo giurisdizionale).

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%28DIOG%29, 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 sulla giustizia (Justice Manual), anch'esso disponibile in rete all'indirizzo https://www.justice.gov/jm/justicemanualprevede ulteriori norme e politiche che limitano le attività investigative dei procuratori federali.

Poteri civili e regolamentari (interesse pubblico)

([4]) Inoltre l'articolo 2705, lettera b), della SCA autorizza il governo a ottenere un'ordinanza di un organo giurisdizionale, basata su una comprovata necessità di protezione dalla divulgazione, che vieti a un prestatore di servizi di comunicazione di notificare volontariamente ai propri utenti il ricevimento della notifica dell'avvio di un procedimento giudiziario ai sensi della SCA. Nell'ottobre 2017 il Procuratore generale aggiunto Rod Rosenstein ha pubblicato un memorandum indirizzato agli avvocati e agli agenti del Dipartimento della Giustizia contenente orientamenti destinati a garantire che le domande per l'ottenimento di provvedimenti cautelari siano adattate ai fatti e alle preoccupazioni specifiche di un'indagine e che fissa un termine massimo di un anno per il periodo per il quale una domanda può chiedere il posticipo della notifica. Nel maggio del 2022 il Procuratore generale aggiunto, Lisa Monaco, ha pubblicato orientamenti supplementari sull'argomento che, tra l'altro, hanno stabilito i requisiti interni di approvazione da parte del Dipartimento della Giustizia per le domande di proroga di un provvedimento cautelare oltre il termine iniziale di un anno e hanno imposto la cessazione dell'efficacia dei provvedimenti cautelari in concomitanza con la chiusura di un'indagine.

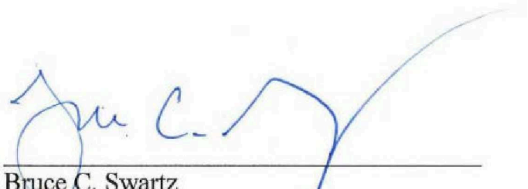
Riguardo all'accesso ai dati detenuti da imprese presenti negli Stati Uniti vigono limitazioni rilevanti anche sotto il profilo civile o regolamentare (ossia di "interesse pubblico"). Gli enti che hanno competenze civili o di regolamentazione possono citare le imprese ingiungendo loro di trasmettere 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. (norme federali in materia di procedura civile), norma 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 (codice degli Stati Uniti, titolo 31, articolo 5318; codice dei regolamenti federali, titolo 31, capitolo X), mentre un'altra società può invocare la legge sull'informativa corretta nel credito (codice degli Stati Uniti, 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, titolo 12, articoli 3401-3423). 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 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.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ALLEGATO VII

UFFICIO DEL DIRETTORE DELL'INTELLIGENCE NAZIONALE - UFFICIO LEGALE

WASHINGTON, DC 20511

9 dicembre 2022

Leslie B. Kiernan,
Giureconsulta
Dipartimento del
Commercio degli Stati Uniti, 1401 Constitution
Ave., NW Washington, DC 20230

Gentile signora Kiernan,

il 7 ottobre 2022 il presidente Biden ha firmato il decreto presidenziale 14086, *Enhancing Safeguards for United States Signals Intelligence Activities,* che rafforza la rigorosa serie di garanzie in materia di privacy e libertà civili che si applicano alle attività di intelligence dei segnali degli Stati Uniti. Tra queste figurano: obbligo di soddisfacimento da parte delle attività di intelligence dei segnali di obiettivi legittimi elencati; divieto esplicito di tali attività ai fini di specifici obiettivi vietati; messa in atto di procedure nuove per garantire che le attività di intelligence dei segnali perseguano tali obiettivi legittimi e non obiettivi vietati; obbligo di conduzione delle attività di intelligence dei segnali soltanto dopo aver accertato, sulla base di una valutazione ragionevole di tutti i fattori pertinenti, che tali attività sono necessarie per far progredire una priorità di intelligence convalidata e soltanto in misura e in modo proporzionati alla priorità di intelligence convalidata per la quale sono state autorizzate; e istruzione ai servizi della comunità dell'intelligence di aggiornare le loro politiche e procedure al fine di rispecchiare le garanzie richieste dal decreto presidenziale in materia di intelligence dei segnali. L'aspetto più rilevante consiste nel fatto che il decreto presidenziale introduce altresì un meccanismo indipendente e vincolante che consente alle persone provenienti da "Stati qualificati", designati ai sensi del decreto presidenziale stesso, di presentare ricorso qualora ritengano di essere state oggetto di attività illecite statunitensi di intelligence dei segnali, comprese le attività che violano le tutele previste da detto decreto presidenziale.

L'emanazione del decreto presidenziale 14086 da parte del presidente Biden ha segnato il culmine di ben oltre un anno di negoziati dettagliati tra i rappresentanti della Commissione europea e degli Stati Uniti e indica la direzione che le misure che gli Stati Uniti adotteranno per attuare gli impegni assunti nell'ambito del quadro UE-USA per la protezione dei dati personali. Coerentemente con lo spirito di cooperazione che ha prodotto tale quadro, ritengo che Lei abbia ricevuto due serie di domande da parte della Commissione europea sulle modalità di attuazione del decreto presidenziale da parte della comunità dell'intelligence. Sono lieto di rispondere a tali domande con la presente lettera.

Articolo 702 della legge relativa alla vigilanza sull'intelligence esterna del 1978 (articolo 702 FISA)

La prima serie di domande riguarda l'articolo 702 FISA, che consente l'acquisizione, assistita obbligatoriamente da prestatori di servizi di comunicazione elettronica, di informazioni di intelligence esterna ottenuta prendendo a obiettivo cittadini stranieri che si ritiene ragionevolmente siano situati al di fuori degli Stati Uniti. In particolare le domande formulate riguardano l'interazione tra tale disposizione e il decreto presidenziale 14086, nonché le altre garanzie che si applicano alle attività svolte ai sensi dell'articolo 702 FISA.

Innanzitutto, possiamo confermare che la comunità dell'intelligence applicherà le garanzie di cui al decreto presidenziale 14086 alle attività svolte ai sensi dell'articolo 702 FISA.

Numerose altre garanzie si applicano inoltre al ricorso, da parte del governo, all'articolo 702 FISA. Ad esempio tutte le certificazioni a norma dell'articolo 702 FISA devono essere firmate tanto dal Procuratore generale quanto dal direttore dell'intelligence nazionale (DNI), e il governo deve sottoporre tutte queste certificazioni all'approvazione della Corte di vigilanza sull'intelligence esterna (Corte FISA), costituita da giudici indipendenti, nominati a vita a svolgere la professione di giudice, che esercitano un mandato di sette anni non rinnovabile. Tali certificazioni individuano le categorie di informazioni di intelligence esterna da acquisire, che devono soddisfare la definizione, stabilita dalla legge, di informazioni di intelligence esterna, prendendo a obiettivo persone straniere che si ritiene ragionevolmente si trovino al di fuori degli Stati Uniti. Tali certificazioni hanno incluso informazioni relative al terrorismo internazionale e ad altri temi, quali l'acquisizione di informazioni in merito ad armi di distruzione di massa. Ogni certificazione annuale deve essere presentata alla Corte FISA per approvazione in un fascicolo di domanda di certificazione che comprenda le certificazioni del Procuratore generale e del direttore dell'intelligence nazionale, le dichiarazioni giurate rilasciate da determinati capi degli enti di intelligence, le procedure di individuazione degli obiettivi, le procedure di minimizzazione e le procedure di interrogazione che sono vincolanti per il governo. Le procedure di individuazione degli obiettivi richiedono tra l'altro che la comunità dell'intelligence valuti ragionevolmente, sulla base di tutte le circostanze del caso, che l'attività di individuazione degli obiettivi porterà probabilmente alla raccolta di informazioni di intelligence esterna individuate in una certificazione a norma dell'articolo 702 PISA.

Inoltre, nel raccogliere informazioni ai sensi dell'articolo 702 FISA, la comunità dell'intelligence deve: fornire una spiegazione scritta della base della sua valutazione, al momento dell'individuazione degli obiettivi, del fatto che si ritiene che gli obiettivi in questione dovrebbero possedere, ricevere o è probabile che comunichino informazioni di intelligence esterna individuate in una certificazione a norma dell'articolo 702 PISA; confermare che la norma di individuazione degli obiettivi di cui all'articolo 702 della PISA continua ad essere soddisfatta; e cessare la raccolta nel momento in cui tale norma non è più soddisfatta. *Cfr.* comunicazione del governo degli Stati Uniti alla Corte di vigilanza sull'intelligence esterna, *2015 Summary of Notable Section 702 Requirements*, pagg. 2-3 (15 luglio 2015).

Richiedere alla comunità dell'intelligence di registrare per iscritto e confermare regolarmente la validità della sua valutazione secondo cui gli obiettivi di cui all'articolo 702 FISA rispettano le norme applicabili in materia di individuazione degli obiettivi facilita la supervisione da parte della Corte FISA delle attività di individuazione degli obiettivi svolte dalla comunità dell'intelligence. Ogni valutazione e spiegazione registrate della logica alla base dell'individuazione degli obiettivi è esaminata ogni due mesi dagli avvocati incaricati della vigilanza sull'intelligence presso il Dipartimento della Giustizia che svolgono tale funzione di vigilanza in modo indipendente rispetto alle operazioni di intelligence esterna. La sezione del Dipartimento della Giustizia che svolge tale funzione è quindi competente, a sensi di una norma consolidata da tempo della Corte FISA, di segnalare a tale Corte eventuali violazioni delle procedure applicabili. Tale attività di segnalazione, unitamente alle riunioni periodiche tra la Corte FISA e detta sezione del Dipartimento della Giustizia in merito alla vigilanza sulle attività di individuazione degli obiettivi a norma dell'articolo 702 FISA, consente alla Corte FISA di garantire il rispetto dell'articolo 702 FISA e di altre procedure, nonché di assicurare altrimenti la liceità delle attività svolte dal governo. In particolare la Corte FISA può procedere in tal senso in svariati modi, anche adottando decisioni correttive vincolanti volte a porre fine alle attività di raccolta dell'autorità governativa nei confronti di un determinato obiettivo o a modificare o ritardare la raccolta dei dati a norma dell'articolo 702 FISA. La Corte FISA può altresì richiedere al governo di fornire ulteriori relazioni o informazioni sulla sua conformità rispetto alle attività di individuazione degli obiettivi e ad altre procedure oppure richiedere modifiche a tali procedure.

Raccolta "in blocco" dell'intelligence dei segnali

La seconda serie di domande riguarda la raccolta "in blocco" di dati attuata dall'intelligence dei segnali, definita dal decreto presidenziale 14086 come la raccolta autorizzata di grandi quantità di dati di intelligence dei segnali che, in base a considerazioni tecniche od operative, è effettuata senza il filtro delle discriminanti (identificatori o selettori specifici).

Per quanto concerne tali questioni, sottolineiamo innanzitutto che né la FISA né le *National Security Letter* autorizzano la raccolta in blocco. Per quanto concerne la FISA:

— a norma dei titoli I e III FISA, che autorizzano rispettivamente la sorveglianza elettronica e le perquisizioni fisiche, sono necessari (con eccezioni limitate, quali situazioni d'emergenza) un'ordinanza di un organo giurisdizionale e sempre un motivo plausibile per ritenere che l'obiettivo della raccolta dati sia una potenza straniera o l'agente di una potenza straniera (*cfr.* codice degli Stati Uniti, titolo 50, articoli 1805 e 1824);

— la legge USA FREEDOM del 2015 ha modificato il titolo IV FISA, che autorizza l'uso di dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita, conformemente a un'ordinanza di un organo giurisdizionale (tranne in situazioni di emergenza), al fine di imporre al governo di basare le richieste su un "selettore specifico" (*cfr.* codice degli Stati Uniti, titolo 50, articolo 1842, lettera c), punto 3);

— a norma del titolo V FISA, che consente al *Federal Bureau of Investigation* (FBI) di ottenere determinati tipi di documenti aziendali, è necessaria un'ordinanza di un organo giurisdizionale basata su una domanda che specifica che sussistono fatti specifici e circostanziabili che inducono a ritenere che la persona a cui i documenti si riferiscono sia una potenza straniera o l'agente di una potenza straniera (*cfr.* codice degli Stati Uniti, titolo 50, articolo 1862, lettera b), punto 2), lettera B)) ([1]);

— infine l'articolo 702 FISA autorizza 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 (*cfr.* codice degli Stati Uniti, titolo 50, articolo 188la, lettera a)). Pertanto, come ha osservato l'Autorità per la tutela della vita privata e delle libertà civili (PCLOB), la raccolta di dati da parte del governo ai sensi dell'articolo 702 FISA consiste interamente nel prendere a obiettivo singole persone e nell'acquisire comunicazioni associate a tali persone, dalle quali il governo ha motivo di aspettarsi di ottenere determinati tipi di intelligence straniera, affinché il programma non operi raccogliendo comunicazioni in massa. 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,* pag. 103 (2 luglio 2014) ([2]).

Per quanto concerne le National Security Letter, la legge USA FREEDOM del 2015 impone l'obbligo di disporre di un "selettore specifico" per ricorrere a tali lettere. (*cfr.* codice degli Stati Uniti, titolo 12, articolo 3414, lettera a), punto 2); titolo 15, articolo 1681u; titolo 15, articolo 1681v, lettera a); titolo 18, articolo 2709, lettera b)).

Inoltre il decreto presidenziale 14086 stabilisce che va accordata la priorità alla raccolta mirata e che, quando la comunità dell'intelligence effettua una raccolta in blocco, la raccolta in blocco dell'intelligence dei segnali è autorizzata soltanto sulla base della constatazione che l'informazione necessaria per far progredire una priorità convalidata dell'intelligence non può ragionevolmente essere ottenuta mediante una raccolta mirata (*cfr.* decreto presidenziale 14086, articolo 2, lettera c), punto ii). lettera A)).

Inoltre, se la comunità dell'intelligence stabilisce che la raccolta in blocco soddisfa dette norme, il decreto presidenziale 14086 prevede ulteriori garanzie. Nello specifico il decreto presidenziale impone alla comunità dell'intelligence, quando effettua una raccolta in blocco, di applicare metodi e misure tecniche ragionevoli al fine di limitare i dati raccolti soltanto a quanto necessario per far progredire una priorità convalidata dell'intelligence, riducendo al minimo la raccolta di informazioni non pertinenti (*cfr. ibidem*). Il decreto stabilisce inoltre che le attività di intelligence dei segnali, che comprendono interrogazioni dell'intelligence dei segnali ottenuta mediante raccolta in blocco, devono essere condotte soltanto dopo aver accertato, sulla base di una valutazione ragionevole di tutti i fattori pertinenti, che le attività sono necessarie per far progredire una priorità convalidata dell'intelligence (*cfr. ibidem,* articolo 2, lettera a), punto ii), lettera A)). Il decreto attua inoltre tale principio stabilendo che la comunità dell'intelligence può interrogare l'intelligence dei segnali non soggetta a minimizzazione, ottenuta mediante raccolta in blocco, nel perseguimento di sei obiettivi ammissibili e che tali interrogazioni devono essere condotte secondo politiche e procedure che tengano adeguatamente conto dell'impatto delle interrogazioni sulla vita privata e sulle libertà civili di tutte le persone, indipendentemente dalla loro cittadinanza o dal luogo in cui possono risiedere (*cfr. ibidem,* articolo 2, lettera c), punto iii), lettera D)). Infine il decreto prevede la gestione, la sicurezza e il controllo degli accessi in relazione ai dati raccolti (*cfr. ibidem,* articolo 2, lettera c), punto iii), lettere A) e B)).

* * * * *

Ci auguriamo che tali chiarimenti siano utili. Non esiti a contattarci in caso di ulteriori domande in merito alle modalità che la comunità dell'intelligence statunitense intende adottare ai fini dell'attuazione del decreto presidenziale 14086.

([1]) Dal 2001 al 2020, il titolo V FISA ha consentito all'FBI di chiedere alla Corte FISA l'autorizzazione ad ottenere "elementi tangibili" pertinenti per talune indagini autorizzate (*cfr.* legge USA PATRIOT, Pub. L. No. 107-56, 115 Stat. 272, articolo 215 (2001)). Tale formulazione, che è stata abbandonata e non costituisce pertanto più il testo della legge, ha fornito l'autorità in virtù della quale il governo ha raccolto in blocco metadati telefonici. Anche prima dell'abbandono di questa disposizione, tuttavia, la legge USA FREEDOM l'aveva modificata al fine di imporre al governo di basare una richiesta alla Corte FISA su un "selettore specifico" (*cfr.* legge USA FREEDOM, Pub. L. No. 114-23, 129 Stat. 268, articolo I 03 (2015)).

([2]) Gli articoli 703 e 704, che autorizzano la comunità dell'intelligence a prendere a obiettivo persone statunitensi situate all'estero, impongono l'ottenimento di un'ordinanza di un organo giurisdizionale (fatta eccezione in situazioni di emergenza) e richiedono sempre un motivo plausibile per ritenere che l'obiettivo sia una potenza straniera, un agente di una potenza straniera o un funzionario o dipendente di una potenza straniera (*cfr.* codice degli Stati Uniti, titolo 50, articoli 1881b e 1881c).

Sincerely,

Christopher C. FONZONE,
Giureconsulto

ALLEGATO VIII

Elenco delle abbreviazioni

Nella presente decisione figurano le seguenti abbreviazioni:

AAA	American Arbitration Association (associazione americana per l'arbitrato)
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations (orientamenti del Procuratore generale per le operazioni dell'FBI all'interno degli USA)
APA	Administrative Procedure Act (legge sulle procedure amministrative)
CIA	Central Intelligence Agency (agenzia centrale per l'intelligence)
CLPO ODNI	Civil Liberties Protection Officer of the Director of National Intelligence (addetto alla tutela della vita privata e alle libertà civili dell'Ufficio del direttore dell'intelligence nazionale)
CNSS	Committee on National Security Systems (comitato sui sistemi di sicurezza nazionale)
collegio del DPF UE-USA	collegio del quadro UE-USA per la protezione dei dati personali
Corte di giustizia	Corte di giustizia dell'Unione europea
Corte FISA	Foreign Intelligence Surveillance Court (Corte di vigilanza sull'intelligence esterna)
decisione	decisione di esecuzione della Commissione a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali
decreto presidenziale 12333	decreto presidenziale 12333 "United States Intelligence Activities"
decreto presidenziale 14086,	decreto presidenziale 14086 "Enhancing Safeguards for US Signals Intelligence Activities"
DHS	Department of Homeland Security (Dipartimento della Sicurezza interna)
DNI	Director of National Intelligence (direttore dell'intelligence nazionale)
DOT	U.S. Department of Transportation (Dipartimento dei Trasporti degli USA)
DPF UE-USA o DPF	EU-U.S. Data Privacy Framework (quadro UE-USA per la protezione dei dati personali)
DPRC	Data Protection Review Court (Tribunale del riesame in materia di protezione dei dati)
ECOA	Equal Credit Opportunity Act (legge sulle pari opportunità nel credito)
ECPA	Electronic Communications Privacy Act (legge sulla privacy nelle comunicazioni elettroniche)
elenco degli aderenti al DPF	elenco degli aderenti al quadro per la protezione dei dati personali
FBI	Federal Bureau of Investigation (Ufficio federale investigativo)
FCRA	Fair Credit Reporting Act (legge sull'informativa corretta nel credito)
FISA	Foreign Intelligence Surveillance Act (legge relativa alla vigilanza sull'intelligence esterna)
FISCR	Foreign Intelligence Surveillance Court of Review (Corte di controllo della vigilanza sull'intelligence esterna)
FOIA	Freedom of Information Act (legge sulla libertà di informazione)
FRA	Federal Records Act (legge federale sulle registrazioni)
FTC	U.S. Federal Trade Commission (Commissione federale per il commercio degli USA)
HIPAA	Health Insurance Portability and Accountability Act (legge sulla portabilità e responsabilità dell'assicurazione sanitaria)
ICDR	International Centre for Dispute Resolution (Centro internazionale per la composizione delle controversie)
IOB	Intelligence Oversight Board (Autorità di vigilanza sull'intelligence)

NIST	National Institute of Standards and Technology (Istituto nazionale per le norme e la tecnologia)
NSA	National Security Agency (Agenzia per la sicurezza nazionale)
NSL	National Security Letter (lettera di sicurezza nazionale)
ODNI	Office of the Director of National Intelligence (Ufficio del direttore dell'intelligence nazionale)
OMB	Office of Management and Budget (Ufficio per la gestione e il bilancio)
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (Ufficio per la tutela della vita privata e le libertà civili del Dipartimento di giustizia)
PCLOB	Privacy and Civil Liberties Oversight Board (Autorità per la tutela della vita privata e delle libertà civili)
PIAB	President's Intelligence Advisory Board (Comitato presidenziale consultivo sull'intelligence)
PPD 28	Presidential Policy Directive 28 (direttiva presidenziale 28)
principi	principi del quadro UE-USA per la protezione dei dati personali
regolamento (UR) 2016/679	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)
regolamento del Procuratore generale	Attorney General Regulation on the Data Protection Review Court (regolamento sul "Data Protection Review Court" emesso dal Procuratore generale degli Stati Uniti)
SAOP	Senior Agency Official for Privacy (funzionario senior dell'ente competente per la tutela della vita privata)
SEE	Spazio economico europeo
Unione	Unione europea
USA	Stati Uniti d'America