Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Office fédéral de la justice **UFG**
Domaine de direction Droit public
Unité Projets législatifs I

30 aprile 2024

Valutazione dell'adeguatezza – Stati Uniti

Istituzione di un quadro per il trasferimento di dati personali dalla Svizzera alle organizzazioni certificate negli Stati Uniti (*Swiss-U.S. data privacy framework*) – valutazione dell'adeguatezza del livello di protezione dei dati personali

BJ-D-72B33401/379

Indice

1 Situazione iniziale

1.1 Sistema di valutazione dell'adeguatezza introdotto dalla legge del 25 settembre 2020 sulla protezione dei dati

Il nuovo diritto in materia di protezione dei dati, in vigore dal 1° settembre 2023, ha introdotto un cambio di competenza: secondo l'articolo 16 capoverso 1 della legge del 25 settembre 2020[1] sulla protezione dei dati (LPD) e l'articolo 8 capoverso 1 dell'ordinanza del 31 agosto 2022[2] sulla protezione dei dati (OPDa), spetta al Consiglio federale determinare se uno Stato, un territorio, un determinato settore di uno Stato o un organismo internazionale garantisce una protezione adeguata dei dati. L'allegato 1 OPDa elenca gli Stati, i territori, determinati settori di uno Stato e gli organismi internazionali che offrono una protezione adeguata.

Compete comunque all'Ufficio federale di giustizia[3] valutare, sotto il profilo giuridico, l'adeguatezza della protezione dei dati. La valutazione viene pubblicata.

1.2 Quadro previgente

Conformemente alla legge del 19 giugno 1992 sulla protezione dei dati (non più in vigore), l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) teneva un elenco indicativo degli Stati che garantivano una protezione adeguata dei dati.

L'11 gennaio 2017, l'IFPDT vi aveva aggiunto gli Stati Uniti per lo scambio di dati con le aziende certificate secondo i principi dello scudo per la privacy tra Svizzera e Stati Uniti (*Swiss-U.S. privacy shield*), un quadro pressoché identico a quello istituito tra UE e Stati Uniti.

Il 16 luglio 2020, tuttavia, nella sentenza sul caso Schrems II (causa C-311/18), la Corte di giustizia dell'Unione europea (CGUE) ha invalidato il meccanismo di trasferimento di dati personali dall'UE agli Stati Uniti dichiarando insufficiente la protezione che offriva: il meccanismo ammetteva infatti deroghe sproporzionate alla protezione dei dati per le attività di sorveglianza dei servizi di intelligence statunitensi e non offriva agli interessati rimedi giuridici adeguati.

Anche se la decisione della CGUE non è vincolante per la Svizzera, l'IFPDT ha ritenuto comunque necessario valutare se escludere gli Stati Uniti dall'elenco indicativo degli Stati che garantiscono un livello di protezione adeguato, e questo in considerazione del principio generale dello Stato di diritto, della necessità di garantire la certezza del diritto e del fatto che il quadro per lo scambio di dati personali tra l'UE e gli Stati Uniti era praticamente uguale a quello tra la Svizzera e gli Stati Uniti. Nel suo parere dell'8 settembre 2020, l'IFPDT è giunto alla conclusione che gli Stati Uniti non soddisfacevano più i requisiti per garantire una protezione adeguata dei dati ai sensi della legge in materia, ragion per cui ha deciso di

---

1 RS **235.1**

2 RS **235.11**

3 In collaborazione con altri uffici competenti conformemente all'art. 7 cpv. 1 lett. d dell'ordinanza sull'organizzazione del Dipartimento federale di giustizia e polizia (Org-DFGP; RS **172.213.1**).

escluderli dall’elenco. Di conseguenza, il Consiglio federale non ha inserito gli Stati Uniti nell’elenco dell’allegato 1 OPDa al momento dell’entrata in vigore del nuovo diritto in materia di protezione dei dati il 1° settembre 2023.

1.3 Istituzione di un quadro per il trasferimento di dati personali dalla Svizzera alle organizzazioni certificate negli Stati Uniti

In seguito alla loro esclusione dall’elenco dell’IFPDT, gli Stati Uniti hanno intrattenuto colloqui anche con la Svizzera, oltre che con l’UE.

Questo dialogo tra i due Paesi ha portato all’istituzione di un quadro commerciale per le organizzazioni certificate (costituito dai principi, compresi quelli supplementari, del quadro per la protezione dei dati tra la Svizzera e gli Stati Uniti), alla pubblicazione di vari documenti da parte del governo e delle autorità statunitensi competenti (decreto presidenziale 14086 del 7 ottobre 2022, regolamento sul Tribunale del riesame in materia di protezione dei dati emanato dal Procuratore generale degli Stati Uniti il 7 ottobre 2022, direttiva 126 della comunità dell’intelligence emanata il 6 dicembre 2022 dalla direzione dell’intelligence nazionale), alla designazione della Svizzera il 7 giugno 2024 come Stato che beneficia del meccanismo di ricorso a due livelli – compreso l’accesso al Tribunale del riesame in materia di protezione dei dati –, nonché alla consegna delle lettere delle autorità statunitensi che confermano gli impegni assunti. Tutti questi documenti[4], consultabili ai link indicati nell’ultima pagina, costituiscono il quadro per il trasferimento di dati personali dalla Svizzera alle organizzazioni certificate negli Stati Uniti (*Swiss-U.S. data privacy framework,* di seguito: DPF CH-USA).

La seguente valutazione ha lo scopo di stabilire se gli Stati Uniti garantiscono un livello di protezione adeguato per il trasferimento di dati personali tra i titolari o i responsabili del trattamento in Svizzera e le organizzazioni certificate negli Stati Uniti, sulla base dei criteri di valutazione stabiliti nell’OPDa.

2 Criteri di valutazione dell’adeguatezza

L’articolo 8 OPDa stabilisce i criteri da prendere in considerazione nel valutare l’adeguatezza, segnatamente:

a) gli impegni internazionali dello Stato o dell’organismo internazionale, in particolare nel settore della protezione dei dati;
b) lo Stato di diritto e il rispetto dei diritti dell’uomo;
c) la legislazione vigente in particolare in materia di protezione dei dati, la sua attuazione e la giurisprudenza pertinente;
d) l’effettiva garanzia dei diritti delle persone interessate e della tutela giurisdizionale;
e) l’effettivo funzionamento di una o più autorità indipendenti responsabili della protezione dei dati nello Stato in questione o alle quali è assoggettato un organismo internazionale e dotate di poteri e competenze sufficienti.

[4] Disponibili soltanto in lingua inglese.

L'allegato 1 OPDa contiene l'elenco di Stati, territori, determinati settori di uno Stato e organismi internazionali che garantiscono una protezione adeguata dei dati. Tale elenco è vincolante.

Per protezione adeguata s'intende una protezione sostanzialmente equivalente a quella garantita dal diritto svizzero in materia di protezione dei dati. Non si tratta di confrontare punto per punto i sistemi, bensì di determinare se, nel complesso, il sistema di uno Stato, un territorio, un determinato settore di uno Stato o un organismo internazionale offre un livello di protezione sostanzialmente equivalente a quello svizzero per quanto riguarda le disposizioni sulla protezione dei dati, la loro attuazione e i meccanismi di controllo impiegati. In questo contesto, occorre tenere conto delle differenti tradizioni giuridiche e culturali tra la Svizzera e uno Stato, un territorio, un determinato settore di uno Stato o un organismo internazionale oggetto di una valutazione di adeguatezza.

L'UE applica criteri simili nel valutare l'adeguatezza del livello di protezione dei dati personali in Stati terzi (cfr. art. 45 del regolamento generale sulla protezione dei dati[5]).

3 Quadro commerciale per il trasferimento di dati personali tra i titolari o i responsabili del trattamento in Svizzera e le organizzazioni certificate negli Stati Uniti

3.1 Legislazione applicabile

3.1.1 Principi del quadro

I principi, compresi quelli supplementari, del quadro per il trasferimento di dati personali dalla Svizzera alle organizzazioni certificate negli Stati Uniti (di seguito: principi DPF CH-USA o principi)[6] si basano su un sistema di certificazione secondo il quale le organizzazioni degli Stati Uniti (ovvero le aziende) che desiderano beneficiare di tale quadro si impegnano a rispettare una serie di principi in materia di protezione dei dati. Per poter essere certificata in base al DPF CH-USA, un'organizzazione dev'essere soggetta ai poteri di indagine ed esecuzione della Commissione federale del commercio (*Federal Trade Commission*) o del Dipartimento dei trasporti (*Department of transportation*), nonché certificare ogni anno la sua adesione ai principi del quadro.

Secondo tali principi, per dati personali s'intendono quelli riguardanti una persona identificata o identificabile, e rientranti nel campo di applicazione della LPD e delle sue ordinanze, che un'organizzazione negli Stati Uniti riceve dalla Svizzera e registra in qualsiasi forma. Analogamente, la nozione di trattamento è definita come qualsiasi operazione o insieme di operazioni compiute sui dati personali, con o senza l'ausilio di processi automatizzati, 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

---

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), GU L 119 del 4.5.2016, pag. 1, consultabile qui EUR-Lex - 32016R0679 - IT - EUR-Lex (europa.eu).

[6] Cfr. link ai documenti di riferimento alla fine del presente rapporto.

cancellazione o la distruzione. Questi due importanti concetti sono quindi definiti come nel diritto svizzero.

I principi DPF CH-USA garantiscono il rispetto dei principi fondamentali previsti dal diritto svizzero in materia di protezione dei dati (art. 6 LPD).

I dati personali devono essere trattati in modo lecito e proporzionato, possono essere raccolti soltanto per uno scopo determinato ed essere trattati ulteriormente soltanto in modo compatibile con tale scopo. Nel DPF CH-USA ciò è garantito sostanzialmente dal principio dell’integrità dei dati e della limitazione dello scopo (*Data Integrity and Purpose Limitation Principle*), ma anche da quello della scelta (*Choice Principle*): un’organizzazione deve dare all’interessato la possibilità di decidere se i suoi dati personali possono essere divulgati a terzi o utilizzati per uno scopo che differisce in modo significativo da quello per cui sono stati inizialmente raccolti o successivamente autorizzati.

I dati personali devono essere esatti e trattati in modo proporzionato agli scopi perseguiti; inoltre, non possono essere conservati più a lungo di quanto necessario per conseguire gli scopi per cui sono stati raccolti. Nel DPF CH-USA ciò è garantito dal principio dell’integrità dei dati e della limitazione dello scopo nonché da quello della scelta.

La sicurezza dei dati deve essere garantita: i titolari e i responsabili del trattamento devono adottare misure di sicurezza ragionevoli e adeguate in considerazione dei rischi associati al trattamento dei dati e del tipo di dati trattati. Nel DPF CH-USA questo è garantito dal principio della sicurezza (*Security Principle*).

In base al principio della trasparenza, le organizzazioni sono tenute a informare gli interessati in merito ai principali aspetti del trattamento dei loro dati personali, in particolare in merito all’adesione al DPF CH-USA, al tipo di dati raccolti, allo scopo del trattamento, ai loro diritti e ai mezzi di ricorso disponibili. Nel DPF CH-USA ciò è garantito dal principio dell’informativa (*Notice Principle*). Le organizzazioni devono rendere pubbliche le loro norme in materia di protezione dei dati ispirate ai principi DPF CH-USA.

Gli interessati dispongono di determinati diritti azionabili nei confronti del titolare o del responsabile del trattamento, in particolare il diritto di accesso ai dati, quello di opporsi al loro trattamento e quello di farli rettificare e cancellare. Gli interessati hanno in particolare il diritto di ottenere, senza doversi giustificare, la conferma che una determinata organizzazione sta trattando i loro dati personali e di richiedere i dati in questione nonché informazioni sullo scopo del trattamento, sulle categorie di dati personali trattati e sui destinatari cui sono comunicati i dati. Questo diritto di accesso può essere limitato solo in circostanze eccezionali analoghe a quelle previste dal diritto svizzero in materia di protezione dei dati, ad esempio se interessi preponderanti di un terzo lo esigono. Inoltre gli interessati hanno il diritto di ottenere la rettifica di dati inesatti e la cancellazione dei dati trattati in violazione dei principi. Nel DPF CH-USA ciò è garantito dal principio dell’accesso (*Access Principle, Supplementary Principle on Access*).

Al trasferimento successivo di dati personali tra un’organizzazione certificata e un terzo titolare o responsabile del trattamento si applicano norme specifiche conformemente al principio della responsabilità per il trasferimento successivo (*Accountability for Onward Transfer Principle*): i dati possono essere trasferiti successivamente soltanto per scopi limitati e specifici, sulla base di un contratto e unicamente se tale contratto impone al terzo destinatario dei dati di fornire il medesimo livello di protezione garantito dai principi.

In virtù del principio di ricorso, applicazione e responsabilità (*Recourse, Enforcement and Liability Principle*), le organizzazioni certificate devono prevedere meccanismi efficaci per garantire il rispetto dei principi e adottare misure atte a verificare che la loro politica sulla protezione dei dati adempia ai principi e venga effettivamente rispettata. Allo scopo, possono predisporre un sistema di autovalutazione oppure controlli esterni della conformità.

Ai dati degni di particolare protezione ai sensi del diritto svizzero si applicano garanzie specifiche: le organizzazioni devono ottenere il consenso esplicito degli interessati (*opt-in*) per poter divulgare i loro dati a terzi o utilizzarli per scopi diversi da quelli inizialmente previsti o successivamente autorizzati dagli interessati stessi in virtù del loro diritto di scelta. Tale consenso non è tuttavia necessario in determinate circostanze, paragonabili alle deroghe previste dal diritto svizzero, ad esempio se interessi preponderanti di un terzo lo esigono. Nel caso del DPF CH-USA ciò è garantito dal principio della scelta e da quello supplementare sui dati sensibili (*Supplementary Principle on Sensitive Data*).

3.1.2 Campo d'applicazione

Il quadro commerciale si applica ai dati personali[7] trasferiti dalla Svizzera a organizzazioni statunitensi che hanno certificato la loro adesione ai principi (v. n. 3.1.1 sopra).

Si applica alle organizzazioni statunitensi qualificate come titolari del trattamento ai sensi dell'articolo 5 lettera j LPD o come responsabili del trattamento ai sensi dell'articolo 5 lettera k LPD. I responsabili del trattamento devono impegnarsi per contratto ad agire solo su istruzioni del titolare del trattamento in Svizzera e ad assistere quest'ultimo nel rispondere a chi esercita i propri diritti secondo i principi.

3.2 Garanzie, autorità indipendente, rimedi giuridici

3.2.1 Amministrazione, certificazione e vigilanza

Il quadro commerciale è amministrato dal Dipartimento del commercio degli Stati Uniti (di seguito: Dipartimento del commercio).

Per autocertificarsi o chiedere il rinnovo (annuale) di un'autocertificazione esistente in virtù del DPF CH-USA, le organizzazioni sono tenute a dichiarare pubblicamente il loro impegno a rispettare i principi, a rendere disponibili le loro politiche in materia di protezione dei dati e ad attuarle pienamente. Devono anche informare il Dipartimento del commercio in particolare in merito agli scopi per i quali verranno trattati i dati personali, al pertinente meccanismo di ricorso indipendente e all'organo statutario incaricato di garantire il rispetto dei principi. Le organizzazioni che si autocertificano per la prima volta possono fare pubblicamente riferimento alla loro adesione ai principi solo dopo che il Dipartimento del commercio le avrà inserite nell'elenco degli aderenti da lui pubblicato e aggiornato.

Il Dipartimento del commercio esercita anche una funzione di vigilanza. Al fine di garantire una corretta applicazione del DPF CH-USA, pubblicherà, tenendolo aggiornato, l'elenco delle organizzazioni che si sono autocertificate presso il Dipartimento e hanno dichiarato il loro

[7] È fatta eccezione per i dati raccolti per la pubblicazione, la divulgazione o altre forme di comunicazione pubblica di materiale giornalistico e per le informazioni contenute in materiale già pubblicato e divulgato da archivi mediatici.

impegno ad aderire ai principi, e terrà un registro delle organizzazioni rimosse dall'elenco, indicando per ciascuna il motivo dell'esclusione. Depennerà dall'elenco le organizzazioni che abbandonano volontariamente il DPF CH-USA o che non rinnovano l'autocertificazione annuale. Queste organizzazioni devono continuare ad applicare i principi ai dati personali ricevuti nell'ambito del DPF CH-USA e dichiarare ogni anno al Dipartimento del commercio il loro impegno in tal senso (per tutto il tempo in cui conserveranno tali dati) oppure garantire una protezione adeguata dei dati personali con un altro mezzo autorizzato (p. es. un contratto che integri totalmente le clausole tipo approvate, stabilite o riconosciute dall'IFPDT) o ancora restituire o cancellare i dati. Il Dipartimento del commercio depennerà dall'elenco anche le organizzazioni che non hanno sistematicamente rispettato i principi e che dovranno quindi restituire o cancellare i dati personali ricevuti nell'ambito del DPF CH-USA.

Il Dipartimento del commercio è chiamato a verificare se le organizzazioni soddisfano i requisiti di certificazione, in particolare se continuano a rispettare i principi. Allo scopo effettuerà controlli a campione di organizzazioni selezionate a caso e di organizzazioni specifiche che presentino potenziali problemi, in particolare se riceve reclami o se l'organizzazione non risponde in modo soddisfacente alle richieste di informazioni. In alcuni casi, l'organizzazione può essere deferita all'autorità competente per l'adozione di eventuali misure coercitive.

Il Dipartimento del commercio effettuerà controlli per assicurare che nessuna organizzazione, in particolare quelle depennate dall'elenco, dichiari il falso in merito alla propria adesione ai principi. In determinati casi, potrà deferire il caso all'autorità competente per l'adozione di eventuali misure coercitive.

3.2.2 Garanzia dell'applicazione del quadro

Per poter aderire al quadro, le organizzazioni devono essere soggette alla giurisdizione di una delle seguenti autorità statunitensi, la Commissione federale del commercio o il Dipartimento dei trasporti, entrambe dotate dei necessari poteri d'indagine e di esecuzione per garantire il rispetto dei principi[8].

La Commissione federale del commercio è composta da cinque commissari nominati dal presidente degli Stati Uniti e in seguito confermati dal Senato. I commissari, che durante il loro mandato di sette anni non possono assumere altre attività o altri impieghi, possono essere revocati dal presidente unicamente per giusta causa. La Commissione ha il compito di proteggere il pubblico da pratiche commerciali ingannevoli o sleali e da metodi di concorrenza sleale. Può indagare sul rispetto dei principi così come sulle false dichiarazioni in merito all'adesione al quadro commerciale. Inoltre può chiedere decisioni amministrative o decisioni giudiziarie federali nei confronti di determinate organizzazioni e verificarne il rispetto obbligando le organizzazioni in questione a fornire i documenti necessari; infine può adire le vie legali per far rispettare le decisioni in caso di trasgressioni.

Il Dipartimento dei trasporti ha la competenza esclusiva per disciplinare le pratiche a protezione dei dati applicate dalle compagnie aeree; condivide invece con la Commissione federale del commercio la competenza per le pratiche a protezione dei dati nella vendita di

[8] Cfr. le lettere della Commissione e del Dipartimento accessibili tramite il link corrispondente alla fine del documento.

servizi di trasporto aereo ad opera delle agenzie di viaggio. In caso di controversie, il Dipartimento dei trasporti può chiedere a un giudice amministrativo indipendente e imparziale del Dipartimento o a un tribunale statunitense di obbligare la ditta a cessare le pratiche imputate o ad astenersene, oppure di infliggere sanzioni civili[9]. Il Dipartimento dei trasporti si è impegnato a dare la priorità alle indagini sulle presunte violazioni dei principi, ad adottare le opportune misure nei casi di falsa dichiarazione in merito all'adesione al quadro commerciale e a monitorare le relative decisioni d'esecuzione nonché a garantirne la pubblicazione.

Alla luce di quanto sopra, la Commissione federale del commercio e il Dipartimento dei trasporti possono essere considerate autorità di controllo indipendenti con poteri e competenze sufficienti a garantire un livello adeguato di protezione dei dati personali.

3.2.3 Rimedi giuridici

Nell'ambito della loro certificazione, le organizzazioni devono adempiere al principio di ricorso, applicazione e responsabilità (v. n. 3.1.1) prevedendo meccanismi di ricorso indipendenti, effettivi e facilmente accessibili, atti a consentire di dirimere, in modo rapido e senza costi per l'interessato, qualsiasi controversia insorta.

Le organizzazioni possono scegliere meccanismi di ricorso indipendenti in Svizzera o negli Stati Uniti e optare per programmi di protezione dei dati sviluppati dal settore privato e racchiudenti i principi; in alternativa possono optare per un'autorità di controllo tra quelle previste dal loro statuto o dalla legge che trattano singoli reclami e dirimono controversie oppure scegliere di impegnarsi a collaborare con l'IFPDT.

Gli interessati possono presentare un reclamo direttamente all'organizzazione, a un organo indipendente di risoluzione delle controversie da questa designato o all'IFPDT. Il Dipartimento del commercio rinvierà le organizzazioni non in grado di dirimere una controversia alla Commissione federale del commercio e al Dipartimento dei trasporti, i quali daranno priorità ai casi di non conformità segnalati dal Dipartimento del commercio e dall'IFPDT. Gli interessati possono presentare un reclamo direttamente alla Commissione federale del commercio attraverso la banca dati *Consumer Sentinel*; per presentare un reclamo contro le compagnie aeree e i rivenditori che fanno servizio di biglietteria possono invece utilizzare il sito del Dipartimento dei trasporti.

Le organizzazioni e i meccanismi di ricorso indipendenti sono tenuti a trattare i reclami senza indugio. Se un'organizzazione non si conforma alla decisione di un organo indipendente o di un ente governativo, può essere depennata dall'elenco degli aderenti pubblicato e aggiornato dal Dipartimento del commercio.

Gli interessati possono presentare un reclamo anche all'IFPDT. Per accelerarne il trattamento, l'IFPDT è in contatto diretto con il Dipartimento del commercio. Una volta ricevuto il reclamo, l'IFPDT lo inoltra al Dipartimento del commercio, che amministra il quadro

[9] Cfr. titolo 49 del Codice degli Stati Uniti, regolamento relativo ai trasporti, accessibile qui: 49 USC Ch. 461: INVESTIGATIONS AND PROCEEDINGS (house.gov).

commerciale; ciò può comportare l'esclusione dell'organizzazione in questione dall'elenco degli aderenti pubblicato e aggiornato dal Dipartimento del commercio.

Se non è stato possibile risolvere il reclamo in uno dei modi appena illustrati, l'interessato può chiedere, a determinate condizioni e in ultima ratio, l'arbitrato vincolante descritto all'allegato 1 dei principi: un collegio arbitrale composto da uno o da tre arbitri (a seconda di quanto concordato dalle parti) può ordinare misure riparatorie individuali di carattere non pecuniario come l'accesso, la rettifica, la cancellazione o la restituzione dei dati personali. Il Dipartimento del commercio e la Svizzera stileranno un elenco di arbitri scelti in funzione della loro indipendenza, integrità ed esperienza. Il Centro internazionale per la risoluzione delle controversie (*International Centre for Dispute Resolution*) dell'Associazione americana per l'arbitrato (*American Arbitration Association*)[10] gestirà i casi di arbitrato. I procedimenti dinanzi a un collegio arbitrale sono disciplinati da una serie di norme arbitrali concordate e da un codice di condotta per gli arbitri nominati. È possibile adire i tribunali statunitensi per far rispettare le decisioni arbitrali emesse[11].

La tutela giurisdizionale è assicurata quando i rimedi giuridici appena descritti garantiscono decisioni e misure di riparazione efficaci nei casi di reclamo per non conformità ai principi del DPF CH-USA da parte di organizzazioni certificate.

4 Accesso da parte delle autorità pubbliche ai dati personali trasferiti negli Stati Uniti

4.1 Accesso ai fini del perseguimento penale

4.1.1 Legislazione applicabile, garanzie

La Costituzione degli Stati Uniti garantisce che le autorità pubbliche non dispongano di un potere illimitato o arbitrario di sequestrare dati personali. Il quarto emendamento[12] ha lo scopo di tutelare la sfera privata e la sicurezza dell'individuo da ingerenze arbitrarie da parte del governo. Le norme che regolano i mandati di perquisizione o di sequestro si applicano sia alle perquisizioni e ai sequestri di tipo fisico sia ai sequestri di contenuti memorizzati su supporti elettronici. Il quarto emendamento prevede che l'attività del governo sia sempre proporzionata, anche nei casi in cui non occorre alcun mandato.

Ai fini del perseguimento penale (*criminal law enforcement*), i procuratori federali (*federal prosecutors*)[13] e gli inquirenti federali (*federal investigative agents*)[14] possono accedere ai dati

---

[10] Dopo l'entrata in vigore del quadro commerciale, il sito del Centro fornirà informazioni chiare e concise sull'arbitrato e sulla procedura per farne domanda: International Centre for Dispute Resolution | ICDR.org.

[11] Cfr. titolo 9 del Codice degli Stati Uniti (*US Code*), disposizioni sull'arbitrato, consultabile qui: ARBITRATION (house.gov)

[12] Cfr. la Costituzione degli Stati Uniti, consultabile qui: U.S. Senate: Constitution of the United States

[13] I procuratori federali sono agenti del Dipartimento della giustizia.

[14] Gli inquirenti federali sono affiliati al Federal Bureau of Investigation (FBI), aggregato al Dipartimento della giustizia.

personali trattati da organizzazioni certificate secondo le procedure descritte di seguito, applicabili indipendentemente dalla nazionalità o dal luogo di residenza dell'interessato.

Nelle indagini su determinati reati gravi, un *grand jury* può emettere – solitamente su richiesta di un procuratore federale – una citazione a comparire nei confronti di una persona al fine di imporle di produrre o mettere a disposizione documenti aziendali, informazioni conservate su supporti elettronici o altri beni materiali[15]. È inoltre possibile ricorrere alle citazioni a comparire per ottenere questo tipo di documenti e informazioni o altri beni materiali anche nelle indagini per frodi in ambito medico, abusi su minori, a protezione dei servizi segreti e per reati in materia di stupefacenti, così come nelle indagini degli ispettori generali. In tutti i casi le informazioni devono essere rilevanti per l'indagine e la citazione non può essere irragionevole, vale a dire eccessiva, vessatoria o gravosa; il destinatario può contestarla per questi motivi.

Diverse disposizioni legali[16] prevedono che le autorità penali possano accedere ai dati relativi alle comunicazioni. Un giudice può autorizzare la raccolta in tempo reale di metadati (numero composto, instradamento della comunicazione, destinatario e segnale) di un numero telefonico o di un messaggio di posta elettronica, a condizione che le informazioni ottenibili siano rilevanti per un'indagine penale in corso. L'impiego di dispositivi che registrano i dati di traffico delle comunicazioni può essere autorizzato per un periodo massimo di 60 giorni, prorogabile soltanto con una nuova decisione giudiziale. Inoltre le informazioni sugli abbonati, i dati sul traffico e i contenuti archiviati delle comunicazioni detenuti dai fornitori di servizi Internet, da società telefoniche e da altri fornitori di servizi sono accessibili su mandato giudiziale, emesso se vi sono motivi plausibili per ritenere che l'account contenga prove di un reato. Le autorità penali possono ottenere una citazione a comparire per le informazioni relative alla registrazione degli abbonati, agli indirizzi IP e alla fatturazione. Per la maggior parte dei metadati archiviati, un giudice può emettere un mandato se ritiene che siano pertinenti e rilevanti per un'indagine penale in corso.

Le autorità penali possono intercettare in tempo reale comunicazioni orali, analogiche o elettroniche sulla base di un mandato giudiziale che conferma, tra le altre cose, l'esistenza di motivi plausibili per ritenere che l'intercettazione fornirà prove di un reato o del nascondiglio di un latitante.

Se ritiene probabile che vengano rinvenuti oggetti sequestrabili e utilizzabili ad esempio come prova di un reato, il giudice può emettere un mandato di perquisizione o di sequestro. L'interessato può chiedere d'ignorare i mezzi di prova ottenuti in modo illecito e utilizzati in un procedimento penale. Il titolare dei dati tenuto a divulgare dati in forza di un mandato (p. es.

---

[15] Cfr. le norme federali di procedura penale (*Federal Rules of Criminal Procedure*), consultabili qui: Current Rules of Practice & Procedure | United States Courts (uscourts.gov)

[16] Cfr. titolo 18 del Codice degli Stati Uniti, disposizioni sui reati e il procedimento penale (in particolare gli art. 2510 segg., 2701 segg. e 3121 segg.), consultabile qui: OLRC Home (house.gov)

un'azienda certificata) può contestare l'obbligo di divulgazione in quanto indebitamente gravoso[17].

Oltre a quanto appena descritto, esistono le linee guida emanate dal procuratore generale degli Stati Uniti (*Advocate General*) per limitare ulteriormente l'accesso ai dati da parte delle autorità pubbliche ai fini del perseguimento penale e tutelare la sfera privata. Si tratta in particolare delle linee guida per le operazioni nazionali dell'FBI[18], che tra le altre cose impongono metodi di indagine il meno invasivi possibile, tenendo conto della potenziale ingerenza nella sfera privata e del potenziale danno alla reputazione.

Per le indagini svolte a norma delle leggi degli Stati federati valgono garanzie simili. Le autorità penali degli Stati federati utilizzano i mandati e le citazioni a comparire in modo analogo a quello descritto per le autorità federali, seppur talvolta con garanzie aggiuntive previste dalle costituzioni o dalle leggi del singolo Stato. Le garanzie statali devono essere almeno equivalenti a quelle sancite dalla Costituzione degli Stati Uniti.

Garanzie simili si applicano anche alle citazioni amministrative (*administrative subpoenas*) emesse per ottenere l'accesso ai dati detenuti a fini civili o normativi dalle società negli Stati Uniti, ossia a dati di interesse pubblico. Le autorità con competenze civili o normative possono chiedere l'accesso ai soli dati pertinenti per questioni che rientrano nella loro sfera di competenza[19]. Il destinatario di una citazione amministrativa può contestarne l'esecuzione; la citazione deve infatti essere ragionevole[20]. Sebbene il ricorso a una citazione amministrativa non sia soggetto a previa autorizzazione giudiziale, esso è soggetto a esame giurisdizionale in caso di contestazione da parte del destinatario o se l'autorità che l'ha emessa ne chiede l'esecuzione in giudizio. Oltre a queste garanzie generali, si possono applicare requisiti specifici più rigorosi derivanti da alcune leggi[21]. Ad ogni modo devono essere soddisfatti i requisiti previsti dal quarto emendamento della Costituzione degli Stati Uniti.

---

17 Cfr. le norme federali di procedura penale (*Federal Rules of Criminal Procedure*)

18 Consultabili qui: The Attorney General's Guidelines for Domestic FBI Operations (justice.gov)

19 In tale contesto, anche la giurisprudenza della Corte Suprema degli Stati Uniti sottolinea la necessità di trovare un equilibrio tra l'importanza dell'interesse pubblico e l'importanza degli interessi del singolo in materia di tutela della sfera privata. Cfr. *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946), consultabile qui: U.S. Reports: Okla. Press Pub. Co. v. Walling, 327 U.S. 186 (1946). (loc.gov).

20 Cfr. i criteri menzionati in precedenza relativamente alle citazioni a comparire nelle indagini penali.

21 Ad esempio, gli istituti finanziari possono contestare, appellandosi alla legge sul segreto bancario e i pertinenti atti di esecuzione, le citazioni amministrative che ingiungono loro di comunicare determinati tipi di informazioni, cfr. il titolo 31 del Codice degli Stati Uniti, disposizioni sul denaro e le finanze, consultabile qui: OLRC Home (house.gov).

È opportuno evidenziare che gli Stati Uniti hanno confermato – con lettera del Dipartimento della giustizia – le garanzie applicabili e le limitazioni d'accesso appena descritte[22].

L'ulteriore utilizzo dei dati raccolti è retto da una direttiva centrale (circolare n. A-130 dell'Ufficio per la gestione e il bilancio, *Office of Management and Budget*)[23], che deve essere attuata e rispettata da tutte le autorità federali, comprese quelle penali, quando trattano dati personali identificabili. Le autorità sono tenute a limitare la creazione, la raccolta, l'uso, il trattamento, l'archiviazione, la gestione, la diffusione e la divulgazione di dati personali identificabili dell'interessato a quanto legalmente consentito, pertinente e ragionevolmente necessario per il corretto adempimento dei loro compiti. Devono inoltre istituire un programma generale di tutela della sfera privata (al fine di p. es. gestire i rischi o individuare, documentare e segnalare eventuali casi di non conformità).

La normativa sull'e-government[24] impone alle autorità federali di predisporre misure atte a garantire la sicurezza dei dati e commisurate al rischio e all'entità dei danni che potrebbero derivare da un accesso, un uso, una divulgazione, un'alterazione, una modifica o una distruzione non autorizzati. Inoltre devono nominare un responsabile delle informazioni (*Chief Information Officer*) incaricato di assicurare il rispetto dei requisiti di sicurezza dei dati e di effettuare una valutazione annuale indipendente. Una valutazione d'impatto sulla protezione dei dati è richiesta a tutte le autorità federali che sviluppano o acquisiscono nuove tecnologie informatiche per raccogliere, conservare o diffondere dati in forma identificabile o che procedono a una nuova raccolta di dati.

L'Ufficio per la gestione e il bilancio e l'Istituto nazionale per gli standard e la tecnologia (*National Institute of Standards and Technology*) hanno emanato norme vincolanti per gli enti federali (comprese le autorità penali) e contenenti requisiti minimi in materia di sicurezza dei dati: controllo dell'accesso, sensibilizzazione e formazione, piani di emergenza, reazione agli incidenti, strumenti di verifica e di responsabilizzazione, garanzia dell'integrità dei sistemi e dei dati, valutazione dei rischi in materia di sicurezza e protezione dei dati ecc.[25]

La normativa sui documenti federali[26] impone alle autorità federali di adottare misure che assicurino l'integrità fisica dei dati detenuti e li proteggano da accessi non autorizzati.

---

[22] Cfr. la lettera del Dipartimento della giustizia, consultabile al link corrispondente alla fine del documento.

[23] Consultabile qui: Review-Doc-2016--466-1.docx (archives.gov)

[24] Cfr. titolo 44 cap. 36 del Codice degli Stati Uniti

[25] Cfr. la circolare n. A-130 dell'Ufficio per la gestione e il bilancio; NIST SP 800-53, Rev. 5, Control Mappings to ISO/IEC 27001, luglio 2023, consultabile qui: SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)

[26] Cfr. titolo 44 cap. 31 del Codice degli Stati Uniti

Per quanto riguarda la conservazione dei dati, le autorità federali sono tenute a stabilire periodi di conservazione, che devono essere approvati dall'Amministrazione degli archivi nazionali (*National Archives and Record Administration*)[27]. La loro durata è fissata in funzione di diversi fattori, come il tipo di indagine e la rilevanza dei mezzi di prova per l'indagine.

4.1.2 Autorità indipendente, rimedi giuridici

4.1.2.1 Vigilanza

Le attività delle autorità penali federali sono monitorate da vari organismi, giudiziari e non, che garantiscono una vigilanza indipendente[28]. Come illustrato al numero 4.1.1, nella maggior parte dei casi si tratta di una vigilanza preventiva da parte del potere giudiziario, che deve autorizzare le singole misure di raccolta dei dati, mentre altri organismi vigilano sulle attività delle autorità penali.

Svariate autorità penali impiegano addetti alla tutela della sfera privata e alle libertà civili (*Civil Liberties and Privacy Officers*, di seguito addetti CLP)[29], chiamati a vigilare sulle procedure per assicurare che l'autorità tenga debito conto degli aspetti inerenti alla sfera privata e alle libertà civili e abbia predisposto procedure adeguate per trattare i relativi reclami. I responsabili di ciascuna autorità devono garantire che gli addetti CLP dispongano della documentazione e delle risorse necessarie per adempiere il loro mandato, abbiano accesso al materiale e al personale necessari per svolgere le loro funzioni e siano informati e consultati in merito alle proposte di modifica delle politiche in materia. Gli addetti CLP devono riferire periodicamente al Congresso, in particolare in merito al numero e al tipo di reclami ricevuti dalle autorità e alle azioni intraprese, nonché in merito all'impatto delle attività da loro svolte.

Inoltre, un ispettore generale[30] indipendente[31] supervisiona le attività del Dipartimento della giustizia, compreso l'FBI. Si occupa di svolgere, in maniera indipendente, indagini, verifiche e ispezioni sui programmi e le attività del Dipartimento[32], ha accesso – se necessario emettendo una citazione – a tutti i fascicoli, le relazioni, le verifiche, gli esami, i documenti, le raccomandazioni o altro materiale pertinente e può raccogliere testimonianze. Sebbene i

---

[27] Cfr. titolo 44 cap. 29 del Codice degli Stati Uniti

[28] I meccanismi menzionati al n. 4.1.2.1 si applicano anche alla raccolta e all'uso dei dati da parte delle autorità federali per finalità civili e normative. Le autorità federali civili e normative sono soggette al controllo da parte dei rispettivi ispettori generali e del Congresso.

[29] Cfr. titolo 42 cap. 21E del Codice degli Stati Uniti

[30] Cfr. titolo 5 parte I cap. 4 del Codice degli Stati Uniti

[31] Gli ispettori generali sono inamovibili; possono essere rimossi dall'incarico soltanto dal presidente degli Stati Uniti, che deve comunicare per iscritto al Congresso i motivi della destituzione.

[32] Cfr. il piano strategico 2020-2024 dell'ispettore generale del Dipartimento della giustizia, consultabile qui: Strategic Plan Draft - To AIGs (justice.gov)

correttivi raccomandati dall'ispettore generale non siano vincolanti, le relazioni da lui redatte sono in genere rese pubbliche e trasmesse al Congresso, che può così esercitare la sua funzione di vigilanza. L'ispettore generale riceve ed esamina i reclami presentati da privati.

Inoltre, le autorità penali impegnate in attività antiterrorismo sono soggette alla supervisione dell'Autorità di vigilanza sulla sfera privata e le libertà civili (*Privacy and Civil Liberties Oversight Board*, di seguito PCLOB), un organismo esecutivo indipendente composto da cinque membri nominati dal presidente degli Stati Uniti per un mandato fisso di sei anni previa approvazione da parte del Senato; in nessun caso può contare più di tre membri dello stesso partito[33]. Tale autorità adempie compiti e attua politiche nella lotta contro il terrorismo al fine di tutelare la sfera privata e le libertà civili. Ha accesso a tutti i fascicoli, le relazioni, le verifiche, gli esami, i documenti e le raccomandazioni pertinenti delle autorità federali, comprese le informazioni classificate, e può raccogliere testimonianze. Riceve le relazioni trasmesse dagli addetti CLP delle varie autorità federali, può rivolgere raccomandazioni al governo e alle autorità penali e riferisce periodicamente alle commissioni del Congresso e al presidente. Le relazioni devono essere per quanto possibile rese pubbliche.

Infine le attività in materia penale sono soggette alla vigilanza delle commissioni giudiziarie della Camera dei rappresentanti e del Senato, che esercitano una vigilanza costante ricorrendo a vari strumenti, in particolare audizioni, indagini, riesami e relazioni.

4.1.2.2 Rimedi giuridici

Nella maggior parte dei casi le autorità penali devono ottenere un'autorizzazione giudiziaria preventiva per poter raccogliere dati personali. Ciò non vale tuttavia per le citazioni amministrative, limitate a situazioni specifiche e soggette a un esame giurisdizionale indipendente, perlomeno nei casi in cui non sia richiesta l'esecuzione per via giudiziaria. In particolare, i destinatari di citazioni amministrative possono contestarle dinanzi a un giudice se le ritengono irragionevoli, vale a dire eccessive, vessatorie o gravose. Gli interessati possono presentare richieste o reclami alle autorità penali in merito al trattamento dei loro dati personali e richiedere così l'accesso e la rettifica dei loro dati[34]. Per quanto concerne le attività antiterrorismo, gli interessati possono presentare un reclamo agli addetti CLP delle autorità penali[35].

Esistono inoltre diversi rimedi giuridici da utilizzare nei confronti di un'autorità o di uno dei suoi funzionari a motivo del trattamento di dati personali. Questi rimedi[36] sono aperti a tutti, indipendentemente dalla nazionalità, purché siano soddisfatte le condizioni applicabili.

---

[33] Cfr. titolo 42 cap. 21E del Codice degli Stati Uniti

[34] Cfr. la circolare n. A-130 dell'Ufficio per la gestione e il bilancio

[35] Cfr. titolo 42 cap. 21E del Codice degli Stati Uniti

[36] Cfr. le normative sulla procedura amministrativa e la trasparenza (cfr. titolo 5 del Codice degli Stati Uniti) e la normativa sulla confidenzialità delle comunicazioni elettroniche (cfr. titolo 18 del Codice degli Stati Uniti)

In generale, in virtù delle disposizioni sul sindacato giurisdizionale previste dalla normativa sulle procedure amministrative[37], chiunque subisca un illecito, un danno o un torto a causa di una decisione di un'autorità ha diritto di chiedere al giudice di dichiarare illegittime e nulle le decisioni, constatazioni e conclusioni amministrative che risultano arbitrarie, futili, viziate da abuso di potere o altrimenti non conformi alla legge.

Più nello specifico, la normativa sulla riservatezza delle comunicazioni elettroniche[38], che introduce tutta una serie di diritti a tutela della sfera privata, disciplina l'accesso, ai fini dell'applicazione della legge, ai contenuti delle comunicazioni orali, analogiche o elettroniche conservate da terzi fornitori di servizi. Sancisce la punibilità dell'accesso illegale (ossia non autorizzato dal giudice o altrimenti non consentito) a tali comunicazioni e offre alla persona lesa la possibilità di intentare un'azione civile dinanzi a un tribunale federale statunitense per ottenere il risarcimento dei danni effettivi e punitivi e chiedere un'equa riparazione o una decisione dichiarativa in tal senso nei confronti degli Stati Uniti o del funzionario governativo che ha deliberatamente commesso tale illecito.

Varie altre normative[39] conferiscono agli interessati il diritto di intentare un'azione contro un'autorità o un funzionario statunitense a motivo del trattamento dei dati personali che li riguardano.

Infine, la normativa sulla trasparenza[40] conferisce a chiunque il diritto di ottenere l'accesso alle informazioni in possesso delle autorità federali, anche se contengono dati personali. Una volta esperiti i rimedi giuridici amministrativi, l'interessato può invocare tale diritto dinanzi a un giudice, a meno che non si applichi una deroga alle disposizioni di legge o una pertinente esclusione speciale secondo cui le informazioni in questione non possono essere divulgate pubblicamente. In questi casi, spetta al giudice valutare se una deroga si applica o è stata legittimamente invocata dall'autorità pertinente.

4.2 Accesso ai fini della sicurezza nazionale

4.2.1 Legislazione applicabile, garanzie

Per motivi di sicurezza nazionale e nel rispetto di condizioni e garanzie specifiche, le autorità statunitensi possono raccogliere i dati personali trasferiti dalla Svizzera alle organizzazioni certificate. In tale contesto è importante esaminare con attenzione la raccolta di informazioni mediante l'intercettazione e l'analisi dei segnali elettromagnetici (*signals intelligence* o intelligence dei segnali), che implica la raccolta di comunicazioni elettroniche e dati tratti da sistemi d'informazione ed eventualmente contenenti dati personali.

---

[37] Cfr. titolo 5 del Codice degli Stati Uniti

[38] Cfr. titolo 18 parte I cap. 121 del Codice degli Stati Uniti

[39] P. es. la normativa sulle intercettazioni, le frodi e gli abusi informatici (cfr. titolo 18 del Codice degli Stati Uniti)

[40] Cfr. titolo 5 del Codice degli Stati Uniti

Conformemente al decreto presidenziale (*executive order*) 12333 del 1981[41] relativo alle attività dei servizi di intelligence statunitensi, i dati personali possono essere raccolti anche al di fuori degli Stati Uniti, quindi anche durante il loro trasferimento dalla Svizzera verso gli Stati Uniti.

Dopo che le organizzazioni certificate negli Stati Uniti hanno ricevuto i dati personali, i servizi di intelligence statunitensi possono chiedere l'accesso a tali dati nella misura consentita dalle leggi in vigore, in particolare la normativa relativa alla vigilanza sull'intelligence esterna (*Foreign Intelligence Surveillance Act*, FISA)[42].

Il 7 ottobre 2022 il presidente degli Stati Uniti ha emanato il decreto presidenziale 14086[43] che migliora le garanzie per le attività di intelligence dei segnali: sostituisce in larga misura[44] la direttiva presidenziale 28 (*Presidential Policy Directive 28,* PPD-28)[45], si applica a tutte le attività di intelligence dei segnali, sia a quelle rette dalla FISA che a quelle rette dal decreto 12333, ed è vincolante per l'intera comunità dell'intelligence statunitense. Introduce limitazioni e garanzie che vanno a integrare quelle previste dalla FISA e dal decreto 12333 e istituisce un nuovo meccanismo di ricorso per invocare e applicare tali garanzie. I servizi di intelligence hanno aggiornato le loro politiche e procedure per conformarle al decreto 14086. Dopo varie consultazioni, in particolare del procuratore generale, dell'addetto CLP della direzione dell'intelligence nazionale (*Office of the Director of National Intelligence*, ODNI) e della PCLOB, queste politiche e procedure sono state rese pubbliche il 3 luglio 2023[46].

Il decreto presidenziale 14086 stabilisce una serie di requisiti applicabili a tutte le attività di intelligence dei segnali. Tali attività devono fondarsi su una legge o un'autorizzazione presidenziale ed essere conformi al diritto statunitense, compresa la Costituzione. Per assicurare che nella pianificazione di tali attività venga tenuto conto della sfera privata e delle libertà civili di tutti gli individui, indipendentemente dalla loro nazionalità o dal loro luogo di residenza, sono necessarie garanzie adeguate; in particolare occorre stabilire, sulla base di un'adeguata valutazione di tutti i fattori rilevanti, che tali attività sono necessarie per portare avanti una priorità convalidata dell'intelligence. Le attività vanno proporzionate alla priorità per la quale sono state autorizzate, trovando un giusto equilibrio tra l'importanza della priorità perseguita e l'impatto sulla sfera privata e le libertà civili degli interessati.

---

41 Cfr. Executive Orders | National Archives

42 Cfr. titolo 50 cap. 36 del Codice degli Stati Uniti

43 Cfr. i link ai testi di riferimento alla fine del documento

44 Il decreto presidenziale 14086 sostituisce la direttiva PPD-28 ad eccezione di alcuni articoli specifici (revoca parziale della PPD-28).

45 Cfr. Presidential Policy Directive -- Signals Intelligence Activities | whitehouse.gov (archives.gov)

46 Cfr. INTEL - ODNI Releases IC Procedures Implementing New Safeguards in Executive Order 14086

I requisiti menzionati sono corroborati da una serie di garanzie atte ad assicurare che l'ingerenza nei diritti delle persone si limiti a quanto necessario e proporzionato per raggiungere un obiettivo legittimo.

Il decreto 14086 limita i motivi per i quali possono essere raccolti dati nel contesto di attività di intelligence dei segnali. Da un lato, stabilisce gli obiettivi legittimi, 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; dall'altro, elenca alcuni obiettivi che non sono mai legittimi, ad esempio limitare la libera espressione di idee od opinioni politiche a persone o media. Inoltre, i dati possono essere raccolti soltanto per portare avanti una priorità in materia di intelligence. Le priorità sono fissate dalla direttrice dell'intelligence nazionale e valutate dall'addetto CLP dell'ODNI; dopodiché vengono sottoposte per approvazione al presidente degli Stati Uniti. In questo modo viene garantito che nell'elaborare le priorità venga tenuto debito conto della tutela della sfera privata.

Una volta definita una priorità, viene deciso, sulla base di una serie di requisiti, se e come raccogliere l'intelligence dei segnali per portare avanti tale priorità. I requisiti concretizzano le norme generali in materia di necessità e proporzionalità stabilite nel decreto 14086. L'intelligence dei segnali può essere raccolta soltanto dopo aver stabilito, sulla base di un'adeguata valutazione di tutti i fattori rilevanti, che i dati sono necessari per portare avanti una specifica priorità in materia. Nello stabilire questo criterio di necessità, gli enti di intelligence statunitensi devono considerare la disponibilità, la fattibilità e la validità di altre fonti e altri metodi meno intrusivi ed eventualmente dare loro la priorità.

Se ritenuta necessaria, la raccolta deve essere quanto più mirata possibile. Onde evitare un'ingerenza sproporzionata nella sfera privata e nelle libertà civili, vale a dire per trovare un giusto equilibrio tra le esigenze di sicurezza nazionale e la tutela della sfera privata e delle libertà civili, occorre tenere debito conto di tutti i fattori rilevanti, quali la natura dell'obiettivo perseguito, il grado di ingerenza dell'attività di raccolta (compresa la sua durata), il presunto contributo della raccolta al raggiungimento dell'obiettivo perseguito, le conseguenze ragionevolmente prevedibili per le persone, nonché la natura e la sensibilità dei dati da raccogliere.

La raccolta in blocco di intelligence dei segnali, ossia in grandi quantità senza l'impiego di criteri di selezione specifici[47], può essere effettuata soltanto al di fuori degli Stati Uniti in virtù del decreto presidenziale 12333. Anche in questo caso va data la priorità alla raccolta mirata. Conformemente al decreto presidenziale 14086, la raccolta in blocco è consentita solo se le informazioni necessarie per portare avanti una priorità convalidata non possono essere ottenute ragionevolmente con una raccolta mirata; inoltre, alla raccolta in blocco si applicano garanzie specifiche: vanno impiegati metodi e misure tecniche per limitare i dati raccolti a quanto necessario per portare avanti la priorità convalidata, riducendo al minimo la raccolta di informazioni irrilevanti; le informazioni raccolte in blocco possono essere utilizzate esclusivamente per perseguire sei obiettivi specifici, tra cui la protezione contro il terrorismo e contro lo spionaggio straniero, il sabotaggio o l'assassinio. Infine l'intelligence dei segnali

[47] La raccolta in blocco va distinta dalla raccolta generalizzata e indiscriminata («sorveglianza di massa») senza limitazioni e garanzie.

raccolta in blocco può essere consultata solo se necessario per portare avanti una priorità convalidata in vista dei sei obiettivi specifici e in conformità con politiche e procedure che tengano debito conto dell'impatto delle consultazioni dei dati sulla sfera privata e le libertà civili di tutte le persone, indipendentemente dalla loro nazionalità o dal loro luogo di residenza.

Oltre ai requisiti di cui al decreto presidenziale 14086, la raccolta di dati relativi all'intelligence dei segnali trasferiti a un'organizzazione certificata negli Stati Uniti è soggetta a limitazioni e garanzie specifiche disciplinate dall'articolo 702 FISA, secondo cui il procuratore generale e la direttrice dell'intelligence nazionale determinano ogni anno le categorie di intelligence esterna da acquisire sottoponendo certificazioni alla Corte di vigilanza sull'intelligence esterna (*Foreign Intelligence Surveillance Court*, di seguito Corte FISA). Le certificazioni devono essere abbinate a procedure per individuare i target, minimizzare la quantità di dati raccolti e consultare i dati, approvate anche dalla Corte e giuridicamente vincolanti per gli enti di intelligence statunitensi.

La Corte FISA è un organo giurisdizionale indipendente le cui decisioni possono essere impugnate dinanzi alla Corte di controllo della vigilanza sull'intelligence esterna (*Foreign Intelligence Surveillance Court of Review*) e, in ultima istanza, alla Corte suprema degli Stati Uniti[48]. È coadiuvata da un comitato permanente formato da cinque avvocati e cinque specialisti in materia di sicurezza nazionale e libertà civili allo scopo di garantire che gli aspetti inerenti alla tutela della sfera privata siano adeguatamente presi in considerazione.

Le decisioni in merito all'individuazione dei singoli target sono prese dall'Agenzia per la sicurezza nazionale (*National Security Agency*, NSA) conformemente alle pertinenti procedure approvate dalla Corte FISA, che impongono all'NSA di valutare, tenendo conto di tutte le circostanze, se concentrare le attività di raccolta dati su una determinata persona consentirebbe di acquisire una categoria di intelligence estera indicata in una certificazione. I target sono individuati grazie a selettori che identificano dispositivi di comunicazione specifici come l'indirizzo e-mail o il numero di telefono del target, ma mai parole chiave o nomi di persone. L'NSA deve documentare la base fattuale per la selezione del target e confermare, a intervalli regolari dopo l'individuazione iniziale, che le norme applicabili in materia continuano a essere rispettate; in caso contrario la raccolta di dati va interrotta. La selezione di ciascun target da parte dell'NSA e la corrispondente registrazione di ciascuna valutazione e motivazione alla base di tale selezione sono verificate ogni due mesi dagli uffici di vigilanza sull'intelligence presso il Dipartimento della giustizia, tenuti a segnalare qualsiasi violazione alla Corte FISA e al Congresso.

Le altre basi giuridiche relative alla raccolta di dati personali trasferiti a organizzazioni certificate negli Stati Uniti prevedono diverse limitazioni e garanzie. In generale, vietano espressamente la raccolta di dati in blocco e impongono l'uso di selettori specifici. Per poter svolgere attività di sorveglianza elettronica individualizzate, gli enti di intelligence devono presentare alla Corte FISA una domanda corredata di un'esposizione dei fatti e delle circostanze a giustificazione del sospetto fondato che il dispositivo di comunicazione in questione sia utilizzato o stia per essere utilizzato da una potenza straniera o da un agente di

[48] Cfr. titolo 50 cap. 36 del Codice degli Stati Uniti

una potenza straniera. Tra le altre cose la Corte FISA valuta se dai fatti esposti risultano motivi plausibili per ritenere fondato il sospetto di un uso a detti fini. Alla Corte FISA va presentata una domanda anche per perquisire locali o beni al fine di ispezionare o sequestrare informazioni, materiali o beni o per installare dispositivi di intercettazione delle comunicazioni in entrata e in uscita.

Al trattamento dei dati personali raccolti dagli enti di intelligence statunitensi nel contesto dell’intelligence dei segnali si applicano una serie di garanzie. Innanzitutto, ogni ente di intelligence deve garantire una sicurezza adeguata dei dati e impedire ogni tipo di accesso non autorizzato. L’accesso ai dati raccolti deve essere limitato al personale autorizzato e formato che necessita di tali informazioni per svolgere la propria attività. Più in generale gli enti di intelligence devono garantire la formazione adeguata dei propri collaboratori e rispettare le norme della comunità dell’intelligence in materia di accuratezza e obiettività, in particolare per quanto riguarda la qualità e l’affidabilità dei dati, la considerazione di fonti di informazione alternative e l’obiettività nello svolgere le analisi. Alla conservazione dei dati si applicano inoltre gli stessi periodi di conservazione indipendentemente dalla nazionalità delle persone. Alla diffusione di dati personali raccolti nel contesto dell’intelligence dei segnali si applicano invece norme specifiche: ad esempio, i dati personali non possono essere diffusi soltanto in ragione della nazionalità o del Paese di residenza di una persona o allo scopo di aggirare i requisiti stabiliti nel decreto 14086. Infine, per facilitare la verifica del rispetto dei requisiti legali applicabili e offrire mezzi di ricorso efficaci, ogni ente di intelligence è tenuto a conservare una documentazione adeguata sulla raccolta di intelligence dei segnali. Oltre alle citate garanzie del decreto 14086, applicabili all’uso delle informazioni raccolte nel contesto dell’intelligence dei segnali, tutti gli enti di intelligence statunitensi devono adempiere requisiti più generali in materia di limitazione delle finalità, minimizzazione dei dati, accuratezza, sicurezza, conservazione e diffusione dei dati come previsto in particolare dall’istruzione 1253 del comitato sui sistemi di sicurezza nazionale relativa alla categorizzazione della sicurezza e alla selezione dei controlli per i sistemi di sicurezza nazionale, dalla circolare numero A-130 dell’Ufficio per la gestione e il bilancio e da altre normative applicabili.

4.2.2 Autorità indipendente, rimedi giuridici

4.2.2.1 Vigilanza

Le attività degli enti di intelligence sono monitorate da vari organismi. Il decreto 14086 impone a ciascun ente di disporre di collaboratori di alto livello competenti in materia di diritto, di vigilanza e di conformità alle norme al fine di garantire il rispetto del diritto statunitense applicabile. In particolare, tali collaboratori devono monitorare periodicamente le attività di intelligence dei segnali e garantire che venga posto rimedio a eventuali casi di non conformità. Gli enti di intelligence devono dare loro accesso a tutte le informazioni utili per adempiere le loro funzioni e non possono adottare misure che ostacolino o influenzino indebitamente le loro attività di vigilanza. Inoltre, qualsiasi caso rilevante di non conformità, individuato da un collaboratore incaricato della vigilanza o da qualsiasi altra persona, deve essere prontamente segnalato al capo dell’ente di intelligence e alla direttrice dell’intelligence nazionale, che devono assicurare l’adozione di tutte le misure necessarie per porvi rimedio ed evitare che quanto accaduto si ripeta.

Alla stregua delle autorità penali anche gli enti di intelligence dispongono di addetti CLP[49], chiamati tra le altre cose a vigilare sulle procedure al fine di garantire che il dipartimento/ente tenga adeguatamente conto degli aspetti inerenti alla tutela della sfera privata e alle libertà civili e abbia predisposto meccanismi adeguati per trattare i reclami di chi sostiene che la propria sfera privata o le proprie libertà civili siano state violate. I capi degli enti di intelligence devono garantire che gli addetti CLP dispongano delle risorse necessarie per adempiere il loro mandato, abbiano accesso al materiale e al personale necessari per svolgere le loro funzioni e siano informati e consultati in merito alle proposte di modifica delle politiche in materia. Gli addetti CLP riferiscono periodicamente al Congresso e alla PCLOB in merito al numero e al tipo di reclami ricevuti dal dipartimento/dall'ente, ne illustrano brevemente il trattamento e informano in merito alle verifiche effettuate e alle indagini condotte, nonché all'impatto delle attività da loro svolte.

Ciascun ente di intelligence dispone di un ispettore generale indipendente incaricato, tra le altre cose, di vigilare sulle attività di intelligence esterna. L'Ufficio dell'ispettore generale della comunità dell'intelligence, aggregato all'ODNI, vanta una competenza generale su tutta la comunità dell'intelligence. Gli ispettori generali sono indipendenti ed effettuano controlli e indagini sui programmi e sulle attività condotte dall'ente in questione per finalità di intelligence nazionale, anche in relazione a casi di abuso o violazione delle disposizioni di legge. Hanno accesso – se necessario emettendo una citazione – a tutti i dati, le relazioni, le verifiche, gli esami, i documenti, le raccomandazioni o altro materiale pertinente e possono raccogliere testimonianze. Segnalano alle autorità penali i casi di sospetto reato e raccomandano ai capi degli enti di intelligence l'adozione di eventuali misure correttive. Sebbene tali raccomandazioni non siano vincolanti, le relazioni redatte, comprese quelle sulle misure successive intraprese (o non intraprese), sono in genere rese pubbliche e trasmesse al Congresso consentendogli di esercitare la propria funzione di vigilanza.

L'Autorità di vigilanza sull'intelligence (*Intelligence Oversight Board*), istituita in seno al Comitato presidenziale consultivo sull'intelligence (*President's Intelligence Advisory Board*), vigila sul rispetto di tutte le norme applicabili, compresa la Costituzione statunitense, da parte della comunità dell'intelligence. Il Comitato è composto da 16 membri nominati dal presidente e non facenti parte del governo statunitense, mentre l'Autorità è costituita da un massimo di cinque membri designati dal presidente tra quelli del Comitato. Conformemente al decreto 12333, i capi di tutti gli enti di intelligence sono tenuti a segnalare all'Autorità di vigilanza sull'intelligence qualsiasi attività di intelligence che abbiano motivo di ritenere illegale o contraria a un decreto o una direttiva presidenziale. Dal canto suo, l'Autorità è tenuta a informare il presidente in merito alle attività di intelligence che potrebbero a suo avviso essere contrarie al diritto nazionale (in particolare i decreti) e che non sono state trattate in modo adeguato dal procuratore generale, dalla direttrice dell'intelligence nazionale o dal capo di un ente di intelligence. Inoltre, è tenuta a informare il procuratore generale di possibili violazioni del diritto penale.

Gli enti di intelligence sono inoltre soggetti al controllo della PCLOB. Conformemente al suo atto istitutivo, la PCLOB ha competenze strategiche e operative in materia di antiterrorismo al fine di tutelare la sfera privata e le libertà civili. Per controllare le attività degli enti di

[49] Cfr. titolo 42 del Codice degli Stati Uniti

intelligence, ha accesso a tutti i dati, le relazioni, le verifiche, i documenti, le carte e le raccomandazioni dell'ente in questione, comprese le informazioni classificate, e può raccogliere testimonianze. Può rivolgere raccomandazioni alle autorità e riferisce periodicamente alle commissioni del Congresso e al presidente. Le relazioni della PCLOB, comprese quelle presentate al Congresso, devono essere per quanto possibile rese pubbliche. La PCLOB vigila inoltre sull'attuazione del decreto 14086 verificando in particolare se le procedure degli enti di intelligence sono compatibili con il decreto e se il meccanismo di ricorso funziona correttamente (v. n. 4.2.2.2).

Accanto a questi meccanismi di vigilanza del ramo esecutivo, le commissioni Giustizia e Intelligence della Camera dei rappresentanti e del Senato (*House and Senate Intelligence and Judiciary Committees*) vigilano su tutte le attività di intelligence esterna. I membri di queste commissioni hanno accesso alle informazioni classificate e ai metodi e programmi di intelligence. Dette commissioni esercitano la loro funzione di vigilanza in vari modi, in particolare attraverso audizioni, indagini, riesami e relazioni. Ricevono relazioni periodiche sulle attività di intelligence, in particolare dal procuratore generale, dalla direttrice dell'intelligence nazionale, dagli enti di intelligence e da altri organismi di vigilanza (p. es. gli ispettori generali).

Più in generale la comunità dell'intelligence si adopera in vari modi per garantire la trasparenza delle sue attività di intelligence. Nel 2015, ad esempio, l'ODNI ha adottato i principi di trasparenza in materia di intelligence e un corrispondente piano di attuazione[50]. In tale contesto, la comunità dell'intelligence ha reso e continua a rendere pubbliche parti declassificate di politiche, procedure, relazioni di vigilanza ecc.

Infine, in virtù della FISA, la raccolta di dati personali è soggetta anche a vigilanza da parte della Corte FISA. All'occorrenza la Corte può ordinare all'ente di intelligence in questione di adottare misure correttive, che possono essere di natura individuale o strutturale e spaziare ad esempio dalla cessazione della raccolta di dati alla cancellazione di dati ottenuti illecitamente o alla modifica delle pratiche di raccolta. Inoltre, nell'ambito del riesame annuale delle certificazioni, la Corte FISA esamina i casi di non conformità per stabilire se le certificazioni presentate soddisfano i requisiti della FISA. Se ritiene che le certificazioni chieste dal governo a norma dell'articolo 702 FISA siano insufficienti, segnatamente in ragione di inadempienze, può emettere una decisione in tal senso (*deficiency order*) che impone al governo di porre rimedio alla violazione entro 30 giorni o di cessare o rinunciare ad attuare la certificazione. Infine la Corte FISA valuta i problemi di conformità riscontrati e può imporre modifiche di procedura o ulteriori attività di vigilanza e rendicontazione per risolverli.

4.2.2.2 Rimedi giuridici

Gli interessati hanno diverse possibilità per promuovere un'azione dinanzi a un giudice indipendente e imparziale e per accedere ai propri dati personali, chiedere la verifica della legittimità dell'accesso ai propri dati da parte delle autorità pubbliche e, in caso di violazione accertata, porvi rimedio facendo rettificare o cancellare i dati in questione.

---

[50] Cfr. The Principles of Intelligence Transparency for the IC (dni.gov)

In virtù del decreto 14086 è istituito un meccanismo di ricorso specifico, integrato dal regolamento del procuratore generale, del 7 ottobre 2022, che istituisce il Tribunale del riesame in materia di protezione dei dati (*Data Protection Review Court,* di seguito Tribunale del riesame), al fine di trattare e risolvere i reclami ricevuti in merito ad attività di intelligence dei segnali negli Stati Uniti. Chiunque risieda in Svizzera ha il diritto di presentare un reclamo per una presunta violazione del diritto statunitense in materia di attività di intelligence dei segnali che lede la sua sfera privata o le sue libertà civili. Possono ricorrere a tale meccanismo le persone provenienti da Stati od organizzazioni regionali di integrazione economica designati come qualificati dal procuratore generale degli Stati Uniti. Il 7 giugno 2024, la Svizzera è stata designata come Stato qualificato[51].

Una persona in Svizzera che intende presentare un reclamo di questo tipo deve prima rivolgersi all'IFPDT in quanto autorità di controllo indipendente responsabile della protezione dei dati personali in Svizzera e della trasmissione dei reclami nel quadro del meccanismo di ricorso. Questa procedura garantisce un facile accesso al meccanismo di ricorso in quanto consente agli interessati di rivolgersi a un'autorità con cui comunicare nella propria lingua. Affinché l'autorità possa iniziare le verifiche del caso, occorre fornire alcune informazioni per verificare che il reclamo è stato presentato da un individuo nonché alcune informazioni di base sui dati personali (come l'indirizzo e-mail o il numero di telefono) che si sospetta siano stati trasferiti negli Stati Uniti, sui mezzi con cui si sospetta tale trasferimento sia avvenuto, l'identità (se nota) degli enti pubblici statunitensi che si ritiene siano coinvolti nella presunta violazione e la natura della misura richiesta, ad esempio la cancellazione dei dati. Non è invece necessario dimostrare che i dati personali sono stati effettivamente raccolti da enti di intelligence statunitensi o sono stati oggetto di attività di intelligence dei segnali. In questo contesto, l'IFPDT riceve il reclamo, verifica l'identità della persona e appura se sono state fornite le informazioni di base; in caso affermativo, lo trasmette alla competente autorità statunitense.

L'esame iniziale dei reclami presentati spetta all'addetto CLP dell'ODNI, il cui ruolo e i cui poteri sono stati estesi alle misure specifiche prese a norma del decreto 14086. La direttiva 126[52] della comunità dell'intelligence, emanata dall'ODNI, illustra in dettaglio le procedure per attuare il meccanismo ai sensi del decreto 14086. All'interno della comunità dell'intelligence, l'addetto CLP dell'ODNI ha il compito di assicurare che la tutela della sfera privata e delle libertà civili sia adeguatamente integrata nelle politiche e nelle procedure dell'ODNI e degli enti di intelligence, di vigilare sul rispetto, da parte dell'ODNI, dei requisiti applicabili in materia, nonché di valutare l'impatto sulla sfera privata. L'addetto CLP dell'ODNI può essere rimosso dall'incarico dal direttore dell'intelligence nazionale soltanto per giusta causa, ossia in caso di condotta illecita, commissione di un reato, violazione della sicurezza, negligenza o incapacità. Nell'effettuare l'esame iniziale, l'addetto CLP dell'ODNI ha accesso alle informazioni necessarie per la valutazione e può contare sull'assistenza obbligatoria degli addetti CLP dei vari enti di intelligence. Agli enti di intelligence, così come alla direttrice dell'intelligence nazionale, è vietato ostacolare o influenzare indebitamente l'esame. Nell'esaminare un reclamo, l'addetto CLP dell'ODNI deve applicare la legge in modo

[51] Cfr. i link ai testi di riferimento alla fine del documento

[52] Cfr. i link ai testi di riferimento alla fine del documento

imparziale, tenendo conto sia degli interessi di sicurezza nazionale inerenti alle attività di intelligence dei segnali sia della tutela della sfera privata. Nell’ambito del suo esame l’addetto CLP dell’ODNI stabilisce se il diritto statunitense applicabile è stato violato; in tal caso dispone una misura correttiva adeguata che ponga pieno rimedio alla violazione accertata, ordinando ad esempio di cessare l’acquisizione illecita di dati, di cancellare i dati raccolti illecitamente o i risultati di consultazioni improprie di dati altrimenti raccolti lecitamente, di riservare a personale adeguatamente formato l’accesso ai dati raccolti in modo lecito o di richiamare le relazioni di intelligence contenenti dati acquisiti o diffusi senza legittima autorizzazione. Le decisioni dell’addetto CLP dell’ODNI sui singoli reclami, comprese le misure correttive, sono vincolanti per gli enti di intelligence interessati, a meno che il Tribunale del riesame non emetta successivamente una decisione contraria. L’addetto CLP dell’ODNI deve conservare la documentazione del suo esame e fornire una decisione classificata che espliciti la base delle sue constatazioni fattuali, le prove di una violazione tra quelle contemplate e la misura correttiva ritenuta adeguata. Se dall’esame emerge una violazione di un’autorità soggetta alla vigilanza della Corte FISA, l’addetto CLP dell’ODNI deve fornire anche una relazione classificata al procuratore generale aggiunto per la sicurezza nazionale, a sua volta tenuto a segnalare la violazione alla Corte FISA, la quale può adottare ulteriori misure.

Una volta completato l’esame, l’addetto CLP dell’ODNI ne informa il reclamante con risposta standard tramite l’IFPDT indicando se sono state rilevate violazioni tra quelle contemplate. In caso di violazioni lo informa che sono state disposte misure correttive adeguate. Questa procedura consente di tutelare la riservatezza delle attività nell’interesse della sicurezza nazionale, fornendo al contempo all’interessato una decisione impugnabile confermante che il suo reclamo è stato debitamente esaminato e giudicato. Del resto l’interessato viene informato della possibilità di adire il Tribunale del riesame per far verificare la decisione dell’addetto CLP dell’ODNI e del fatto che, in caso di appello al Tribunale, sarà designato un avvocato speciale per rappresentare i suoi interessi e per garantire che il collegio del Tribunale sia pienamente informato sulle questioni di diritto e di fatto relative al caso.

Qualsiasi reclamante e qualsiasi membro della comunità dell’intelligence può adire il Tribunale del riesame per chiedere la verifica della decisione dell’addetto CLP dell’ODNI. Se un servizio della comunità dell'intelligence chiede il riesame della decisione dell’addetto CLP dell’ODNI dinanzi al Tribunale, sarà designato un avvocato speciale per rappresentare gli interessi del reclamante e per garantire che il collegio del Tribunale sia pienamente informato sulle questioni di diritto e di fatto relative al caso. La domanda deve essere presentata entro 60 giorni dal ricevimento della notifica che l’esame dell’addetto CLP dell’ODNI è stato completato e deve comprendere tutte le informazioni che il reclamante desidera comunicare al Tribunale del riesame (p. es. argomentazioni su questioni di diritto). Anche in questo caso gli interessati in Svizzera devono presentare la loro domanda all’IFPDT, che la trasmetterà al Tribunale.

Il Tribunale del riesame, istituito dal procuratore generale in base al decreto 14086, è un organo giudiziario indipendente composto da almeno sei giudici nominati dal procuratore generale in consultazione con la PCLOB, il segretario al Commercio e la direttrice dell’intelligence nazionale per un mandato rinnovabile di quattro anni. La nomina dei giudici da parte del procuratore generale si basa sui criteri utilizzati dall’esecutivo per valutare i candidati alla magistratura federale, tenendo conto dell’esperienza giudiziaria. Inoltre i giudici devono operare nel settore della giustizia (ossia essere membri attivi dell’ordine forense e abilitati a esercitare la professione legale) e avere un’esperienza adeguata in materia di protezione dei dati e di sicurezza nazionale. Il procuratore generale deve garantire che

almeno la metà dei giudici disponga di esperienza giudiziaria e che tutti i giudici siano autorizzati ad accedere a informazioni classificate relative alla sicurezza nazionale. Inoltre, i giudici non possono lavorare nel ramo esecutivo al momento della loro nomina o averci lavorato nei due anni precedenti. Durante il loro mandato presso il Tribunale del riesame non possono ricoprire funzioni o impieghi ufficiali all'interno del governo statunitense diversi da quello di giudici presso il Tribunale del riesame. L'indipendenza del processo decisionale è data da una serie di garanzie. In particolare, il ramo esecutivo (il procuratore generale e gli enti di intelligence) non possono ostacolare o influenzare indebitamente la verifica da parte del Tribunale del riesame, tenuto a pronunciarsi in modo imparziale e ad attenersi a un regolamento interno approvato a maggioranza. I suoi giudici possono essere destituiti esclusivamente dal procuratore generale e soltanto per giusta causa (condotta illecita, commissione di un reato, violazione della sicurezza, negligenza o incapacità), conformemente alle norme in materia di deontologia professionale e incapacità della magistratura (*Rules for Judicial-Conduct and Judicial-Disability Proceedings*)[53].

Le domande presentate al Tribunale del riesame sono esaminate da collegi di tre giudici, tra cui un presidente, che devono attenersi al codice deontologico dei giudici statunitensi (*Code of Conduct for U.S. Judges*). Ciascun collegio è assistito da un avvocato speciale, il quale ha accesso a tutte le informazioni relative al caso, comprese quelle classificate. L'avvocato speciale garantisce che gli interessi del reclamante siano rappresentati e che il collegio giudicante sia ben informato su tutte le questioni di diritto e di fatto pertinenti. Per meglio posizionarsi in merito a una domanda presentata al Tribunale del riesame, l'avvocato speciale può scrivere al reclamante chiedendo informazioni. Il Tribunale del riesame verifica le decisioni adottate dall'addetto CLP dell'ODNI, sia in relazione a un'eventuale violazione del diritto statunitense applicabile, sia in relazione alle misure correttive adeguate, basandosi almeno sul fascicolo dell'esame condotto dall'addetto CLP dell'ODNI, nonché su tutte le informazioni e le osservazioni fornite dal reclamante, dall'avvocato speciale o da un ente di intelligence. Un collegio del Tribunale del riesame ha accesso a tutte le informazioni necessarie per la verifica, che può ottenere tramite l'addetto CLP dell'ODNI.

A verifica terminata, il Tribunale del riesame può statuire che non vi sono prove di attività di intelligence dei segnali implicanti dati personali del reclamante oppure ritenere giuridicamente corrette e suffragate da prove sostanziali le decisioni dell'addetto CLP dell'ODNI o ancora pronunciare le sue proprie conclusioni qualora non concordi con quelle dell'addetto CLP dell'ODNI. In quest'ultimo caso la decisione del Tribunale prevale ed è vincolante per l'addetto CLP dell'ODNI e gli enti di intelligence.

In tutti i casi il Tribunale del riesame adotta una decisione a maggioranza ed emette un verdetto scritto. Se dalla verifica emerge una violazione delle disposizioni applicabili, nella decisione specifica le misure correttive adeguate, ad esempio cancellare i dati raccolti illecitamente e i risultati di consultazioni condotte impropriamente, riservare a personale adeguatamente formato l'accesso ai dati raccolti in modo lecito o richiamare relazioni di intelligence contenenti dati acquisiti o diffusi senza legittima autorizzazione. La decisione del Tribunale è vincolante e definitiva. Inoltre, se dalla verifica emerge una violazione da parte di

[53] Cfr. il decreto presidenziale 14086 e il regolamento del procuratore generale, come pure il sito del Tribunale del riesame, dove figura l'elenco dei giudici attuali con una breve presentazione della loro carriera: https://www.justice.gov/opcl/redress-data-protection-review-court.

un'autorità soggetta alla vigilanza della Corte FISA, il Tribunale deve fornire anche una relazione classificata al procuratore generale aggiunto per la sicurezza nazionale, a sua volta tenuto a segnalare la violazione alla Corte FISA, che può adottare ulteriori misure. Ogni decisione di un collegio del Tribunale del riesame è trasmessa all'addetto CLP dell'ODNI. Se la verifica è stata avviata a seguito di una domanda presentata dal reclamante, quest'ultimo viene informato dall'IFPDT, con risposta standard, se sono state rilevate violazioni tra quelle contemplate. In caso di violazioni viene informato delle misure correttive disposte. L'Ufficio per la tutela della sfera privata e le libertà civili del Dipartimento della giustizia tiene un archivio di tutte le informazioni esaminate e di tutte le decisioni adottate dal Tribunale del riesame, messe a disposizione dei futuri collegi come precedenti non vincolanti. Anche il Dipartimento del commercio tiene un archivio di tutte le persone che hanno presentato un reclamo. Per garantire maggiore trasparenza, almeno ogni cinque anni il Dipartimento del commercio deve contattare gli enti di intelligence interessati al fine di verificare se le informazioni relative a un esame da parte dell'addetto CLP dell'ODNI o a una verifica da parte del Tribunale del riesame sono state declassificate. In caso affermativo, l'interessato viene informato tramite l'autorità pubblica competente che può chiedere l'accesso alle informazioni ormai disponibili ai sensi del diritto applicabile.

Infine il corretto funzionamento di questo meccanismo di ricorso è soggetto a una valutazione periodica e indipendente effettuata nello specifico ogni anno dalla PCLOB, un organismo indipendente[54]. Nel contesto di tale valutazione, la PCLOB controlla tra l'altro se l'addetto CLP dell'ODNI e il Tribunale del riesame hanno trattato i reclami entro i termini stabiliti, se hanno ottenuto pieno accesso alle informazioni necessarie, se le garanzie sostanziali stabilite nel decreto presidenziale 14086 sono state adeguatamente prese in considerazione nella procedura di riesame e se la comunità dell'intelligence si sia pienamente conformata alle decisioni. La PCLOB presenta una relazione sull'esito della sua valutazione al presidente, al procuratore generale, alla direttrice dell'intelligence nazionale, ai capi dei singoli enti di intelligence, all'addetto CLP dell'ODNI e alle commissioni in materia di intelligence del Congresso; tale relazione viene poi resa pubblica in una versione non classificata. Il procuratore generale, la direttrice dell'intelligence nazionale, l'addetto CLP dell'ODNI e i capi degli enti di intelligence sono tenuti ad attuare o a soddisfare in altro modo tutte le raccomandazioni contenute nelle relazioni. Ogni anno la PCLOB certifica inoltre pubblicamente se il meccanismo di ricorso sta trattando o meno i reclami in linea con i requisiti stabiliti nel decreto presidenziale 14086.

Oltre al meccanismo specifico istituito in virtù del decreto presidenziale 14086, tutte le persone (indipendentemente dalla loro nazionalità o dal loro luogo di residenza) hanno la possibilità di adire anche i tribunali ordinari statunitensi. In particolare la FISA e una legge correlata offrono la possibilità di intentare una causa civile contro gli Stati Uniti per ottenere un risarcimento pecuniario quando le informazioni personali sono state usate o divulgate in maniera illecita e dolosa, di procedere contro funzionari statunitensi per ottenere un risarcimento pecuniario e di contestare la liceità della sorveglianza quando il governo degli Stati Uniti intende usare o divulgare contro l'interessato le informazioni raccolte o ricavate dalla sorveglianza elettronica in un procedimento giudiziario o amministrativo negli Stati Uniti.

[54] Il decreto presidenziale 14086 invita la PCLOB a condurre una valutazione annuale del funzionamento del meccanismo di ricorso. La PCLOB ha accettato di effettuare tali valutazioni (cfr. Oversight Projects - PCLOB).

Un rimedio giuridico più generale è offerto dalla normativa sulla procedura amministrativa, in base alla quale chiunque subisca un illecito, un danno o un torto a causa dell'azione di un ente pubblico può ricorrere al sindacato giurisdizionale.

In virtù della normativa sulla trasparenza[55], chiunque ha il diritto di accedere alle informazioni in possesso delle autorità federali, anche a quelle contenenti dati personali. Tale accesso può facilitare anche l'avvio di procedimenti dinanzi ai tribunali ordinari, in particolare riguardo alla legittimazione ad agire. Gli enti possono non divulgare le informazioni che rientrano in determinate eccezioni elencate, tra cui le informazioni classificate relative alla sicurezza nazionale e quelle relative a indagini di autorità penali. I reclamanti insoddisfatti della decisione hanno la possibilità di impugnarla chiedendo una verifica amministrativa e, successivamente, giudiziaria dinanzi ai tribunali federali.

5 Altri criteri

5.1 Impegni internazionali

È importante tenere conto degli impegni internazionali, non solo quelli in materia di protezione dei dati, ma anche, ad esempio, quelli risultanti dagli accordi sullo scambio di informazioni.

Gli Stati Uniti hanno aderito a diversi quadri internazionali comportanti impegni in materia di tutela della sfera privata e dei diritti umani in generale.

In quanto membri dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), gli Stati Uniti sono coinvolti nei lavori sulla governance dei dati e la tutela della sfera privata. Si sono impegnati a rispettare il quadro di protezione della sfera privata stabilito dall'OCSE, in particolare le linee guida sulla protezione della sfera privata[56]. Inoltre hanno contribuito attivamente a elaborare la dichiarazione che disciplina l'accesso delle autorità pubbliche ai dati personali detenuti dal settore privato[57].

Gli Stati Uniti hanno aderito alla Convenzione sulla cibercriminalità[58] del Consiglio d'Europa (Convenzione di Budapest).

Sono anche membri della Cooperazione economica Asia-Pacifico (APEC) e hanno aderito al quadro sulla protezione della sfera privata dell'APEC[59].

---

[55] Cfr. titolo 5 del Codice degli Stati Uniti

[56] Consultabile qui: OECD Legal Instruments

[57] Consultabile qui: OECD Legal Instruments

[58] Consultabile qui: Convenzione sulla cibercriminalità (coe.int); RS **0.311.43**

[59] Consultabile qui: APEC Privacy Framework

La Commissione federale del commercio è membro accreditato dell'Assemblea mondiale della sfera privata (*Global Privacy Assembly*)[60] mentre la PCLOB e l'addetto CLP del Dipartimento della giustizia sono osservatori.

Anche gli accordi bilaterali o multilaterali di libero scambio o gli accordi sul commercio digitale possono essere rilevanti se contengono clausole sulla protezione dei dati personali e sui flussi transfrontalieri di dati. Al riguardo si possono citare in particolare l'accordo di libero scambio tra Stati Uniti, Messico e Canada e l'accordo tra Stati Uniti e Giappone[61]. Gli Stati Uniti stanno inoltre partecipando ai negoziati per un accordo sul commercio digitale, attualmente in corso su iniziativa congiunta dei membri dell'OMC[62].

5.2 Stato di diritto

Gli Stati Uniti sono una repubblica federale formata da 50 Stati, ai quali si aggiungono altri territori non considerati Stati. La forma di governo è la democrazia.

La politica estera, l'esercito, le attività di intelligence e il commercio estero sono di competenza del Governo federale. I 50 Stati federati sono competenti per altri settori, tra cui la giustizia e l'istruzione.

La Costituzione degli Stati Uniti, risalente al 1787, è la più antica costituzione moderna ancora in vigore. Sancisce la separazione dei poteri: il potere legislativo è esercitato dal Congresso, che si compone di due camere, il Senato e la Camera dei rappresentanti; il potere esecutivo è assicurato dal presidente e dal vicepresidente degli Stati Uniti; la Corte suprema è il massimo organo del potere giudiziario e in quanto tale esamina i casi trattati dai tribunali federali di grado inferiore, nonché i casi vertenti su questioni di diritto federale o sull'interpretazione della Costituzione. L'indipendenza del potere giudiziario è garantita dalla Costituzione.

5.3 Diritti umani

Il criterio del rispetto dei diritti umani va esaminato tenendo conto dell'intero quadro giuridico di uno Stato, soprattutto nell'ottica della tutela da ingerenze sproporzionate nella sfera privata.

La Costituzione degli Stati Uniti elenca alcuni diritti fondamentali che le autorità federali o statali non possono violare e che sono applicati dal potere giudiziario. Tali diritti corrispondono in parte a quelli contenuti nella dichiarazione universale dei diritti umani[63],

---

[60] Cfr. Global Privacy Assembly

[61] Cfr. Digital Trade & E-Commerce FTA Chapters | United States Trade Representative (ustr.gov)

[62] Cfr. WTO | Joint Initiative on E-Commerce

[63] Consultabile qui: Dichiarazione universale dei diritti umani

come la libertà di espressione, la libertà di credo, la libertà di riunione, l'uguaglianza e le garanzie procedurali.

Alcune decisioni della Corte Suprema hanno inoltre riguardato la protezione degli interessi relativi alla sfera privata in diversi contesti, in particolare quello del quarto emendamento, che stabilisce un diritto contro le perquisizioni e i sequestri irragionevoli da parte del governo[64].

6 Conclusione

Come si può evincere da quanto illustrato, è istituito un quadro giuridico che disciplina l'accesso da parte delle autorità penali o delle autorità di sicurezza nazionale degli Stati Uniti ai dati personali trasferiti dalla Svizzera a organizzazioni certificate, definisce le condizioni alle quali l'accesso è possibile e garantisce che l'accesso e l'ulteriore utilizzo dei dati sia limitato a quanto necessario e proporzionato per raggiungere l'interesse pubblico perseguito. Gli interessati hanno a disposizione vari rimedi giuridici per far valere queste garanzie, che sono pertanto efficaci.

Alla luce della presente valutazione, l'Ufficio federale di giustizia conclude che gli Stati Uniti garantiscono un livello di protezione adeguato per i dati personali che un titolare del trattamento o un responsabile del trattamento in Svizzera trasferisce a organizzazioni certificate negli Stati Uniti nell'ambito del DPF CH-USA.

Se tale valutazione sarà approvata dal Consiglio federale, i titolari del trattamento e i responsabili del trattamento in Svizzera potranno trasferire dati personali alle organizzazioni certificate negli Stati Uniti senza dover chiedere ulteriori garanzie (cfr. art. 16 cpv. 1 LPD).

Link ai testi di riferimento

- Principi, compresi quelli supplementari, del quadro commerciale tra la Svizzera e gli Stati Uniti sulla protezione dei dati per le organizzazioni certificate; lettere di conferma degli impegni assunti, redatte dalle seguenti autorità: Dipartimento della giustizia, Dipartimento del commercio (*Secretary of Commerce* e ODNI), Amministrazione internazionale del commercio, Commissione federale del commercio e Dipartimento dei trasporti: https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3
- Decreto presidenziale 14086 del 7 ottobre 2022: https://www.state.gov/executive-order-14086-policy-and-procedures
- Regolamento del procuratore generale degli Stati Uniti (*U.S. Attorney General*) che istituisce il Tribunale del riesame in materia di protezione dei dati, pubblicato il 7 ottobre 2022: https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court
- Direttiva 126 della comunità dell'intelligence, emanata dall'ODNI il 6 dicembre 2022: https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf

[64] Cfr. *Griswold v. Connecticut, 381 US 479 (1965), consultabile qui:* Griswold v. Connecticut: 381 US 479 (1965): Justia US Supreme Court Center

- Designazione della Svizzera del 7 giugno 2024 come Stato avente accesso al meccanismo di ricorso a due livelli, compreso il Tribunale per il riesame in materia di protezione dei dati: https://www.justice.gov/opcl/media/1355326/dl?inline, cfr. anche https://www.justice.gov/opcl/executive-order-14086