COMMISSIONE
EUROPEA

Bruxelles, 9.10.2024
COM(2024) 451 final

RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

sul primo riesame periodico del funzionamento della decisione di adeguatezza relativa al quadro UE-USA per la protezione dei dati personali

1. PRIMO RIESAME PERIODICO – CONTESTO, PREPARAZIONE E PROCESSO

Nella decisione del 10 luglio 2023 (la "decisione di adeguatezza"), la Commissione ha constatato che il quadro UE-USA per la protezione dei dati personali (DPF) garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea a organizzazioni presenti negli Stati Uniti d'America[1]. La decisione di adeguatezza prescrive alla Commissione di effettuare riesami periodici, il primo dei quali dovrebbe aver luogo dopo un anno dalla data di notifica della decisione di adeguatezza agli Stati membri. Il primo riesame si conclude con la presente relazione.

Come previsto dal considerando 211 della decisione di adeguatezza, il presente primo riesame, che ha avuto luogo dopo il primo anno di funzionamento del nuovo quadro, è stato orientato a verificare se tutti gli elementi previsti dal quadro siano stati attuati e funzionino efficacemente. Il riesame ha riguardato tutti gli aspetti del funzionamento del quadro, anche alla luce degli sviluppi giuridici intervenuti dopo l'adozione della decisione di adeguatezza.

In preparazione del riesame, la Commissione ha raccolto informazioni dai portatori di interessi pertinenti, in particolare dalle organizzazioni non governative (ONG) con competenze in materia di diritti e tutela della vita privata nell'ambiente digitale[2], dalle organizzazioni certificate ai sensi del DPF, attraverso le loro associazioni di categoria[3], nonché dalle autorità statunitensi che intervengono nell'attuazione del quadro. La Commissione ha inoltre raccolto i riscontri del grande pubblico attraverso uno specifico invito a presentare contributi sul portale "Di' la tua"[4].

Il 18 e 19 luglio 2024 si è tenuta a Washington D.C. una riunione di riesame, inaugurata dal commissario UE per la Giustizia e i consumatori Didier Reynders e dalla segretaria al Commercio degli Stati Uniti d'America Gina Raimondo[5].

---

[1] Decisione di esecuzione (UE) 2023/1795 della Commissione, del 10 luglio 2023, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali.

[2] La Commissione ha inviato un questionario a nove ONG (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology) concentrandosi sugli sviluppi pertinenti del quadro giuridico statunitense, sui meccanismi di vigilanza e di controllo dell'attuazione e sul funzionamento dei meccanismi di ricorso. Il 9 luglio 2024 i servizi della Commissione e i rappresentanti dell'EDPB hanno inoltre tenuto una riunione online con tali ONG.

[3] La Commissione ha inviato un questionario a nove associazioni di categoria (associazione dell'industria del software e dell'informazione, camera di commercio degli Stati Uniti, consiglio per l'industria delle tecnologie dell'informazione, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, associazione dell'industria dei computer e delle comunicazioni, Engine), concentrandosi sull'esperienza delle imprese certificate ai sensi del DPF, in particolare sul processo di certificazione, sulle misure adottate per conformarsi ai principi del DPF, sui meccanismi per la gestione delle richieste e dei reclami delle persone, ecc.

[4] I commenti ricevuti sono disponibili al seguente indirizzo: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_it.

[5] La riunione di riesame è stata organizzata per argomento e ciascun punto all'ordine del giorno specifico è stato introdotto da una breve presentazione da parte dell'autorità statunitense competente, del rappresentante dell'UE o dell'organizzazione, cui è seguita una sessione dettagliata di domande e risposte. Gli "aspetti commerciali" del quadro (ossia l'applicazione e il rispetto degli obblighi applicabili alle imprese certificate ai sensi del DPF) sono stati trattati il primo giorno, mentre le questioni relative all'accesso ai dati personali da parte di pubbliche amministrazioni sono state discusse il secondo giorno.

Per quanto riguarda l'UE, il riesame è stato condotto da rappresentanti della direzione generale della Giustizia e dei consumatori della Commissione europea, insieme a cinque rappresentanti designati dal comitato europeo per la protezione dei dati (EDPB) e provenienti da diverse autorità nazionali di protezione dei dati e dal Garante europeo della protezione dei dati[6]. Per quanto riguarda gli Stati Uniti, hanno partecipato rappresentanti del Dipartimento del Commercio, del Dipartimento di Stato, della Commissione federale del Commercio (FTC), del Dipartimento dei Trasporti (DOT), dell'Ufficio del direttore dell'intelligence nazionale (ODNI), del Dipartimento della Giustizia, dell'ispettore generale della comunità dell'intelligence, nonché membri dell'Autorità per la tutela della vita privata e delle libertà civili (PCLOB). Inoltre, durante le pertinenti sessioni di riesame, hanno fornito informazioni rappresentanti delle organizzazioni che offrono servizi indipendenti di composizione delle controversie e dell'American Arbitration Association. Il riesame è stato inoltre alimentato dalle presentazioni delle organizzazioni certificate ai sensi del DPF sulle modalità con cui le imprese rispettano i requisiti del quadro.

Le constatazioni della Commissione sono state alimentate anche da documenti disponibili al pubblico, quali decisioni giudiziarie, norme e procedure di attuazione delle autorità statunitensi competenti, relazioni e studi di organizzazioni non governative, relazioni sulla trasparenza pubblicate dalle imprese certificate ai sensi del DPF, relazioni annuali di organi di vigilanza indipendenti e articoli dei media.

2. CONSTATAZIONI

2.1. Aspetti commerciali

2.1.1. Il processo di certificazione

Per poter ricevere dati personali trasferiti dall'UE in virtù del DPF, un'impresa statunitense deve certificare, e in seguito certificare nuovamente su base annuale, presso il Dipartimento del Commercio la propria adesione a requisiti specifici in materia di protezione dei dati (i "principi del DPF"). Ai fini dell'ottenimento della certificazione un'impresa deve assoggettarsi ai poteri di indagine e di esecuzione della FTC o del DOT, impegnarsi pubblicamente a rispettare i principi del DPF, divulgare la propria politica della privacy e dare loro attuazione integrale[7]. Prima di finalizzare una certificazione, il Dipartimento del Commercio verifica se l'impresa abbia soddisfatto tutti i requisiti di certificazione[8].

Nella riunione di riesame, il Dipartimento del Commercio ha spiegato che, in questo primo anno di esistenza del DPF, l'attenzione è stata posta sulla messa a punto del processo di certificazione, che comprende lo sviluppo di appositi strumenti informatici, l'aggiornamento delle procedure, il dialogo con le imprese e lo svolgimento di altre attività di sensibilizzazione. Alla data della riunione di riesame più di 2 800 imprese hanno ottenuto la certificazione ai sensi del DPF. Ciò significa che, nel primo anno di funzionamento[9], un maggior numero di imprese ha ottenuto la certificazione ai sensi del DPF rispetto al regime precedente, lo scudo per la privacy. In base alle informazioni fornite dal Dipartimento del Commercio, il 70 % dei

[6] I rappresentanti della Commissione e dell'EDPB si sono riuniti il 12 giugno e il 10 luglio 2024 per preparare il riesame, discutere i contributi ricevuti e individuare gli aspetti che richiedono ulteriori informazioni e chiarimenti.
[7] Allegato I, parte I, punto 2, della decisione di adeguatezza.
[8] Allegato III della decisione di adeguatezza.
[9] Nel periodo corrispondente erano state certificate nell'ambito dello scudo per la privacy 2 400 imprese.

partecipanti è costituito da PMI e un gran numero di imprese aderenti al DPF (47 %) rientra nel settore dell'informazione, della comunicazione e della tecnologia. Inoltre il 60 % delle imprese è certificato esclusivamente per i dati non relativi alle risorse umane, il 2,5 % è certificato esclusivamente per i dati relativi alle risorse umane e il 37,5 % è certificato per entrambi i tipi di dati.

Il Dipartimento del Commercio ha adottato le procedure necessarie per la gestione delle domande delle imprese. Le imprese devono presentare le loro domande di certificazione sul sito web del Dipartimento del Commercio dedicato al DPF (https://www.dataprivacyframework.gov/), che contiene informazioni sulle modalità di adesione al DPF[10] e sugli obblighi delle imprese ai sensi del quadro[11]. Una squadra specifica del Dipartimento del Commercio, sotto la responsabilità di un direttore del quadro per la protezione dei dati personali, è competente per tutti gli aspetti relativi alla gestione e all'amministrazione del DPF, compresi il processo di certificazione e il controllo della conformità. Ogni domanda è assegnata a uno specifico membro del personale che rimane responsabile per quanto riguarda l'impresa interessata durante l'intero processo di certificazione.

Per essere certificate ai sensi del quadro, le imprese presentano la loro domanda, corredata di un progetto di politica della privacy. Il Dipartimento del Commercio ne verifica la conformità ai requisiti pertinenti del DPF. Quando le organizzazioni desiderano certificare diversi soggetti all'interno di un gruppo aziendale (ad esempio diverse filiali), il Dipartimento del Commercio chiede ed esamina una politica della privacy globale, che indichi chiaramente tutti i soggetti cui si applica, oppure politiche distinte per ciascun soggetto. Il Dipartimento del Commercio verifica inoltre presso il meccanismo di ricorso indipendente[12] indicato nella domanda se l'organizzazione vi si è effettivamente registrata. Per le imprese che scelgono il comitato delle autorità di protezione dei dati (ad esempio perché trattano dati relativi alle risorse umane), il Dipartimento del Commercio verifica se l'impresa abbia corrisposto i contributi spese richiesti per avvalersi del comitato. Ove necessario, il Dipartimento del Commercio verifica altresì se il richiedente rientra nella giurisdizione della FTC o del DOT (ed è pertanto ammissibile all'adesione al DPF).

Se tutte le condizioni sono soddisfatte, il Dipartimento del Commercio informa l'organizzazione che può pubblicare la propria politica della privacy con riferimento al DPF sul suo sito web. Una volta che la politica della privacy è pubblica, il Dipartimento del Commercio conferma la certificazione e inserisce l'impresa nell'elenco degli aderenti al DPF sul proprio sito web. Il DPF può essere utilizzato per ricevere dati personali dall'UE a partire dalla data in cui il Dipartimento del Commercio inserisce l'organizzazione in tale elenco[13].

Come spiegato nel corso della riunione di riesame, i controlli effettuati finora dal Dipartimento del Commercio hanno portato al rigetto di 33 domande, in quanto non soddisfacevano i requisiti del DPF. In generale, il Dipartimento del Commercio collabora con l'impresa per porre rimedio a eventuali carenze. Qualora rilevi carenze, il Dipartimento del Commercio informa l'impresa che deve porvi rimedio e che in caso di mancata risposta entro un determinato termine, o di

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Meccanismi di composizione delle controversie del settore privato atti a consentire d'istruire e dirimere, senza costi per la persona, qualsiasi reclamo da questa presentato o qualsiasi controversia insorta.

[13] Allegato I, parte I, punto 3, della decisione di adeguatezza.

mancato completamento dell'autocertificazione secondo le procedure del Dipartimento del Commercio, la domanda sarà considerata abbandonata. Se la certificazione iniziale non viene completata/modificata entro 12 mesi, il Dipartimento del Commercio la considera abbandonata.

Il termine per la ricertificazione annuale è specificato nell'elenco degli aderenti al DPF per ciascuna impresa. Per ricordare alle imprese la necessità di richiedere la ricertificazione, il Dipartimento del Commercio ha creato un sistema che ricorda che la certificazione sta per scadere. Le organizzazioni ricevono un sollecito un mese prima, poi due settimane prima e infine un giorno prima della scadenza. Quelle che hanno lasciato scadere la loro certificazione sono depennate dall'elenco degli aderenti al DPF. Come descritto nell'allegato III della decisione di adeguatezza, il Dipartimento del Commercio dispone sul proprio sito web di una sezione specifica in cui sono elencate le organizzazioni statunitensi che non partecipano più attivamente, con indicazione dei rispettivi motivi (ad esempio scadenza o abbandono) per cui le imprese interessate sono state depennate dall'elenco ("elenco di imprese non attive"). Quando le organizzazioni sono depennate dall'elenco degli aderenti al DPF per aver lasciato scadere la propria certificazione, il Dipartimento del Commercio le contatta al fine di verificare se desiderano abbandonare il regime oppure ricertificarsi e, in quest'ultimo caso, verificare che durante la scadenza abbiano applicato i principi del DPF ai dati personali ricevuti nell'ambito di tale quadro e chiarire quali misure adotteranno per affrontare le questioni in sospeso che hanno ritardato la ricertificazione. Quando le imprese notificano di voler abbandonare il DPF, il Dipartimento del Commercio chiede loro di confermare se intendono restituire o cancellare i dati ricevuti nell'ambito del DPF; conservarli e continuare ad applicare i principi del DPF a tali dati (il che deve essere confermato annualmente); oppure conservarli e introdurre altre tutele (come le clausole contrattuali tipo adottate dalla Commissione europea).

I riscontri ricevuti dalle associazioni di categoria e dalle imprese indicano che le imprese certificate ai sensi del DPF hanno adottato una serie di misure per garantire il rispetto dei principi del DPF. Ad esempio, per rispettare il *principio su ricorso, controllo e responsabilità*, le organizzazioni hanno effettuato controlli interni mediante autovalutazione o attraverso una verifica esterna della conformità. I due meccanismi di ricorso indipendenti del settore privato che hanno partecipato alla riunione di riesame hanno spiegato di effettuare anche un esame esterno della conformità attraverso la revisione delle politiche della privacy, e uno di essi ha spiegato che prevede anche verifiche e controlli a campione, concentrandosi ad esempio sui principi sull'*accesso*, sulla *scelta* e sul *trasferimento successivo*. Inoltre le imprese certificate hanno elaborato programmi interni di conformità e meccanismi di vigilanza, formato i dipendenti, attuato meccanismi per consentire alle persone di esercitare i loro diritti, effettuato valutazioni dell'impatto sulla vita privata e riesaminato i contratti esistenti.

2.1.2. Controllo della conformità, casi di millantata adesione e applicazione

Ai sensi del DPF, il Dipartimento del Commercio è responsabile del controllo del rispetto dei principi del DPF attraverso l'uso di diversi strumenti, tra cui controlli d'ufficio (di propria iniziativa), controlli a campione ad hoc e questionari sulla conformità. Ciò comprende la ricerca e il trattamento dei casi di millantata adesione al quadro, ad esempio tramite ricerche su internet[14].

[14] Cfr. l'allegato III della decisione di adeguatezza. Possono verificarsi casi di millantata adesione, ad esempio, quando un'impresa dichiara di partecipare al DPF e non ha mai avviato il processo di certificazione, o lo ha avviato ma non lo ha completato o ha lasciato scadere la certificazione.

Per controllare il rispetto dei principi da parte delle imprese aderenti al DPF, nell'ultimo anno il Dipartimento del Commercio si è basato principalmente su ricerche ad hoc sul web e su controlli sui media (sociali). Il Dipartimento del Commercio ha riferito di non aver individuato problemi di conformità ai principi del DPF in questo primo anno e di non aver deferito alcuna impresa all'FTC o al DOT per l'adozione di eventuali azioni coercitive. Ha inoltre istituito un apposito punto di contatto per agevolare la cooperazione con le autorità di protezione dei dati e ricevere i reclami sporti dalle persone e i deferimenti da parte di altre autorità (ad esempio le autorità di protezione dei dati o l'FTC). Tuttavia nel corso dell'ultimo anno non sono pervenuti deferimenti né reclami. Mentre in questo primo anno di funzionamento del DPF si è posto l'accento sulla messa a punto del quadro e del processo di certificazione, nella riunione di riesame il Dipartimento del Commercio ha spiegato che intende effettuare controlli di conformità con strumenti automatizzati per realizzarli in modo più sistematico e attualmente sta sviluppando gli strumenti informatici necessari a tal fine.

La Commissione prende atto che, in questo primo anno, il Dipartimento del Commercio ha dovuto concentrare i propri sforzi sull'istituzione del quadro e sul processo di certificazione. In futuro è importante che il Dipartimento del Commercio intensifichi gli sforzi per controllare e verificare il rispetto dei principi, il che è necessario per garantire un livello costantemente elevato di conformità al quadro e per individuare le situazioni in cui si rendono necessarie ulteriori azioni coercitive, compresi eventuali casi di millantata adesione da parte delle imprese. A tale riguardo, la Commissione accoglie con favore il fatto che il Dipartimento del Commercio abbia confermato l'intenzione di sviluppare e utilizzare strumenti (automatizzati) per individuare in modo più efficace e sistematico le questioni in materia di conformità e i casi di millantata adesione e ritiene che ciò dovrebbe rientrare in uno sforzo più ampio volto a fare un uso maggiore dei diversi strumenti a sua disposizione (ad esempio controlli a campione, questionari di verifica della conformità, richieste di informazioni, ecc.), anche per verificare la conformità ai requisiti specifici previsti dal DPF[15].

Le organizzazioni aderenti al DPF sono soggette alla competenza giurisdizionale dell'FTC e del DOT. Durante la riunione di riesame, il DOT ha confermato di avere predisposto tutti i processi per adottare le opportune azioni coercitive. Ha inoltre spiegato che pochissime imprese soggette alla sua competenza giurisdizionale hanno aderito al DPF (ossia alcuni rivenditori che fanno servizio di biglietteria, ma nessuna compagnia aerea). L'FTC ha confermato di verificare sistematicamente le violazioni del DPF in ciascuna delle sue indagini sulla privacy. Finora l'FTC non ha ricevuto alcun deferimento da altre autorità. Ha ricevuto alcuni reclami che menzionavano il DPF, sebbene due di essi riguardassero imprese inserite nell'"elenco delle imprese non attive", due riguardassero imprese che non partecipavano al quadro e uno non riguardasse dati personali trasferiti dall'UE. Al momento della stesura della presente relazione l'FTC non aveva emesso decisioni per imporre il rispetto del DPF, sebbene abbia confermato che diverse imprese certificate ai sensi del DPF sono attualmente oggetto di indagine.

La Commissione accoglie con favore il fatto che l'FTC controlli sistematicamente le violazioni del DPF in tutte le sue indagini sulla privacy. Poiché il mantenimento dell'efficacia del DPF dipende dalla sua rigorosa applicazione, si prevede che l'FTC eserciterà ulteriormente i suoi poteri di indagine nell'ambito del quadro, anche conducendo in modo proattivo azioni di

[15] Ad esempio, per quanto riguarda i trasferimenti successivi, avvalendosi della possibilità prevista dal principio 3, lettera b), del DPF di richiedere un sunto o un estratto rappresentativo delle pertinenti disposizioni sulla tutela della vita privata contenute nei contratti per i trasferimenti successivi.

indagine a tappeto incentrate sul rispetto dei requisiti specifici del DPF e/o su determinati settori.

2.1.3. Gestione dei reclami

Il DPF offre ai cittadini dell'UE diverse possibilità di ricorso per i casi di mancato rispetto dei principi del DPF da parte di organizzazioni certificate[16]. Ciò comprende la ricerca di una composizione attraverso contatti diretti con un'organizzazione aderente al DPF, che deve fornire una risposta alla persona interessata entro 45 giorni. La persona può anche sporgere reclamo presso un meccanismo di ricorso indipendente designato da un'organizzazione per esaminare e risolvere i casi di reclamo. A seconda delle circostanze, potrebbe trattarsi di un organo di composizione alternativa delle controversie o di un'autorità di protezione dei dati[17]. Infine, come extrema ratio nel caso in cui gli altri mezzi di ricorso disponibili non abbiano offerto una soluzione soddisfacente per il reclamo sporto dall'interessato, la persona può chiedere l'arbitrato vincolante del collegio del DPF UE-USA.

2.1.3.1. Gestione dei reclami da parte delle imprese

Le risposte delle associazioni di categoria e delle imprese ai questionari inviati dalla Commissione indicano che le imprese certificate ai sensi del DPF hanno ricevuto quasi nessun reclamo da parte di persone in merito al mancato rispetto dei principi del DPF. Allo stesso tempo, le imprese hanno messo in atto diversi meccanismi e strumenti per consentire alle persone di esercitare i loro diritti e presentare reclami, anche tramite moduli online, posta elettronica e per telefono.

2.1.3.2. *Meccanismi di ricorso indipendenti*

I riscontri ricevuti durante la riunione di riesame e le informazioni fornite dalle associazioni di categoria indicano che è stato presentato un numero molto basso di reclami ai meccanismi di ricorso indipendenti. Tra i meccanismi di ricorso indipendenti scelti dalle imprese figurano BBB National Programs, JAMS, TRUSTe e VeraSafe. Il DPF prevede che i meccanismi di ricorso indipendenti pubblichino una relazione annuale contenente statistiche aggregate sull'utilizzo dei loro servizi di composizione delle controversie. Al momento dell'adozione della presente relazione, tutti i meccanismi di ricorso indipendenti interessati avevano pubblicato le loro relazioni annuali[18].

---

[16] Cfr. la sezione 2.4 della decisione di adeguatezza.

[17] Le organizzazioni aderenti al DPF sono tenute a cooperare con l'autorità di protezione dei dati per l'esame e la risoluzione del caso di reclamo, se questo riguarda il trattamento di dati sulle risorse umane raccolti nel contesto di un rapporto di lavoro oppure se l'organizzazione ha accettato volontariamente di essere sottoposta alla supervisione delle autorità di protezione dei dati.

[18] ANA - https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs - https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA - https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights association https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS - https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services - https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution - https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;

Inoltre, nel corso della riunione di riesame, BBB e VeraSafe hanno presentato in dettaglio le loro attività dell'ultimo anno. Hanno segnalato un aumento del numero di imprese partecipanti che scelgono i loro servizi rispetto ai regimi precedenti e hanno indicato di aver ricevuto alcuni reclami, sebbene la stragrande maggioranza non fosse ammissibile. Ad esempio, BBB ha ricevuto 87 reclami da cittadini dell'UE, di cui solo due ammissibili alla composizione. Sebbene BBB abbia spiegato che i reclami sono gestiti generalmente entro cinque giorni lavorativi in media, quei due reclami sono stati infine archiviati a causa della mancata risposta da parte degli interessati. VeraSafe ha ricevuto 26 reclami, di cui sei ammissibili alla composizione. Due di quelli riguardanti richieste di accesso e cancellazione sono stati risolti, mentre due sono rimasti in sospeso e due sono stati ritirati o archiviati a causa della mancata risposta da parte dell'interessato. Entrambi i meccanismi di ricorso indipendenti hanno spiegato che intendono rispondere ai reclami nella lingua dell'interessato.

Quando trattano dati relativi alle risorse umane trasferiti dall'UE, le imprese aderenti al DPF sono obbligate a scegliere le autorità di protezione dei dati dell'UE come meccanismo di ricorso indipendente per quanto riguarda tali dati, mentre sono libere di farlo o meno per gli altri tipi di dati personali trasferiti in virtù del DPF. Di fatto, al momento del riesame oltre la metà delle imprese certificate ai sensi del DPF ha optato per questa soluzione[19], che è ben accetta. Dall'adozione della decisione di adeguatezza, l'EDPB ha adottato il regolamento interno per il "comitato informale delle autorità di protezione dei dati dell'UE". Il comitato è competente a fornire un parere vincolante alle organizzazioni statunitensi nei casi di reclami irrisolti nell'ambito del DPF sporti da persone in merito al trattamento dei dati personali trasferiti dall'UE nell'ambito del DPF. Conformemente al suo regolamento interno, il comitato è costituito da un'autorità di protezione dei dati che funge da autorità di protezione dei dati capofila e da altre autorità di protezione dei dati designate come co-esaminatori[20]. Esso fornisce un parere vincolante entro 60 giorni dal ricevimento di un reclamo nell'ambito del DPF. L'EDPB ha inoltre pubblicato un modello di modulo di reclamo per la presentazione di reclami alle autorità di protezione dei dati[21], nonché "domande frequenti per i cittadini europei"[22] e le imprese europee[23] sul DPF. Al momento del riesame il comitato non aveva ricevuto alcun reclamo.

2.1.3.3. Il meccanismo di arbitrato vincolante

Il Centro internazionale per la composizione delle controversie (*International Centre for Dispute Resolution*, ICDR), che è la divisione internazionale dell'*American Arbitration Association*, è stato selezionato dal Dipartimento del Commercio per amministrare il meccanismo arbitrale vincolante. A seguito dell'adozione della decisione di adeguatezza, il

VeraSafe - https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Poco dopo la data della riunione di riesame, il sito web del DPF ha indicato che 1 511 dei 2 892 partecipanti disponevano di un'autorità di protezione dei dati dell'UE come meccanismo di ricorso.

[20] Il 17 aprile 2024 l'EDPB ha adottato il regolamento interno del "comitato informale delle autorità di protezione dei dati dell'UE" conformemente al quadro UE-USA per la protezione dei dati personali. È consultabile al seguente indirizzo: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.

Dipartimento del Commercio, insieme alla Commissione, ha selezionato 11 arbitri con esperienza nel settore della tutela della vita privata e provenienti da contesti diversi, tra cui arbitrato, magistratura, mondo accademico e società civile[24]. Inoltre le norme arbitrali[25] per il collegio del DPF e un codice di condotta per gli arbitri[26] sono stati adottati e sono tutti disponibili sul sito web dell'ICDR. Al momento del riesame, il meccanismo di arbitrato non era ancora stato attivato da cittadini dell'UE.

2.1.4. Orientamento, cooperazione e sensibilizzazione

Dall'entrata in vigore del DPF, il Dipartimento del Commercio ha svolto varie attività di sensibilizzazione organizzando campagne informative itineranti, webinar e conferenze; rivolgendosi alle associazioni di categoria e interagendo direttamente con più di 3 000 imprese per fornire informazioni sul DPF. Ha inoltre pubblicato orientamenti, anche sotto forma di domande frequenti rivolte alle persone nonché alle imprese dell'UE e degli Stati Uniti[27]. A sua volta l'EDPB ha elaborato moduli di reclamo e domande frequenti rivolte a persone e imprese. Analogamente, la Commissione ha pubblicato una serie di domande e risposte e una scheda informativa sul DPF al momento dell'adozione della sua decisione di adeguatezza[28].

Nel contempo, dalla riunione di riesame è emerso che sono necessari ulteriori lavori per sensibilizzare i cittadini e fornire orientamenti alle imprese. I contributi ricevuti dalle imprese e dai meccanismi di ricorso indipendenti e il bassissimo numero di reclami suggeriscono che le persone potrebbero non essere sempre consapevoli dei loro diritti e/o del meccanismo per esercitarli. Durante la riunione di riesame, il Dipartimento del Commercio ha espresso interesse a collaborare con le autorità di protezione dei dati dell'UE per sensibilizzare i cittadini dell'UE in merito al quadro. La Commissione incoraggia tali iniziative e sta inoltre adottando misure per informare le persone in modo più adeguato, anche fornendo ulteriori informazioni sul DPF sul proprio sito web, ad esempio inserendo link e riferimenti ai pertinenti documenti di orientamento adottati dall'EDPB, dal Dipartimento del Commercio e da altre autorità statunitensi.

Per quanto riguarda gli orientamenti sui principi del DPF, durante la riunione di riesame i rappresentanti dell'EDPB hanno convenuto di cooperare nei prossimi mesi per fornire ulteriori chiarimenti sulla nozione di dati relativi alle risorse umane ai sensi del DPF e sugli obblighi specifici che si applicano al trattamento di tali dati. Sono stati esaminati diversi elementi da includere in tali orientamenti. Ad esempio, gli orientamenti potrebbero riguardare alcuni scenari pratici in cui i dati sui dipendenti sarebbero trattati nell'ambito del DPF (ad esempio da un fornitore di servizi cloud) e potrebbero spiegare per tali scenari quali obblighi del DPF sarebbero pertinenti. Inoltre potrebbero suggerire alle imprese che ricevono i dati sull'impiego di cittadini dell'UE (ma che non utilizzano necessariamente tali dati nel contesto di un rapporto di lavoro) di scegliere il comitato delle autorità di protezione dei dati come meccanismo di ricorso indipendente. Ciò garantirebbe a tali persone la possibilità di rivolgersi a un'autorità che è "vicina a casa" e che, in caso di necessità, ha maggiore dimestichezza con le leggi nazionali applicabili ai dati relativi alle risorse umane.

---

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Cfr. ad esempio https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

Inoltre un aspetto specifico in cui sembra che sarebbero utili ulteriori orientamenti (anche sulla base dei contributi ricevuti dalle associazioni di categoria) riguarda i requisiti del DPF per i trasferimenti successivi. Il Dipartimento del Commercio ha indicato inoltre che sarebbe opportuno valutare se alcuni settori possano beneficiare di ulteriori orientamenti sull'applicazione dei principi del DPF alle loro attività, ad esempio il settore della ricerca sanitaria e dei servizi finanziari.

La Commissione accoglie con favore la disponibilità di entrambe le parti a elaborare orientamenti e si aspetta che i lavori sui temi summenzionati inizino a breve.

Più in generale, sono stati istituiti diversi meccanismi per garantire gli scambi e la cooperazione tra le autorità statunitensi e le autorità di protezione dei dati, anche attraverso la nomina di punti di contatto specifici all'interno dell'FTC e del Dipartimento del Commercio per gestire le richieste e i deferimenti da parte delle autorità di protezione dei dati.

2.1.5. Sviluppi pertinenti nell'ordinamento giuridico statunitense

Da quando è stata adottata la decisione di adeguatezza, si sono registrati diversi sviluppi nel quadro giuridico statunitense in materia di tutela della vita privata, tra cui sviluppi legislativi, normativi e giurisprudenziali. Tali sviluppi segnalano in generale una maggiore convergenza tra gli approcci dell'UE e degli Stati Uniti a determinate sfide relative alla tutela della vita privata, anche attraverso l'uso di concetti giuridici analoghi. Alcuni di questi sviluppi sono in corso e dovranno essere ulteriormente monitorati.

A livello federale, il presidente ha emesso diversi decreti presidenziali pertinenti per l'uso dei dati personali. In particolare, il decreto presidenziale 14117 del 28 febbraio 2024[29] vieta o limita le operazioni che coinvolgono determinate categorie di dati personali sensibili (ad esempio dati sanitari, identificatori biometrici, dati genomici umani) con soggetti che si trovano in alcuni "paesi che destano preoccupazione"[30]. Il decreto adottato incarica il Procuratore generale di proporre regolamenti – ancora da emanare al momento dell'adozione della presente relazione – per specificarne ulteriormente l'attuazione. Inoltre il decreto presidenziale 14110 del 30 ottobre 2023 sull'intelligenza artificiale[31] si concentra sullo sviluppo di un'intelligenza artificiale sicura e affidabile. Prescrive a diverse agenzie federali di elaborare norme e orientamenti di sicurezza relativi all'IA, anche per quanto riguarda i rischi specifici dell'IA per la vita privata e le tecniche di tutela della vita privata.

In termini di attività legislativa, mentre negli ultimi anni il Congresso ha introdotto progetti di legge federali in materia di tutela della vita privata, a partire dal luglio 2024 20 Stati USA hanno adottato leggi generali in materia di tutela della vita privata, otto delle quali sono entrate in vigore: California, Colorado, Oregon, Virginia, Connecticut, Utah, Texas e Florida. Inoltre 17 Stati USA hanno adottato una legislazione che affronta il trattamento automatizzato

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Tra questi figurano, come proposto dal Procuratore generale in un avviso preliminare di proposta di regolamentazione pubblicato il 3 maggio 2024, Cina, Cuba, Hong Kong e Macao, Iran, Corea del Nord e Venezuela. Cfr. https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

(o almeno alcune sue forme) e consente in generale esenzioni per determinati tipi di processi decisionali basati sulla "profilazione"[32].

Per quanto riguarda l'evoluzione della giurisprudenza, diversi rappresentanti della società civile hanno richiamato l'attenzione sulla recente sentenza della Corte suprema nella causa *Loper Bright Enterprises/Raimondo* (del 28 giugno 2024). Tale sentenza ribalta la precedente giurisprudenza sulla dottrina *Chevron* in base alla quale i giudici applicano il principio di deferenza alla ragionevole interpretazione della legge da parte di un'agenzia di regolazione in caso di ambiguità presente in una legge applicata da tale agenzia. In particolare, alcune ONG hanno espresso preoccupazione per l'impatto di detta sentenza della Corte suprema sul potere normativo dell'FTC nel settore della tutela della vita privata, pur riconoscendo che potrebbe non avere alcun impatto o avere un impatto limitato sui suoi poteri esecutivi. Nel corso della riunione di riesame, l'FTC ha comunicato che è ancora presto per conoscere la portata esatta di tale sentenza. Allo stesso tempo ha spiegato che il potere normativo dell'FTC di cui alla legge sull'FTC è diverso da quello di altre agenzie amministrative e per il quale la dottrina *Chevron* era meno pertinente. La recente sentenza potrebbe quindi avere un impatto limitato in questo settore.

L'FTC ha fornito inoltre informazioni sui recenti sviluppi del suo approccio al trattamento automatizzato e all'intelligenza artificiale, tra cui l'adozione di una dichiarazione congiunta insieme ad altre autorità di contrasto contro la discriminazione e i pregiudizi nei sistemi automatizzati[33], nonché diverse azioni coercitive, in cui l'FTC si concentra, tra l'altro, sulla trasparenza, sull'equità del trattamento automatizzato e sulla capacità delle persone di contestare i risultati. Il caso più significativo al riguardo è la decisione dell'FTC nei confronti di *Rite Aid* del marzo 2024, che ha imposto un divieto quinquennale sull'utilizzo della tecnologia di riconoscimento facciale a fini di sicurezza da parte di tale impresa[34]. In particolare, l'FTC ha constatato che *Rite Aid* non aveva adottato misure ragionevoli per evitare risultati errati e informare i consumatori della tecnologia utilizzata. Più in generale, in occasione della riunione di riesame l'FTC ha affrontato le sue attuali priorità e in particolare i settori che, a suo avviso, meritano in futuro un approccio esecutivo più proattivo, tra cui la

[32] Sebbene vi siano differenze in merito al significato di "profilazione" tra i diversi Stati, la profilazione è generalmente definita come qualsiasi forma di trattamento automatizzato effettuato su dati personali al fine di valutare, analizzare o prevedere aspetti personali relativi alla situazione economica, alla salute, alle preferenze personali, agli interessi, all'affidabilità, al comportamento, all'ubicazione o ai movimenti di una persona fisica identificata o identificabile. In genere sono i consumatori a poter rifiutare la profilazione. I seguenti Stati hanno elaborato una legislazione in materia di profilazione: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (codice del Delaware Ann. titolo 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (codice dell'Indiana Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (*Online Data Privacy Act* del Maryland del 2024, promulgata il 9 maggio 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (codice del Montana Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (*Data Transparency and Privacy Protection Act* del Rhode Island, promulgata il 29 giugno 2024), Tennessee (codice del Tennessee Ann. § 47-18-3304), Texas (codice delle imprese e del commercio del Texas Ann. § 541.051) e Virginia (codice della Virginia Ann. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

protezione dei dati sensibili (ad esempio dati sanitari, dati biometrici, geolocalizzazione)[35], la protezione dei bambini[36] e dei minori online, e la sicurezza dei dati[37].

La Commissione continuerà a seguire da vicino questi e altri sviluppi negli Stati Uniti, in particolare qualsiasi ulteriore passo verso una legge federale globale sulla tutela della vita privata e il possibile impatto della recente giurisprudenza della Corte suprema sul ruolo dell'FTC in materia di privacy.

La Commissione accoglie con favore le informazioni fornite dall'FTC sulle sue recenti attività di applicazione della legge e sulle attuali priorità che corrispondono in larga misura alle tendenze e alle priorità nell'applicazione della protezione dei dati in Europa. L'FTC sta inoltre partecipando attivamente alla rete che riunisce i paesi che beneficiano di una decisione di adeguatezza dell'UE, che la Commissione ha istituito nel marzo 2024[38]. Questa maggiore convergenza dovrebbe incoraggiare e agevolare una più stretta cooperazione tra le autorità preposte alla tutela della vita privata su entrambe le sponde dell'Atlantico, in particolare per quanto riguarda le questioni attinenti al funzionamento del DPF.

2.2. Aspetti relativi all'accesso e all'uso dei dati personali trasferiti nell'ambito del quadro UE-USA per la protezione dei dati personali da parte delle autorità pubbliche statunitensi

La decisione di adeguatezza contiene una valutazione dettagliata delle norme che disciplinano la raccolta e l'uso dei dati personali trasferiti dall'UE alle imprese certificate ai sensi del DPF da parte delle autorità pubbliche statunitensi, in particolare per finalità di contrasto penale e di sicurezza nazionale. Dall'adozione della decisione di adeguatezza, come confermato dalle autorità statunitensi durante la riunione di riesame, non vi sono stati sviluppi pertinenti per quanto riguarda il quadro giuridico che si applica all'accesso ai dati per finalità di contrasto o normative nel primo anno di esistenza del DPF. Per tale motivo, le constatazioni che seguono riguardano solo gli sviluppi intervenuti nel settore della sicurezza nazionale.

Le conclusioni raggiunte nella decisione di adeguatezza sull'accesso ai dati da parte degli enti di intelligence si basano sull'analisi delle condizioni e delle limitazioni che si applicano alle operazioni di intelligence dei segnali nell'ambito di diverse autorità giuridiche competenti – in particolare l'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna

[35] Cfr. ad esempio la recente ordinanza dell'FTC contro X-Mode per quanto riguarda la vendita e la condivisione di informazioni sensibili in materia di localizzazione (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) e contro Monument per quanto riguarda la divulgazione a terzi di dati sanitari sensibili a fini di commercializzazione (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Ad esempio, l'FTC ha annunciato di recente l'avvio di un'indagine che ha portato a un'azione legale contro TikTok e la sua società madre, Bytedance, per presunta violazione del diritto della vita privata dei minori. Si sostiene che entrambe le imprese non abbiano rispettato l'obbligo di notificare e ottenere il consenso dei genitori prima di raccogliere e utilizzare informazioni personali di minori di età inferiore ai 13 anni (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Cfr. la sintesi delle recenti attività di applicazione della legge in "The FTC 2023 Privacy and Data Security Update": https://ec.europa.eu/commission/presscorner/detail/it/mex_24_1307.

[38] Cfr. https://ec.europa.eu/commission/presscorner/detail/it/mex_24_1307. A seguito della riunione del marzo 2024, si è deciso di tenere una serie di sessioni tematiche. La prima ha avuto luogo nel luglio 2024 e si è concentrata sullo sviluppo di strumenti in grado di sostenere le piccole e medie imprese nel rispetto delle leggi in materia di tutela della vita privata.

(*Foreign Intelligence Surveillance Act*, FISA) e il decreto presidenziale 12333 [39], integrato e rafforzato dal decreto presidenziale sul miglioramento delle garanzie per le attività di intelligence dei segnali degli Stati Uniti (*Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence"*, decreto presidenziale 14086), adottato dal presidente degli Stati Uniti il 7 ottobre 2022. Le garanzie di cui al decreto presidenziale 14086 si applicano a tutte le attività di intelligence dei segnali statunitensi, indipendentemente dalla base giuridica di tali attività e dal luogo in cui si svolgono, e proteggono i dati di cittadini stranieri (compresi gli europei)[40]. Il decreto presidenziale 14086 ha inoltre istituito un nuovo meccanismo di ricorso attraverso il quale tali garanzie vincolanti possono essere invocate e applicate dalle persone nell'UE.

Le sezioni che seguono descrivono le misure adottate dalle autorità statunitensi dopo l'adozione della decisione di adeguatezza per conformarsi al decreto presidenziale 14086, nonché gli sviluppi pertinenti in relazione al quadro giuridico summenzionato.

2.2.1. Sviluppi pertinenti in relazione al quadro giuridico degli Stati Uniti

2.2.1.1. Attuazione del decreto presidenziale 14086 da parte degli enti di intelligence

Le limitazioni e le garanzie introdotte dal decreto presidenziale 14086 integrano quelle previste dall'articolo 702 FISA e dal decreto presidenziale 12333. Sono vincolanti per tutti gli enti di intelligence e sono state ulteriormente rese operative attraverso politiche e procedure adottate da ciascun ente.

Nell'ambito del primo riesame, le autorità statunitensi hanno confermato che non sono state apportate modifiche al decreto presidenziale 14086 dopo la sua adozione. Inoltre è stato chiarito che il presidente degli Stati Uniti non si è avvalso del potere di cui all'articolo 2, lettera b), punto i), lettera B), e all'articolo 2, lettera b), punto ii), lettera C), del decreto presidenziale 14086 per aggiornare l'elenco degli obiettivi legittimi che possono essere perseguiti dall'intelligence dei segnali o l'elenco delle finalità per le quali i dati raccolti in blocco possono essere utilizzati[41]. Per determinare priorità più specifiche in materia di intelligence per le quali l'intelligence dei segnali può essere effettivamente raccolta, il decreto presidenziale 14086 ha messo in atto una procedura specifica. In particolare, l'addetto alla tutela della vita privata e alle libertà civili dell'Ufficio del direttore dell'intelligence nazionale (ODNI) deve essere consultato per valutare, per ciascuna priorità, se 1) la priorità in questione persegua uno o più obiettivi legittimi di cui al decreto presidenziale; 2) non sia concepita né si prevede che dia luogo a una raccolta di intelligence dei segnali per uno degli obiettivi vietati di cui al decreto presidenziale e 3) sia stata stabilita dopo un'adeguata considerazione della vita privata

[39] Altre misure che possono essere adottate ai sensi della FISA in relazione ai dati trasferiti dall'UE sono la sorveglianza elettronica individualizzata (articolo 105 FISA), le perquisizioni fisiche (articolo 302 FISA), l'uso di dispositivi d'intercettazione dei dati informativi della comunicazione in entrata e in uscita (articolo 402 FISA) e la raccolta di documenti aziendali di alcune imprese (vettori pubblici, strutture ricettive pubbliche, strutture di noleggio di veicoli o strutture di immagazzinamento, articolo 501 FISA). Queste diverse basi giuridiche sono analizzate in dettaglio nella decisione di adeguatezza (considerando da 142 a 152).

[40] Per ulteriori informazioni cfr. la sezione 3.2.1.2 della decisione di adeguatezza.

[41] Tali obiettivi/fini legittimi comprendono, ad esempio, la protezione contro lo spionaggio, il sabotaggio, l'assassinio o altre attività di intelligence svolte da parte, per conto di o con l'assistenza di un governo, un'organizzazione o una persona stranieri; la protezione contro il terrorismo, la presa di ostaggi e l'imprigionamento di persone da parte o per conto di un governo, un'organizzazione o una persona stranieri.

e delle libertà civili di tutte le persone[42]. Durante la riunione di riesame l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI ha confermato di aver esaminato le priorità proposte dal direttore dell'intelligence nazionale nel quadro delle priorità nazionali dell'intelligence del 2023, ha concluso che esse rispettavano i requisiti di cui sopra e ha condiviso le sue conclusioni con il direttore dell'intelligence nazionale, il quale a sua volta ha presentato le priorità a fini di convalida al presidente. L'addetto alla tutela della vita privata e alle libertà civili dell'ODNI ha inoltre fornito formazione sui requisiti del decreto presidenziale 14086 alle parti della comunità di intelligence coinvolte nello sviluppo delle priorità in materia di intelligence.

Nell'ultimo anno inoltre le autorità statunitensi hanno adottato ulteriori misure pratiche per l'attuazione del decreto presidenziale 14086 nelle loro operazioni quotidiane. In particolare, gli enti di intelligence hanno messo in atto ulteriori politiche e linee guida interne sull'applicazione del decreto presidenziale, ad esempio procedure interne (attraverso requisiti interni di autorizzazione, controlli documentati degli accessi, in modo che solo le persone adeguatamente formate e in possesso dei requisiti della missione necessari abbiano accesso alle informazioni, ecc.) per garantire che i requisiti di necessità e proporzionalità siano rispettati nel contesto della raccolta mirata e in blocco[43]. Inoltre è stata impartita una formazione sul decreto presidenziale 14086 al personale di diversi enti di intelligence (ad esempio NSA, CIA, FBI), comprese sessioni di formazione annuali e ad hoc organizzate dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e formazioni obbligatorie per tutto il nuovo personale che entra a far parte dell'ODNI.

La Commissione accoglie con favore le varie misure messe in atto per attuare il decreto presidenziale 14086 e garantirne il rispetto. Una volta acquisita maggiore esperienza nell'applicazione pratica delle garanzie di cui al decreto presidenziale, nei prossimi riesami la Commissione gradirebbe avere l'opportunità di discutere esempi concreti delle modalità pratiche di applicazione del decreto presidenziale (nel rispetto delle esigenze di riservatezza applicabili).

2.2.1.2. Nuova autorizzazione dell'articolo 702 FISA

L'articolo 702 FISA consente di prendere a obiettivo cittadini stranieri che si ritiene ragionevolmente si trovino al di fuori degli Stati Uniti, al fine di acquisire informazioni di intelligence esterna. L'acquisizione avviene sulla base di certificazioni annuali presentate alla Corte di vigilanza sull'intelligence esterna (Corte FISA) e da essa approvate. Tali certificazioni identificano categorie specifiche di intelligence esterna da raccogliere. Il 21 luglio 2023 l'ODNI ha annunciato l'esistenza di tre certificazioni approvate ai sensi dell'articolo 702 FISA, che coprono le categorie di intelligence esterna seguenti: 1) governi stranieri e soggetti correlati, 2) lotta al terrorismo e 3) lotta alla proliferazione[44]. Le certificazioni devono inoltre includere le procedure di individuazione degli obiettivi e minimizzazione approvate dalla Corte FISA[45].

---

[42] Articolo 2, lettera b), punto iii), del decreto presidenziale 14086.

[43] Cfr. https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, pubblicate il 3 luglio 2023.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Tali procedure limitano la raccolta di dati in relazione a una specifica finalità di intelligence esterna, limitano l'accesso alle banche dati in cui sono conservate le informazioni acquisite ai sensi dell'articolo 702 FISA (anche attraverso controlli dell'accesso) e impongono limiti all'uso, alla conservazione e alla diffusione di tali informazioni.

In particolare, l'individuazione degli obiettivi è effettuata richiedendo alle imprese statunitensi che soddisfano la definizione di "prestatore di servizi di comunicazione elettronica" ai sensi della FISA di divulgare i dati delle comunicazioni elettroniche per le comunicazioni inviate a o da "selettori", che identificano uno specifico account di comunicazione, ad esempio un numero di telefono o un indirizzo di posta elettronica. Il governo degli Stati Uniti ha pubblicato una serie di materiali sull'articolo 702 FISA per informare il pubblico in merito al funzionamento dei programmi di sorveglianza, ai requisiti applicabili e alle tutele della vita privata, nonché al ruolo della Corte FISA[46].

A causa di una clausola di temporaneità, l'articolo 702 FISA avrebbe dovuto giungere a scadenza alla fine del 2023, salvo nuova autorizzazione del Congresso. Dopo una nuova autorizzazione temporanea senza modifiche, il 19 aprile 2024 il Congresso ha approvato la legge sulla riforma dell'intelligence e la protezione dell'America (*Reforming Intelligence and Securing America Act*, RISAA), autorizzando nuovamente l'articolo 702 FISA per un periodo di due anni e introducendo diverse modifiche. Si possono distinguere a grandi linee due categorie di modifiche: 1) modifiche dell'ambito delle attività di vigilanza autorizzate a norma dell'articolo 702 FISA e 2) modifiche istituzionali e procedurali.

Modifiche dell'ambito delle attività di vigilanza autorizzate a norma dell'articolo 702 FISA

La RISAA ha introdotto tre modifiche principali all'ambito delle attività di vigilanza che possono essere svolte ai sensi dell'articolo 702 FISA.

In primo luogo, la raccolta di riferimento (raccolta "*about*") è stata definitivamente vietata[47]. Si tratta della raccolta di comunicazioni in cui il selettore di cui all'articolo 702 (ad esempio un indirizzo di posta elettronica) non figura in "a" o "da" delle comunicazioni, ma contiene piuttosto un riferimento a tale selettore nella comunicazione (ad esempio, comunicazioni di posta elettronica che non sono inviate all'indirizzo o dall'indirizzo di posta elettronica selezionato, ma includono l'indirizzo di posta elettronica selezionato nel testo o nel corpo dell'e-mail). Sebbene tale raccolta fosse già stata esclusa a seguito di una modifica della FISA nel 2018, tale legge prevedeva ancora la possibilità di riavviare in futuro la raccolta "*about*", secondo una specifica procedura di autorizzazione che coinvolgeva la Corte FISA e il Congresso. L'ultima modifica introdotta dalla RISAA ha eliminato questa possibilità.

In secondo luogo, la definizione di informazioni di intelligence esterna è stata ampliata per includere le informazioni relative alla lotta contro la droga[48]. Nel corso della riunione di riesame, le autorità statunitensi hanno spiegato che ciò è stato introdotto alla luce dell'attuale crisi del fentanil e della crescente minaccia per la sicurezza nazionale da parte dei trafficanti e dei produttori internazionali di stupefacenti. In tale contesto, è stato confermato che tale concetto rientra in diversi obiettivi legittimi elencati nel decreto presidenziale 14086, vale a dire comprendere o valutare le capacità, le intenzioni o le attività di organizzazioni straniere che rappresentano una minaccia attuale o potenziale per la sicurezza nazionale degli Stati Uniti o dei loro alleati; comprendere o valutare le minacce transnazionali che incidono sulla sicurezza globale, compresi i rischi per la salute pubblica; e la protezione dalle minacce criminali transnazionali[49].

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.
[47] Articolo 22 RISAA.
[48] Articolo 23 RISAA.
[49] Articolo 2, lettera b), punto ii), lettera A), punti 2), 3) e 10), del decreto presidenziale 14086.

In terzo luogo, la RISAA ha ampliato la definizione di "prestatore di servizi di comunicazione elettronica", estendendo in tal modo il novero di imprese che possono essere obbligate a fornire informazioni a norma dell'articolo 702 FISA[50]. La definizione comprende ora altri prestatori di servizi che hanno "accesso ad apparecchiature che sono o possono essere utilizzate per trasmettere o archiviare comunicazioni su filo o elettroniche", escludendo esplicitamente le strutture ricettive pubbliche, le abitazioni, le strutture per la collettività e i locali che offrono servizi di ristorazione. In una lettera al Congresso, il Dipartimento della Giustizia ha fatto riferimento a tale modifica come modifica tecnica intesa a coprire un numero "estremamente ridotto" di imprese tecnologiche che, secondo le recenti decisioni della Corte FISA e della Corte di controllo della vigilanza sull'intelligence esterna (*Foreign Intelligence Surveillance Court of Review*, FISCR), non erano comprese nella precedente definizione di prestatori di servizi di comunicazione elettronica[51]. Nella stessa lettera il Dipartimento della Giustizia si è impegnato a restringere l'ambito di applicazione applicando tale definizione esclusivamente al tipo di prestatore di servizi oggetto del contenzioso che ha portato alla decisione della Corte FISA. Di conseguenza, le imprese interessate sono menzionate in un allegato classificato per il Congresso. Diverse ONG, comprese quelle che hanno fornito un riscontro nell'ambito del riesame, hanno espresso preoccupazioni in merito a tale ampliamento, sostenendo che potrebbe potenzialmente coprire molte imprese statunitensi (dal momento che molte di esse prestano un certo tipo di servizio e hanno accesso alle apparecchiature di comunicazione). Alla luce di tali preoccupazioni, con il sostegno della comunità dell'intelligence è stata proposta un'ulteriore modifica in un progetto di legge autorizzativa dell'intelligence per l'esercizio finanziario 2025, attualmente all'esame del Congresso. Tale modifica, se approvata dal Congresso, garantirebbe che le imprese supplementari incluse nella definizione di prestatore di servizi di comunicazione elettronica siano limitate solo a quelle menzionate nelle sentenze della Corte FISA di cui sopra. Il progetto di legge prevede inoltre che ogni direttiva destinata a un'impresa di questo tipo debba essere comunicata alla Corte FISA, per consentire a quest'ultima di verificare se l'impresa rientrerebbe effettivamente nell'ambito di applicazione. Nella sua lettera al Congresso, il Dipartimento della Giustizia si è impegnato a riferire al Congresso con cadenza semestrale in merito a qualsiasi applicazione della definizione aggiornata al fine di consentire al Congresso di esercitare il controllo adeguato per quanto riguarda l'applicazione restrittiva della definizione.

È importante sottolineare che durante la riunione di riesame le autorità statunitensi e la PCLOB hanno confermato che tutte le garanzie di cui al decreto presidenziale 14086 continuano ad applicarsi pienamente a tutte le attività di raccolta e utilizzo dei dati di cui all'articolo 702 FISA, anche a seguito di tali modifiche. Pertanto la RISAA, pur ampliando in qualche modo il novero delle imprese che possono ricevere un'ordinanza, non limita l'esercizio dei diritti. Tuttavia sarà importante monitorare ulteriormente gli sviluppi (legislativi e in materia di comunicazione) e ricevere informazioni sull'applicazione pratica di queste nuove norme. Ciò comprende, ad esempio, l'impatto dell'ampliamento delle definizioni di intelligence esterna e di prestatore di servizi di comunicazione elettronica sul numero di obiettivi di cui all'articolo 702 FISA (come comunicato annualmente dall'ODNI, cfr. infra per quanto riguarda la trasparenza). La futura

[50] Articolo 25 RISAA.

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Cfr. la decisione della Corte FISA del 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) e la sentenza della Corte di controllo della vigilanza sull'intelligence esterna che ha confermato tale decisione (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

relazione sul seguito dato alla recente relazione della PCLOB sull'articolo 702 FISA (cfr. infra) dovrebbe essere particolarmente informativa al riguardo.

Cambiamenti istituzionali e procedurali

In termini di cambiamenti istituzionali e procedurali, la RISAA ha codificato diverse procedure già seguite nella pratica e ha introdotto nuove garanzie. Sebbene alcune di queste riguardino soltanto i cittadini statunitensi, diversi cambiamenti aumentano le tutele sia per i cittadini statunitensi sia per gli stranieri i cui dati possono essere raccolti a norma dell'articolo 702 FISA[52] e sono quindi pertinenti per il funzionamento del DPF.

In primo luogo, è stata introdotta una serie di obblighi aggiuntivi in materia di responsabilità, vigilanza e comunicazione. In particolare, il personale dell'FBI deve ora ricevere una formazione annuale sulle norme che si applicano alle interrogazioni relative alle informazioni ottenute ai sensi dell'articolo 702 FISA[53]. L'FBI deve inoltre riferire al Congresso in merito alle sue attività di interrogazione (ad esempio, il numero di interrogazioni che utilizzano "tecnologie di lavoro batch", ossia l'utilizzo di termini di interrogazione multipli nell'ambito di un'unica interrogazione) e in merito alle misure di responsabilità messe in atto per garantire il rispetto dei requisiti giuridici in materia di interrogazioni (articoli 11 e 12 RISAA). Inoltre l'ispettore generale del Dipartimento della Giustizia è incaricato di elaborare una relazione sul rispetto dei requisiti in materia di interrogazioni da parte dell'FBI (articolo 9 RISAA). Più in generale, per aumentare la trasparenza delle procedure dinanzi alla Corte FISA, l'ODNI e il Procuratore generale sono ora tenuti a completare la verifica ai fini della declassificazione delle decisioni della Corte FISA entro 180 giorni (articolo 7 RISAA). Inoltre le trascrizioni di tutte le udienze dinanzi alla Corte FISA e alla Corte di controllo della vigilanza sull'intelligence esterna (ove le decisioni della Corte FISA possono essere impugnate) devono essere conservate e trasmesse al Congresso (articolo 8 RISAA).

In secondo luogo, la RISAA ha introdotto ulteriori limitazioni all'uso da parte dell'FBI dei dati raccolti a norma dell'articolo 702 FISA. L'articolo 2, lettera d), RISAA prevede che un'interrogazione che utilizza la "tecnologia batch" possa essere effettuata solo previa approvazione di un avvocato all'interno dell'FBI, a meno che non sussistano circostanze impellenti. Inoltre l'FBI ora non può più verificare automaticamente le informazioni non ridotte al minimo acquisite ai sensi dell'articolo 702 FISA e deve invece garantire che gli analisti procedano a una selezione esplicita per effettuare ricerche a fronte di tali informazioni. La RISAA ha inoltre vietato all'FBI di effettuare interrogazioni volte esclusivamente a reperire ed estrarre prove di attività criminose (a meno che non vi sia una ragionevole certezza che possano contribuire ad attenuare o eliminare una minaccia per la vita o un danno personale grave, o se necessario per rispettare gli obblighi di divulgazione nell'ambito di un contenzioso)[54]. Inoltre all'FBI è vietato inglobare dati non ridotti al minimo in archivi analitici,

[52] La RISAA ha introdotto inoltre alcune modifiche per quanto riguarda la tradizionale sorveglianza elettronica individualizzata ai sensi dell'articolo 105 FISA (sulla base di un mandato emesso dalla Corte FISA in presenza di un tipo di motivo plausibile). Una domanda presentata da un ente di intelligence al Procuratore generale per l'ottenimento di un'ordinanza che autorizzi una sorveglianza elettronica individualizzata deve essere accompagnata ora da una dichiarazione giurata che giustifichi la convinzione che le condizioni di cui all'articolo 105 FISA sono soddisfatte (articolo 6, lettera a), RISAA). La possibile durata della sorveglianza elettronica nei confronti di potenze straniere o di agenti di potenze straniere è stata estesa da 120 giorni a un anno (articolo 6, lettera g), RISAA).

[53] Articolo 2, lettera d), RISAA.

[54] Articolo 3, lettera a), RISAA.

a meno che la persona presa a obiettivo non sia pertinente per un'indagine di sicurezza nazionale esistente[55].

In terzo luogo, alcune disposizioni relative allo status e al ruolo degli *amici curiae* presso la Corte FISA sono state modificate[56]. Gli *amici curiae* sono designati come esperti per assistere la Corte FISA (e la FISCR) su questioni relative alla vita privata e alle libertà civili o per contribuire a chiarire questioni tecnologiche quando si gestisce una specifica domanda di un governo. Mentre in precedenza la FISA prescriveva che gli *amici curiae* disponessero di competenze in materia di tutela della vita privata e libertà civili, raccolta di intelligence, tecnologie della comunicazione o altri settori pertinenti, in linea di principio essa richiede ora il possesso di competenze in materia di tutela della vita privata/libertà civili e di raccolta di intelligence. La Corte FISA aveva già la possibilità di nominare un *amicus curiae* in ogni caso ritenuto opportuno ed era tenuta a farlo nell'ambito di un'interpretazione nuova o significativa della legge. A seguito della nuova autorizzazione, la Corte FISA è ora tenuta a nominare un *amicus curiae* anche ogni volta che le viene chiesto di approvare una certificazione ai sensi dell'articolo 702 FISA e le relative procedure (ad esempio procedure di individuazione degli obiettivi), a meno che non ritenga che ciò non sia opportuno o possa comportare ritardi ingiustificati[57]. Inoltre la Corte FISA, anziché nominare un solo *amicus curiae*, può ora decidere di nominare uno o più *amici curiae*. Si precisa inoltre che le informazioni che devono essere fornite dagli *amici curiae* devono essere "limitate ad affrontare le questioni specifiche individuate dalla Corte", anche se i settori sui quali gli *amici curiae* possono formulare osservazioni sono rimasti ampi (ad esempio, argomentazioni giuridiche e informazioni relative alla tutela della vita privata e alle libertà civili dei cittadini statunitensi, alla raccolta di intelligence e alle tecnologie della comunicazione o a qualsiasi altro settore pertinente).

Infine, l'articolo 18 RISAA istituisce una "commissione per le riforme FISA", composta, tra l'altro, da membri del Congresso, dal presidente della PCLOB, dal direttore principale aggiunto dell'intelligence nazionale e dal Procuratore generale aggiunto e da altri membri nominati dal Congresso[58], per raccomandare ulteriori riforme della FISA.

La Commissione seguirà da vicino gli ulteriori sviluppi relativi all'articolo 702 FISA, anche nel contesto delle attività di vigilanza della PCLOB (cfr. infra), dei lavori della commissione per le riforme e del prossimo riesame della FISA dopo due anni.

2.2.1.3. Attività di vigilanza nella pratica: cifre e tendenze

La relazione annuale statistica dell'ODNI sulla trasparenza relativa all'uso, da parte della comunità dell'intelligence, delle autorità nazionali di vigilanza della sicurezza per l'anno civile 2023 (pubblicata nell'aprile 2024)[59] mostra che il numero di obiettivi di cui all'articolo 702 FISA è aumentato da 245 073 nell'anno civile 2022 a 268 590 nell'anno civile 2023. La relazione spiega che le fluttuazioni del numero di obiettivi possono dipendere da una serie di motivi, tra cui cambiamenti nelle priorità operative, eventi mondiali, capacità tecniche, comportamenti obiettivo e cambiamenti nel settore delle telecomunicazioni. La relazione

[55] Articolo 3, lettera b), RISAA. Se necessario a causa di circostanze impellenti, il direttore dell'FBI può decidere un'eccezione a tale disposizione, che deve essere notificata al Congresso.
[56] A fini di chiarezza, tali modifiche non incidono sullo status e sul ruolo degli avvocati speciali dinanzi al tribunale del riesame in materia di protezione dei dati (*Data Protection Review Court*, DPRC), come confermato dagli Stati Uniti nella riunione di riesame.
[57] Articolo 5, lettera b), RISAA.
[58] L'articolo 18 impone specificamente una rappresentanza scelta al di fuori del Congresso.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

indica inoltre che nessun cittadino straniero (rispetto a 1 nel 2021 e a 0 nel 2022) è stato preso a obiettivo ai sensi dell'articolo 402 FISA (intercettazione dei dati informativi della comunicazione in entrata e in uscita), mentre sono state emesse sei ordinanze (rispetto a 11 nel 2021 e nel 2022), per sei obiettivi (rispetto a 13 nel 2021 e a 11 nel 2022), a norma dell'articolo 501 FISA (accesso ai documenti aziendali dei vettori pubblici, delle strutture di noleggio veicoli o delle strutture di immagazzinamento fisico), riguardanti 5 412 identificatori univoci (rispetto a 23 157 nel 2021 e a 55 431 nel 2022) utilizzati per comunicare le informazioni raccolte in virtù di tali ordinanze.

La relazione annuale del Dipartimento della Giustizia sulla legge relativa alla vigilanza sull'intelligence esterna destinata al Congresso indica che, nel corso dell'anno civile 2023, sono state presentate alla Corte FISA 327 domande di sorveglianza elettronica e/o perquisizioni fisiche a fini di intelligence esterna ai sensi, rispettivamente, degli articoli 105 e 302 FISA[60]. Il numero totale di persone prese a obiettivo era compreso tra 500 e 999. Per quanto riguarda le lettere di sicurezza nazionale (*National Security Letter*, NSL), la relazione indica che sono state emesse 10 115 richieste di informazioni su cittadini stranieri (escluse solo le richieste di informazioni relative agli abbonati) in relazione a 3 033 diversi cittadini stranieri[61].

Diverse imprese certificate ai sensi del DPF (ad esempio Google, Meta) si avvalgono della possibilità prevista dal diritto statunitense di pubblicare relazioni sulla trasparenza che informino in merito al numero di richieste ai sensi della FISA e richieste di NSL ricevute durante un determinato periodo di riferimento. Al momento della stesura della presente relazione, le statistiche sulle richieste ai sensi della FISA dopo luglio 2023 non erano ancora disponibili. Google, ad esempio, ha riferito di aver ricevuto da 500 a 999 richieste di NSL riguardanti da 2 000 a 2 499 account tra luglio e dicembre 2023[62]. Meta ha riferito di aver ricevuto da 0 a 499 richieste di NSL riguardanti da 500 a 999 account nello stesso periodo di riferimento[63]. Negli ultimi anni le cifre sono rimaste piuttosto stabili. Per aumentare ulteriormente la trasparenza, alcune imprese (ad esempio Google) pubblicano proattivamente le *National Security Letter* che hanno ricevuto una volta revocate le restrizioni alla non divulgazione[64].

2.2.1.4. Altri sviluppi

Nel contesto della preparazione del riesame, diverse ONG hanno sollevato interrogativi sulle nuove forme di acquisizione di dati da parte degli enti di intelligence statunitensi attraverso l'acquisto di dati da soggetti commerciali, in particolare da intermediari di dati. Hanno spiegato che, sebbene i dati raccolti su tale base debbano ancora essere trattati conformemente ad altri requisiti, ad esempio a norma del decreto presidenziale 12333[65], tale acquisizione avviene al di fuori del quadro della FISA e del decreto presidenziale 14086.

---

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Tali cifre sono rimaste sostanzialmente stabili rispetto al precedente anno di riferimento (2022). A titolo di confronto, nel 2022 sono state presentate 317 domande finali presso la Corte FISA per effettuare sorveglianza elettronica e/o perquisizioni fisiche a fini di intelligence esterna. Il numero totale di persone oggetto di ordinanze di sorveglianza elettronica era compreso tra 0 e 499. Nel 2022 l'FBI ha presentato 9 103 richieste di NSL per ottenere informazioni su cittadini stranieri (escluse solo le richieste di informazioni sugli abbonati). Fonte: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

[62] https://transparencyreport.google.com/user-data/us-national-security.

[63] https://transparency.meta.com/reports/government-data-requests/country/US/.

[64] https://transparencyreport.google.com/user-data/us-national-security.

[65] Cfr. ad esempio l'articolo 2, punto 4, del decreto presidenziale 12333 sulle tecniche di raccolta.

A tale riguardo, è opportuno ricordare che qualsiasi tipo di condivisione volontaria di dati con terzi è soggetto a diverse condizioni dettagliate nell'ambito del DPF. In primo luogo, l'organizzazione certificata non può condividere i dati con un terzo (che non agisce in qualità di agente/responsabile del trattamento) senza fornire preavviso e possibilità di scelta alle persone interessate[66]. In secondo luogo, conformemente al *principio sulla responsabilità in caso di trasferimento successivo*, i trasferimenti successivi possono avere luogo soltanto 1) per finalità limitate e specifiche, 2) sulla base di un contratto stipulato tra l'organizzazione aderente al DPF UE-USA e il terzo e 3) soltanto se tale contratto impone a detto terzo di fornire il medesimo livello di protezione garantito dai principi[67].

Inoltre, come discusso anche durante la riunione di riesame, l'FTC ha adottato azioni coercitive nei confronti degli intermediari di dati che vendono dati sensibili relativi ai consumatori. Ad esempio, in una causa contro *X-Mode* e il suo successore *Outlogic*, il 9 gennaio 2024 l'FTC ha adottato un'ordinanza che vietava all'impresa di vendere dati di geolocalizzazione a terzi e di cancellare i dati che aveva utilizzato e condiviso illecitamente. Dall'indagine dell'FTC è emerso, tra l'altro, che l'impresa non aveva informato pienamente le persone in merito all'uso e alla vendita dei loro dati di geolocalizzazione, non aveva messo in atto misure per consentire alle persone di rifiutare il tracciamento, aveva consentito l'uso dei dati per scopi potenzialmente discriminatori e non aveva posto limiti all'uso di tali informazioni da parte di terzi[68]. La Commissione si attende che l'FTC adotti il medesimo approccio qualora le imprese certificate ai sensi del DPF dovessero condividere i dati in violazione delle disposizioni di cui sopra.

Infine vale la pena ricordare che nel maggio 2024 l'ODNI ha pubblicato il quadro strategico della comunità dell'intelligence per le informazioni disponibili sul mercato[69]. Tale quadro stabilisce una serie di principi e requisiti che gli enti di intelligence dovrebbero rispettare, anche per ridurre al minimo i rischi per la vita privata e le libertà civili, quando acquisiscono e utilizzano informazioni nel contesto di una transazione commerciale.

2.2.2. Vigilanza indipendente

Le attività degli enti di intelligence statunitensi sono soggette al controllo di diversi organismi, tra cui gli addetti alla tutela della vita privata e alle libertà civili, gli ispettori generali, il Congresso e la PCLOB. In particolare, il decreto presidenziale 14086 impone a ciascun ente di intelligence di disporre di funzionari di alto livello competenti in materie giuridiche, di vigilanza e di conformità al fine di garantire il rispetto del diritto statunitense applicabile. Questa funzione di vigilanza è svolta da addetti aventi un ruolo designato in materia di conformità, nonché da funzionari e ispettori generali competenti per la tutela della vita privata e le libertà civili[70]. Tali funzionari devono svolgere una vigilanza periodica delle attività di

[66] Cfr. il considerando 40 della decisione di adeguatezza.
[67] Cfr. il considerando 38 della decisione di adeguatezza.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Gli enti di intelligence sono tenuti a conformarsi al quadro a partire dall'agosto 2024.
[70] Ogni ente di intelligence dispone di un ispettore generale che è indipendente per legge e responsabile dei controlli e delle indagini riguardanti le attività condotte dall'ente in questione per finalità di sicurezza nazionale. Gli ispettori generali sono autorizzati ad accedere a tutto il materiale pertinente (anche classificato), se necessario mediante l'emanazione di una citazione, e possono assumere testimonianze. Gli ispettori generali segnalano i casi

intelligence dei segnali e garantire che sia posto rimedio a eventuali non conformità. Gli enti di intelligence devono fornire a tali funzionari l'accesso a tutte le informazioni pertinenti per svolgere le loro funzioni di vigilanza e non possono intraprendere azioni volte ad ostacolare o influenzare indebitamente le loro attività di vigilanza.

Alla riunione di riesame ha partecipato il consigliere generale dell'Ufficio dell'ispettore generale della comunità dell'intelligence presso l'ODNI, che ha competenza generale su tutta la comunità dell'intelligence ed è autorizzato a esaminare i reclami o le informazioni inerenti a presunti comportamenti illeciti o abusi di potere. Il consigliere generale ha confermato che l'ispettore generale della comunità dell'intelligence verifica sistematicamente il rispetto del decreto presidenziale 14086 nell'ambito delle sue attività di vigilanza. Il consigliere generale ha inoltre fatto riferimento alle recenti attività di vigilanza di altri ispettori generali della comunità dell'intelligence, come specificato nelle relazioni periodiche. Ad esempio, nella sua relazione semestrale al Congresso per il periodo aprile-settembre 2023[71], l'ispettore generale dell'NSA ha fornito informazioni in merito a una valutazione di un quadro di controllo interno dell'NSA per decisioni e richieste di individuazione degli obiettivi. Il consigliere generale ha concluso che tale quadro funziona correttamente per garantire il rispetto delle leggi, delle direttive e delle politiche in materia di tutela delle libertà civili e della vita privata. La stessa relazione menziona anche un'indagine che ha rivelato l'uso improprio, da parte di un dipendente dell'NSA, di uno strumento di intelligence dei segnali per scopi non autorizzati.

Ai sensi del decreto presidenziale 14086, alla PCLOB[72] sono affidate funzioni di vigilanza specifiche[73]. Il presidente della PCLOB e i suoi tre membri hanno partecipato alla riunione di riesame e hanno comunicato che la PCLOB ha fornito consulenza agli enti di intelligence sui rispettivi progetti di politiche e procedure di attuazione del decreto presidenziale 14086 nell'aprile 2023 ed è stata consultata in merito alla nomina dei giudici e degli avvocati speciali del tribunale del riesame in materia di protezione dei dati (*Data Protection Review Court*, DPRC). La PCLOB ha inoltre avviato un progetto di vigilanza per 1) esaminare l'attuazione delle politiche e delle procedure aggiornate adottate dagli enti di intelligence al fine di garantirne la coerenza con il decreto presidenziale e 2) effettuare un riesame annuale del funzionamento del nuovo meccanismo di ricorso (cfr. infra)[74]. I membri della PCLOB hanno confermato che l'Autorità prevede di effettuare entrambi i riesami nel prossimo futuro. Per quanto riguarda i mezzi di ricorso, hanno spiegato che, in assenza di reclami, il riesame

---

di presunte violazioni in materia penale ai fini dell'azione penale e formulano raccomandazioni per azioni correttive rivolte ai capi degli enti in questione. Sebbene le loro raccomandazioni non siano vincolanti, le relazioni che redigono, anche sugli interventi con cui vi si è dato seguito (o sull'assenza di tali interventi), sono in genere rese pubbliche e trasmesse al Congresso. Cfr. al riguardo la nota 136 della decisione di adeguatezza sul ruolo dell'ispettore generale.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] La PCLOB è un ente indipendente cui sono attribuite competenze nel settore delle politiche antiterrorismo e della loro attuazione, al fine di tutelare la vita privata e le libertà civili. Ha facoltà di accedere a tutte le informazioni pertinenti (comprese quelle classificate), di procedere a interrogatori e di assumere testimonianze. Può rivolgere raccomandazioni alle autorità di contrasto e di intelligence e riferire periodicamente al Congresso e al presidente. Le sue relazioni sono messe a disposizione del pubblico nella misura più ampia possibile.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

della PCLOB si concentrerà sulle politiche e sulle procedure messe in atto per istituire il meccanismo.

Per quanto riguarda le altre attività di vigilanza, il 28 settembre 2023 la PCLOB ha pubblicato una relazione sull'articolo 702 FISA[75]. Detta relazione fa seguito a una precedente relazione del 2014 e contiene informazioni fattuali e giuridiche aggiornate sul funzionamento dei programmi di controllo di cui all'articolo 702 FISA. La relazione contiene inoltre raccomandazioni sul rispetto da parte degli enti di intelligence dei requisiti applicabili nonché suggerimenti al Congresso per rafforzare ulteriormente diversi aspetti dell'articolo 702 FISA nel contesto della sua nuova autorizzazione (anche codificando gli obiettivi legittimi delle attività di controllo elencate nel decreto presidenziale 14086)[76]. Durante la riunione di riesame la PCLOB ha comunicato che prevede di ricevere presto risposte da parte degli enti di intelligence sull'attuazione delle sue raccomandazioni, che confluiranno in una futura relazione di seguito. Altri progetti in materia di vigilanza in corso comprendono un progetto sulla lotta al terrorismo nazionale e il suo impatto sulla vita privata e sulle libertà civili e la raccolta da parte dell'FBI di dati open source o disponibili sul mercato[77].

Infine le ONG consultate nel contesto del riesame hanno espresso il timore che il mandato di diversi membri della PCLOB giungerà a scadenza nel prossimo futuro, il che potrebbe potenzialmente lasciare la PCLOB senza un quorum. In particolare, il mandato della presidente è scaduto e il periodo durante il quale può essere mantenuto l'incarico termina nel gennaio 2025, mentre un altro posto è vacante e un terzo posto si renderà vacante sempre nel gennaio del prossimo anno. Durante la riunione di riesame i membri hanno spiegato di non aspettarsi l'assenza di quorum presso la PCLOB in quanto è già stata presentata una candidatura per il posto attualmente vacante (in attesa di conferma da parte del Senato)[78]. Hanno inoltre sottolineato che, anche se la PCLOB perdesse il quorum, ciò non inciderebbe sulla sua capacità di continuare a realizzare progetti di vigilanza. Ciononostante, dato l'importante ruolo della PCLOB nella verifica dell'attuazione del decreto presidenziale 14086, la Commissione monitorerà attentamente la situazione dei futuri posti vacanti e delle designazioni/nomine.

2.2.3. Mezzi di ricorso

Il decreto presidenziale 14086, integrato da un regolamento del Procuratore generale, ha istituito un nuovo meccanismo di ricorso per gestire e risolvere i reclami qualificati presentati da persone fisiche riguardanti attività di intelligence dei segnali statunitensi[79]. Chiunque nell'UE ha il diritto di presentare un reclamo rivolgendosi al meccanismo di ricorso in merito a una presunta violazione del diritto statunitense che disciplina le attività di intelligence dei segnali (ad esempio il decreto presidenziale 14086, l'articolo 702 FISA, il decreto presidenziale 12333) in relazione ai dati personali trasferiti negli Stati Uniti, che lede gli interessi della persona in questione in materia di tutela della vita privata e libertà civili. Le persone possono

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.
[76] La Commissione osserva che alcune di queste raccomandazioni sono state integrate nell'ambito della RISAA, tra cui la raccomandazione sulla raccolta "*about*" o la raccomandazione sul rafforzamento del ruolo degli esperti (*amici curiae*) presso la Corte FISA.
[77] https://www.pclob.gov/OversightProjects.
[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Considerando da 176 a 194 della decisione di adeguatezza.

presentare un reclamo presso un'autorità di protezione dei dati di uno Stato membro dell'UE che, tramite il segretariato dell'EDPB, trasmette il reclamo al meccanismo di ricorso. Il meccanismo è strutturato in due livelli, dove l'esame iniziale dei reclami è effettuato dall'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e le persone hanno la possibilità di impugnare la decisione dell'addetto alla tutela della vita privata e alle libertà civili dinanzi a un DPRC indipendente. Una volta completato l'esame da parte dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI o dal DPRC, i reclamanti sono informati, tramite l'autorità nazionale, in merito al fatto che l'esame non ha individuato alcuna violazione contemplata o l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI/il DPRC ha emesso una decisione che richiede una riparazione adeguata. Le decisioni dell'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e del DPRC sono vincolanti per gli enti di intelligence.

Dall'adozione della decisione di adeguatezza sono state adottate ulteriori misure per rendere pienamente operativo il meccanismo di ricorso.

Per quanto riguarda l'istituzione del DPRC, il 14 novembre 2023 sono stati nominati otto giudici[80] (ossia due giudici in più rispetto al numero minimo previsto dal decreto presidenziale 14086, integrato dal regolamento del Procuratore generale di cui all'articolo 28 del codice dei regolamenti federali, § 201.3, lettera a)). I giudici sono stati nominati sulla base dei criteri stabiliti nel decreto presidenziale 14086 e conformemente alla procedura ivi stabilita, previa consultazione, tra l'altro, della PCLOB[81], e comprendono ex giudici del tribunale distrettuale federale e della Corte d'appello, un ex Procuratore generale degli Stati Uniti e un ex membro della PCLOB. Come richiesto dal decreto presidenziale, almeno la metà dei giudici ha un'esperienza giudiziaria precedente. Inoltre, nell'aprile 2024, sono stati nominati due avvocati speciali – operatori della giustizia con competenze sia in materia di tutela della vita privata che di sicurezza nazionale – per rappresentare gli interessi delle persone dinanzi al DPRC. Nella riunione di riesame è stato confermato che tutti i giudici e gli avvocati speciali hanno ricevuto il più alto nulla osta di sicurezza e possono pertanto avere accesso a materiali classificati nello svolgimento dei loro compiti per il DPRC. Il DPRC ha inoltre pubblicato una serie di domande frequenti, fornendo maggiori informazioni sul proprio ruolo, la propria indipendenza e il proprio funzionamento[82].

Per quanto riguarda la gestione dei reclami, il 6 dicembre 2022 l'ODNI ha adottato la direttiva 126 sulla comunità dell'intelligence, che disciplina in dettaglio (fissando scadenze, istituendo un archivio elettronico e canali di comunicazione sicuri, imponendo all'addetto alla tutela della vita privata e alle libertà civili e ai servizi della comunità dell'intelligence di cooperare con la PCLOB nel contesto del riesame annuale del meccanismo di ricorso, ecc.) diversi aspetti del processo di esame e risoluzione dei reclami[83]. Detta direttiva è applicabile in tutta la comunità dell'intelligence statunitense ed è stata integrata da ulteriori procedure interne adottate dai singoli enti di intelligence in merito alla loro cooperazione con l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI nel contesto della gestione di un reclamo (ad esempio, lo sviluppo di un archivio sicuro per la condivisione dei reclami e dei documenti di risposta; e

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Articolo 3, lettera d), lettera A), del decreto presidenziale 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

garantire le comunicazioni tra gli enti competenti). Nei prossimi mesi il DPRC pubblicherà inoltre norme più dettagliate sulla gestione dei reclami e su altri aspetti procedurali.

Nell'Unione europea e negli Stati Uniti è stata adottata una serie di misure supplementari per informare il grande pubblico e agevolare la presentazione e la gestione dei reclami, tra cui l'adozione da parte dell'EDPB di una nota informativa sul nuovo meccanismo di ricorso[84], un modello di modulo di reclamo (che dovrebbe essere tradotto e pubblicato da tutte le autorità di protezione dei dati nelle rispettive lingue nazionali)[85] e il regolamento interno che disciplina la cooperazione tra le autorità di controllo nazionali e il segretariato dell'EDPB[86]. Analogamente, l'ODNI ha pubblicato domande frequenti e una scheda informativa sul nuovo meccanismo di ricorso e si è impegnato in attività di sensibilizzazione del pubblico[87].

Inoltre, nell'ultimo anno, l'EDPB e le autorità statunitensi competenti hanno collaborato strettamente su diversi aspetti operativi. In particolare, come confermato durante la riunione di riesame, hanno messo in atto un canale di comunicazione criptato per trasmettere i reclami delle autorità nazionali dell'UE al segretariato dell'EDPB, dal segretariato dell'EDPB all'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e all'Ufficio per la tutela della vita privata e le libertà civili (OPCL) del Dipartimento della Giustizia nonché tra l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI e altre autorità degli Stati Uniti (ad esempio il DPRC). Inoltre l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI ha spiegato che sono state predisposte ulteriori procedure interne per la cooperazione dei singoli enti di intelligence con l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI per quanto riguarda la gestione dei reclami.

Infine, l'Ufficio per la tutela della vita privata e le libertà civili, che fornisce sostegno amministrativo al DPRC, ha anche comunicato che il DPRC opera nell'ambito della propria linea di bilancio dedicata e dispone delle strutture necessarie per svolgere i propri compiti, compresi computer e laptop sicuri, telefoni, ecc. Inoltre, come richiesto dal decreto presidenziale 14086, il Dipartimento del Commercio ha adottato le misure necessarie, anche istituendo un canale di comunicazione criptato con l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI, per conservare un registro di tutti i reclami qualificati ricevuti. Il Dipartimento del Commercio contatterà periodicamente l'addetto alla tutela della vita privata e alle libertà civili dell'ODNI per sapere se le informazioni relative a un singolo reclamo sono state declassificate. In caso affermativo, il Dipartimento del Commercio ne informa l'interessato per consentirgli di accedere a tali informazioni.

Al momento della riunione di riesame le autorità di controllo dell'UE non avevano ricevuto alcun reclamo e pertanto il nuovo meccanismo di ricorso non era ancora stato attivato.

---

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_it.

[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_it.

[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_it.

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf e https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

3. CONCLUSIONE

Sulla base delle informazioni raccolte nel corso di questo primo riesame, la Commissione conclude che le autorità statunitensi hanno posto in essere le strutture e le procedure necessarie per garantire l'efficace funzionamento del quadro per la protezione dei dati personali. In tale contesto, la Commissione apprezza particolarmente l'ottima cooperazione con le autorità statunitensi nello svolgimento del riesame.

Sebbene questo primo riesame si sia naturalmente concentrato sulla verifica dell'esistenza di tutti gli elementi costitutivi del quadro, l'esperienza nell'applicazione pratica delle garanzie che si applicano sia al trattamento dei dati da parte di imprese certificate sia all'accesso ai dati da parte delle autorità pubbliche è necessariamente limitata dopo un solo anno di funzionamento. La Commissione seguirà pertanto da vicino gli sviluppi pertinenti nei prossimi mesi e anni, prestando particolare attenzione 1) alle prossime relazioni della PCLOB sull'attuazione del decreto presidenziale 14086 e sul funzionamento del meccanismo di ricorso per l'intelligence dei segnali, in particolare il DPRC; 2) eventuali ulteriori modifiche dell'articolo 702 FISA; e 3) la designazione e la nomina dei membri della PCLOB per coprire i futuri posti vacanti.

Inoltre, per garantire un funzionamento continuo ed efficace, la Commissione formula le raccomandazioni seguenti:

- come annunciato nella riunione di riesame, il Dipartimento del Commercio dovrebbe avvalersi maggiormente dei diversi strumenti previsti dal DPF per controllare il rispetto dei principi da parte delle imprese e individuare i casi di millantata adesione;
- l'FTC dovrebbe sviluppare ulteriormente il suo approccio proattivo alle indagini e all'applicazione del rispetto dei principi del DPF da parte delle imprese certificate; e
- il Dipartimento del Commercio, l'FTC e le autorità di protezione dei dati dell'UE dovrebbero sviluppare strumenti di orientamento comuni sui requisiti fondamentali previsti dai principi del DPF, ad esempio sui dati relativi alle risorse umane e sui trasferimenti successivi.

Alla luce di questo risultato del riesame e come previsto al considerando 211 della decisione di adeguatezza, la Commissione ritiene opportuno effettuare il prossimo riesame periodico dopo tre anni. Ciò dovrebbe consentire di acquisire maggiore esperienza nell'applicazione pratica del DPF e di tenere conto degli sviluppi futuri di cui sopra. La Commissione pertanto, conformemente all'articolo 3, paragrafo 4, della decisione di adeguatezza, consulterà l'EDPB e il comitato istituito a norma dell'articolo 93, paragrafo 1, del regolamento generale sulla protezione dei dati in merito alla periodicità dei futuri riesami.