Parere 5/2023 relativo al progetto di decisione di esecuzione della Commissione europea per quanto riguarda la protezione adeguata dei dati personali nel contesto del quadro per la protezione dei dati UE-USA

Adottato il 28 febbraio 2023

Sintesi

Il 13 dicembre 2022 la Commissione europea ha pubblicato un progetto di decisione sull'adeguatezza ("progetto di decisione"), il quale contiene allegati che costituiscono un nuovo quadro per gli scambi transatlantici di dati personali, il quadro UE-USA per la protezione dei dati personali ("DPF", *Data Privacy Framework*) UE-USA, inteso a sostituire il precedente scudo UE-USA per la privacy, dichiarato invalido dalla Corte di giustizia dell'Unione europea ("CGUE") il 16 luglio 2020 con la sentenza nella causa *Schrems II*. La componente chiave del DPF è costituita dai principi del quadro UE-USA per la protezione dei dati personali, compresi i principi supplementari (collettivamente "i principi del DPF").

Conformemente all'articolo 70, paragrafo 1, lettera s), del regolamento (UE) 2016/679[1] del Parlamento europeo e del Consiglio ("GDPR"), la Commissione ha richiesto il parere del Comitato europeo per la protezione dei dati ("EDPB") in merito al progetto di decisione.

L'EDPB ha valutato l'adeguatezza del livello di protezione offerto negli Stati Uniti d'America ("USA" o "Stati Uniti"), sulla base dell'esame del progetto di decisione. L'EDPB ha valutato tanto gli aspetti commerciali quanto l'accesso e l'utilizzo dei dati personali trasferiti dall'UE da parte di autorità pubbliche negli Stati Uniti.

L'EDPB ha tenuto conto del quadro giuridico dell'UE applicabile in materia di protezione dei dati, come stabilito nel GDPR, nonché dei diritti fondamentali del rispetto della vita privata e alla protezione dei dati di carattere personale sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea e dall'articolo 8 della convenzione europea dei diritti dell'uomo ("CEDU"). Ha inoltre tenuto presente il diritto a un ricorso effettivo e a un giudice imparziale sancito all'articolo 47 della Carta, nonché la giurisprudenza relativa ai vari diritti fondamentali.

Inoltre l'EDPB ha preso in considerazione i requisiti di cui ai criteri di riferimento per l'adeguatezza adottati dall'EDPB[2].

L'obiettivo principale dell'EDPB è fornire un parere alla Commissione circa l'adeguatezza del livello di protezione offerto alle persone i cui dati personali sono trasferiti negli Stati Uniti. È importante precisare che l'EDPB non si aspetta che il quadro per la protezione dei dati personali degli Stati Uniti riproduca la normativa europea sulla protezione dei dati.

Tuttavia l'EDPB ricorda che, in base all'articolo 45 GDPR e alla giurisprudenza della CGUE, la legislazione del paese terzo, per essere considerata fornire un livello di protezione adeguato, deve fornire agli interessati un livello di protezione sostanzialmente equivalente a quello garantito nell'UE.

1.1. Aspetti generali in materia di protezione dei dati personali

Il DPF prevede che l'adesione ai principi del DPF da parte delle organizzazioni del DPF possa essere limitata in alcuni casi (ad esempio nella misura in cui ciò sia necessario per ottemperare all'ordinanza di un organo giurisdizionale o per soddisfare un interesse pubblico). Al fine di individuare meglio l'impatto di tali esenzioni sul livello di protezione degli interessati, l'EDPB raccomanda che la

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

[2] Gruppo di lavoro, Criteri di riferimento per l'adeguatezza, WP 254 rev.01, 28 novembre 2017, come da ultimo rivisti e adottati il 6 febbraio 2018, approvati dall'EDPB il 25 maggio 2018 (in appresso: "criteri di riferimento per l'adeguatezza").

Commissione includa nel progetto di decisione chiarimenti sulla portata delle esenzioni, comprese le garanzie applicabili ai sensi del diritto statunitense.

L'EDPB osserva che la struttura degli allegati e la loro numerazione rendono le informazioni piuttosto difficili da trovare e da consultare. Ciò contribuisce a una presentazione complessivamente complessa del nuovo quadro che raccoglie nei suoi allegati documenti di diverso valore giuridico e può non favorire una buona comprensione dei principi del DPF da parte degli interessati, delle organizzazioni del DPF e delle autorità di protezione dei dati dell'UE. L'EDPB sottolinea inoltre che la terminologia dovrebbe essere utilizzata in modo coerente in tutto il DPF. Analogamente, manca la definizione di alcuni termini essenziali[3].

L'EDPB accoglie con favore gli aggiornamenti apportati ai principi del DPF[4], che costituiranno il quadro giuridico vincolante per le organizzazioni del DPF, ma rileva che, nonostante una serie di modifiche e spiegazioni aggiuntive apportate nei considerando del progetto di decisione, i principi del DPF che le organizzazioni del DPF devono rispettare rimangono sostanzialmente invariati rispetto a quelli applicabili nel contesto dello scudo per la privacy (su cui si sono basati i riesami congiunti annuali del gruppo di lavoro "Articolo 29" (Gruppo di lavoro) e dell'EDPB). I principi del DPF altresì e in larga misura, sono i medesimi del progetto di scudo per la privacy su cui il Gruppo di lavoro ha basato il suo parere del 2016[5]. Per i principi del DPF che sono sostanzialmente invariati, l'EDPB non ritiene necessario ripetere tutte le osservazioni precedentemente formulate dal Gruppo di lavoro. L'EDPB ha deciso di concentrarsi su aspetti specifici che ritiene ancora più rilevanti attualmente, in considerazione dell'evoluzione del contesto giuridico e tecnologico.

Ad esempio l'EDPB osserva che alcune questioni che destano preoccupazione precedentemente sollevate dal Gruppo di lavoro e dall'EDPB in relazione ai principi di cui allo scudo per la privacy rimangono valide. In particolare si tratta dei diritti degli interessati (ad esempio, alcune eccezioni al diritto di accesso e i tempi e le modalità del diritto di opposizione), dell'assenza di definizioni chiave, della mancanza di chiarezza in relazione all'applicazione dei principi del DPF ai responsabili del trattamento e dell'ampia esenzione per le informazioni pubblicamente disponibili[6].

L'EDPB vorrebbe altresì ribadire che il livello di protezione delle persone i cui dati sono trasferiti non deve essere compromesso da trasferimenti successivi dal destinatario iniziale dei dati trasferiti[7]. L'EDPB invita ancora una volta la Commissione a chiarire che le garanzie imposte dal destinatario iniziale all'importatore nel paese terzo devono essere efficaci alla luce della legislazione del paese terzo, prima di un trasferimento successivo nel contesto del DPF.

I rapidi sviluppi nel settore del processo decisionale automatizzato e della profilazione, sempre più spesso ricorrendo all'uso di tecnologie di intelligenza artificiale, richiedono particolare attenzione. L'EDPB accoglie con favore i riferimenti della Commissione alle garanzie specifiche previste dal diritto statunitense pertinente in settori diversi[8]. Tuttavia il livello di protezione per le persone sembra variare a seconda delle norme settoriali specifiche, laddove esistano, che si applicano alla situazione in

[3] È il caso dei termini "procuratore" e "responsabile del trattamento". Inoltre, il concetto di "dati relativi alle risorse umane" deve ancora essere discusso con le autorità statunitensi.

[4] Ad esempio, la precisazione che i dati codificati sono dati personali.

[5] Gruppo di lavoro, Parere 01/2016 sul progetto di decisione sull'adeguatezza del regime dello scudo UE-USA per la privacy, adottato il 13 aprile 2016 (in appresso: "parere 01/2016 del Gruppo di lavoro").

[6] Scudo UE-USA per la privacy - Terzo riesame congiunto annuale, relazione dell'EDPB adottata il 12 novembre 2019, punto 11 (solo in EN).

[7] Capitolo 3, lettera A), punto 9, dei criteri di riferimento per l'adeguatezza in materia di GDPR.

[8] Considerando 35 del progetto di decisione.

questione. L'EDPB sostiene che, al fine di fornire garanzie sufficienti, siano necessarie norme specifiche sul processo decisionale automatizzato, tra cui il diritto della persona fisica di conoscere la logica applicata, di contestare la decisione e di ottenere l'intervento umano quando la decisione la riguarda in modo significativo.

L'EDPB ricorda l'importanza di una vigilanza e di un'applicazione efficaci del DPF e ritiene che i controlli di conformità per quanto concerne i requisiti più sostanziali siano fondamentali. Tali aspetti saranno monitorati attentamente dall'EDPB, anche nel contesto dei riesami periodici. L'EDPB prende atto dei rinnovati impegni contenuti nelle lettere della Commissione federale del commercio ("FTC", *Federal Trade Commission*)[9] e del Dipartimento dei Trasporti ("DoT", *Department of Transportation*)[10] per quanto concerne l'applicazione della normativa, ad esempio al fine di riconoscere la priorità alle indagini relative a presunte violazioni del DPF.

L'EDPB osserva che sono previsti sette mezzi di ricorso per gli interessati dell'UE, qualora i loro dati personali siano trattati in violazione del DPF. Tali meccanismi di ricorso sono i medesimi inclusi nel precedente scudo per la privacy, che erano stati oggetto di osservazioni da parte del Gruppo di lavoro[11]. L'efficacia di tali meccanismi di ricorso sarà monitorata attentamente dall'EDPB, anche nel contesto dei riesami periodici.

1.2. Accesso e uso dei dati personali trasferiti dall'Unione europea negli Stati Uniti da parte di autorità pubbliche

Nel progetto di decisione, la Commissione europea conclude che qualsiasi interferenza nell'interesse pubblico, in particolare per attività di contrasto in materia penale e per finalità di sicurezza nazionale, da parte delle autorità pubbliche statunitensi, in relazione ai diritti fondamentali delle persone i cui dati personali sono trasferiti dall'Unione agli Stati Uniti ai sensi del quadro UE-USA per la protezione dei dati personali, sarà limitata a quanto strettamente necessario per conseguire l'obiettivo legittimo in questione, e che esiste una tutela giuridica efficace contro tale interferenza[12].

La Commissione europea giunge alla sua conclusione dopo un'ampia valutazione del decreto presidenziale (*Executive Order*) 14086 che rafforza le garanzie per le attività di intelligence dei segnali degli Stati Uniti ("decreto presidenziale 14086"). Il decreto presidenziale 14086 è stato emanato dal presidente degli Stati Uniti il 7 ottobre 2022, a seguito delle negoziazioni della Commissione europea con il governo degli Stati Uniti in conseguenza dell'invalidazione della precedente decisione di adeguatezza, denominata scudo per la privacy, da parte della Corte di giustizia dell'Unione europea (CGUE).

L'EDPB auspicherebbe che non solo l'entrata in vigore ma anche l'adozione della decisione siano subordinate, tra l'altro, all'adozione di politiche e procedure aggiornate per l'attuazione del decreto presidenziale 14086 da parte di tutte le agenzie di intelligence statunitensi. L'EDPB raccomanda alla Commissione di valutare tali politiche e procedure aggiornate e di condividere tale valutazione con l'EDPB.

Per quanto concerne l'accesso da parte delle pubbliche amministrazioni ai dati personali trasferiti negli Stati Uniti, l'EDPB ha concentrato la propria analisi sulla valutazione del nuovo decreto presidenziale

[9] Allegato IV del progetto di decisione.
[10] Allegato V del progetto di decisione.
[11] Cfr. in particolare il parere 01/2016 del Gruppo di lavoro, sezione 2.2.6, lettera a).
[12] Considerando 195 del progetto di decisione.

14086, essendo effettivamente destinato ad affrontare e porre rimedio alle carenze individuate dalla CGUE nella sentenza *Schrems II*, quando ha ritenuto invalida la precedente decisione di adeguatezza.

L'EDPB riconosce che il quadro giuridico statunitense per le attività di intelligence dei segnali è stato modificato dall'adozione del decreto presidenziale 14086 e considera le garanzie aggiuntive incluse in tale decreto un miglioramento significativo. Il decreto presidenziale 14086 introduce i concetti di necessità e proporzionalità nel quadro giuridico statunitense sull'intelligence dei segnali e prevede, qualora l'UE dovesse essere designata come organizzazione regionale d'integrazione economica qualificata, un nuovo meccanismo di ricorso per le persone dell'UE. L'EDPB ritiene che il nuovo meccanismo di ricorso sia notevolmente migliorato rispetto al precedente cosiddetto meccanismo di mediazione previsto dallo scudo per la privacy. A differenza del precedente quadro giuridico, che non creava diritti per le persone dell'UE, come è stato esplicitamente osservato dalla CGUE, il nuovo decreto presidenziale 14086 crea tali diritti e fornisce maggiori garanzie per l'indipendenza del Tribunale del riesame in materia di protezione dei dati ("DPRC", *Data Protection Review Court*) e poteri più efficaci per porre rimedio a eventuali violazioni.

Confrontando le garanzie aggiuntive incluse nel decreto presidenziale 14086 con quelle che l'EDPB ha definito le garanzie essenziali europee, come norme elaborate sulla base della giurisprudenza della CGUE e della Corte europea dei diritti dell'uomo (Corte CEDU), l'EDPB ha comunque individuato nella propria valutazione una serie di punti che richiedono ulteriori chiarimenti o attenzione oppure destano preoccupazione. Tali punti rispecchiano il fatto che, sebbene l'EDPB abbia basato il proprio parere sulla sentenza *Schrems II*, la portata della valutazione dell'EDPB include necessariamente considerazioni che vanno al di là delle conclusioni specifiche di cui alla sentenza *Schrems II*.

L'EDPB ritiene necessario chiarire ulteriormente, in particolare, le questioni relative alla "raccolta temporanea in blocco di dati" e all'ulteriore conservazione e diffusione dei dati raccolti (in blocco) nel contesto del quadro giuridico statunitense.

Poiché la verifica dell'equivalenza sostanziale non è una verifica dell'identicità e poiché le garanzie incluse nel nuovo quadro giuridico sull'intelligence dei segnali sono state rafforzate, il principale punto di attenzione e di preoccupazione dell'EDPB si concentra su una valutazione delle garanzie nella loro interezza, seguendo un approccio olistico che tiene conto delle garanzie per l'intero ciclo di trattamento, dalla raccolta dei dati alla loro diffusione, e che include gli elementi di vigilanza e di ricorso.

A questo proposito, l'EDPB sottolinea le risultanze riportate di seguito.

Pur riconoscendo che il decreto presidenziale 14086 introduce i concetti di necessità e proporzionalità nel quadro giuridico dell'intelligence dei segnali, l'EDPB sottolinea la necessità di monitorare attentamente gli effetti di tali modifiche nella pratica, anche in termini di riesame delle politiche e delle procedure interne che attuano le garanzie sancite da tale decreto a livello di agenzia.

L'EDPB accoglie inoltre con favore il fatto che il decreto presidenziale 14086 contenga un elenco di finalità specifiche per le quali la raccolta può o non può avvenire, pur rilevando che gli obiettivi possono essere aggiornati con obiettivi ulteriori, non necessariamente pubblici, alla luce di nuovi motivi imperativi di sicurezza nazionale.

Una carenza individuata in particolare dall'EDPB nel quadro attuale consiste nel fatto che il quadro giuridico statunitense, nel consentire la raccolta in blocco di dati ai sensi del decreto presidenziale 12333, non prevede il requisito dell'autorizzazione preventiva da parte di un'autorità indipendente, come richiesto dalla più recente giurisprudenza della Corte CEDU, né un riesame sistematico

indipendente ex post da parte di un organo giurisdizionale o di un organismo altrettanto indipendente. Per quanto concerne l'autorizzazione preventiva e indipendente della sorveglianza ai sensi dell'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna (FISA, *Foreign Intelligence Surveillance Act*), l'EDPB si rammarica del fatto che la Corte FISA ("FISC", *Foreign Intelligence Surveillance Court*, organo giurisdizionale per la vigilanza dell'intelligence esterna) non riesamini l'applicazione di un programma per verificarne la conformità rispetto al decreto presidenziale 14086 al momento della certificazione del programma che autorizza l'individuazione di cittadini non statunitensi da considerare come obiettivi, anche se le autorità di intelligence che attuano il programma ne sono vincolate. Secondo l'EDPB, le garanzie supplementari contenute in tale decreto dovrebbero comunque essere prese in considerazione anche dalla Corte FISA. L'EDPB ricorda che le relazioni dell'Autorità per la tutela della vita privata e delle libertà civili ("PCLOB", *Privacy and Civil Liberties Oversight Board*) sarebbero particolarmente utili per valutare le modalità di attuazione delle garanzie di cui al decreto presidenziale 14086 e le modalità di loro applicazione quando i dati sono raccolti a norma dell'articolo 702 della FISA e del decreto presidenziale 12333.

Per quanto concerne il meccanismo di ricorso, l'EDPB riconosce miglioramenti significativi relativi ai poteri conferiti al DPRC e alla sua maggiore indipendenza rispetto al mediatore. L'EDPB riconosce altresì le garanzie supplementari previste dal nuovo meccanismo di ricorso, quali il ruolo degli avvocati speciali che comprende la difesa degli interessi del reclamante e il riesame del meccanismo di ricorso da parte della PCLOB. Pur tenendo conto della natura della sicurezza nazionale e delle garanzie previste dal decreto presidenziale 14086, l'EDPB esprime tuttavia preoccupazione in merito all'applicazione generale della risposta standard della DPRC che notifica al reclamante che non sono state individuate violazioni rientranti nell'ambito di applicazione della normativa in questione o che è stata emessa una decisione che richiede l'attuazione di una riparazione adeguata, nonché preoccupazione in merito alla non impugnabilità di tale risposta, considerate congiuntamente. Data l'importanza del meccanismo di ricorso, l'EDPB invita la Commissione a monitorare attentamente il funzionamento pratico di tale meccanismo.

L'EDPB si aspetta che la Commissione dia seguito all'impegno di sospendere, abrogare o modificare la decisione di adeguatezza per motivi di urgenza, in particolare nel caso in cui l'esecutivo degli Stati Uniti decida di limitare le garanzie incluse nel decreto presidenziale[13].

Nel complesso, l'EDPB rileva positivamente i miglioramenti sostanziali che il decreto presidenziale offre rispetto al quadro giuridico precedente, in particolare per quanto concerne l'introduzione dei principi di necessità e proporzionalità e il meccanismo di ricorso individuale per gli interessati dell'UE. In considerazione delle preoccupazioni espresse e dei chiarimenti richiesti, l'EDPB suggerisce che tali preoccupazioni vengano affrontate e che la Commissione fornisca i chiarimenti richiesti al fine di consolidare le basi del progetto di decisione e di garantire un monitoraggio attento dell'attuazione concreta di questo nuovo quadro giuridico, in particolare delle garanzie da esso previste, nei futuri riesami congiunti.

[13] Considerando 212 del progetto di decisione.

Indice

Il Comitato europeo per la protezione dei dati

Il Comitato europeo per la protezione dei dati ha adottato la seguente dichiarazione:

visto l'articolo 70, paragrafo 1, lettera s), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso "GDPR")[1],

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[2],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO IL PRESENTE PARERE:

1 INTRODUZIONE

1.1 Quadro di protezione dei dati degli Stati Uniti

1. Gli Stati Uniti ("USA") e l'Unione europea ("UE") adottano approcci diversi al rispetto della vita privata e alla protezione dei dati. Mentre nell'UE il rispetto della vita privata e la protezione dei dati sono diritti fondamentali garantiti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (la "Carta"), negli Stati Uniti la protezione dei dati è in genere affrontata dal punto di vista della tutela dei consumatori. Di conseguenza gli approcci normativi negli Stati Uniti e nell'UE differiscono tra loro[3].

2. A differenza dell'approccio globale dell'UE adottato dal GDPR, negli Stati Uniti non esiste una legge generale in materia di protezione dei dati a livello federale. La protezione della vita privata negli Stati Uniti è piuttosto realizzata secondo un approccio settoriale e a livello di Stati. Ad esempio, alcuni settori specifici sono oggetto di atti specifici, come nel caso di:

   - *Health Insurance Portability and Accountability Act* (HIPAA)[4];

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE) (GU L 119 del 4.5.2016, pag. 1).

[2] Ai fini del presente parere per "Stati membri" si intendono gli "Stati membri del SEE".

[3] Cfr. anche progetto di decisione di esecuzione della Commissione europea ai sensi 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, pubblicato il 13 dicembre 2022 (in appresso: il "progetto di decisione"), allegato I, sezione I.

[4] La legge sulla portabilità e la responsabilità dell'assicurazione sanitaria del 1996 (HIPAA) è una legge federale statunitense. Istituisce norme nazionali volte a proteggere le informazioni sanitarie sensibili dei pazienti. L'obiettivo dell'HIPAA è proteggere adeguatamente le informazioni sanitarie delle persone, consentendo al contempo la circolazione delle informazioni sanitarie per la fornitura e la promozione di un'assistenza sanitaria

- *Children's Online Privacy Protection Act* (COPPA)[5];
- *Gramm-Leach-Billey Act* (GLBA)[6].

3. Nel settore dell'accesso da parte di pubbliche amministrazioni ai dati personali trasferiti dall'UE agli Stati Uniti si applicano basi giuridiche, limitazioni e garanzie diverse. Le procedure legali per l'accesso alle informazioni per fini di contrasto derivano direttamente dalla costituzione degli Stati Uniti (il quarto emendamento), dalla legislazione e dal diritto processuale oppure dagli orientamenti e dalle politiche del Dipartimento della Giustizia a livello federale o statale. L'accesso alle informazioni per finalità di sicurezza nazionale è disciplinato da diversi strumenti giuridici e in particolare dalla legge relativa alla vigilanza sull'intelligence esterna (FISA, *Foreign Intelligence Surveillance Act*), dal decreto presidenziale 12333, dal recente decreto presidenziale 14086 e dal regolamento sul procuratore generale ("*Attorney General Regulation*")[7] che istituisce un Tribunale del riesame in materia di protezione dei dati ("DPRC").

4. Il 13 dicembre 2022 la Commissione ha pubblicato il progetto di decisione di esecuzione della Commissione ai sensi 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 ("il progetto di decisione"), che contiene in allegato il testo di detto quadro ("il DPF"). Per le ragioni sopra esposte, il progetto di decisione non si basa su un quadro giuridico federale specifico e completo, bensì sul DPF.

5. Il DPF funziona come segue: il Dipartimento del Commercio degli Stati Uniti ("il Dipartimento") emette i principi quadro UE-USA per la protezione dei dati personali, compresi i principi supplementari (collettivamente "i principi") e l'allegato I dei principi ("allegato I"), in virtù della propria autorità statutaria di favorire, promuovere e sviluppare il commercio internazionale (Codice degli Stati Uniti d'America, titolo 15, articolo 1512)[8].

6. L'elaborazione dei "principi" (i "principi del DPF") è stata condotta in consultazione con la Commissione europea (la "Commissione"), l'industria e altri portatori di interessi, al fine di raggiungere l'obiettivo di

---

di qualità elevata. L'HIPAA disciplina l'uso e la divulgazione delle informazioni sanitarie da parte di enti soggetti alla norma sulla privacy. Comprende altresì norme per i diritti delle persone destinati a consentire a queste ultime di comprendere e controllare l'utilizzo delle loro informazioni sanitarie. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] L'obiettivo principale della legge sulla protezione della vita privata online dei minori (COPPA) è consentire ai genitori di controllare quali informazioni personali vengono raccolte in merito ai loro figli di età inferiore ai 13 anni dagli operatori di siti web e servizi online rivolti ai minori (comprese le applicazioni mobili e i dispositivi IoT, quali i giocattoli intelligenti) o di siti destinati al pubblico in generale. La COPPA richiede che tali operatori notifichino un avviso ai genitori e debbano ottenere un consenso verificabile da questi ultimi. Ciò vale anche per i dati di minori stranieri se i siti web o i servizi sono gestiti negli Stati Uniti e sono soggetti alla COPPA. Allo stesso tempo, le norme si applicano anche ai siti web e ai servizi stabiliti all'estero se sono rivolti a minori negli Stati Uniti. Cfr.: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions e allegato IV del progetto di decisione (pag. 3).

[6] Uno degli obiettivi della legge Gramm-Leach-Bliley (GBLA) è proteggere la vita privata dei consumatori nel settore finanziario. La GBLA impone agli istituti finanziari di spiegare ai propri clienti le pratiche di condivisione delle informazioni e di creare garanzie destinate a proteggere le informazioni dei clienti (ad esempio, per le società disciplinate dalla FTC ai sensi della norma in materia di garanzie della FTC). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[7] Ordinanza del procuratore generale n. 5517-2022, che modifica i regolamenti del Dipartimento della Giustizia degli Stati Uniti come da autorizzazione e istruzioni di cui al decreto presidenziale 14086.

[8] Allegato I, sezione I, del progetto di decisione.

facilitare gli scambi e il commercio tra l'UE e gli Stati Uniti[9], assicurando nel contempo agli interessati un livello di protezione sostanzialmente equivalente a quello garantito nell'UE.

7. I principi del DPF sono descritti come una "componente chiave" del DPF. Da un lato, forniscono un "meccanismo pronto all'uso" per il trasferimento di dati dall'UE agli Stati Uniti. Dall'altro, i dati personali trasferiti dall'UE agli Stati Uniti sono salvaguardati e protetti come richiesto dal diritto dell'UE.

8. Il DPF è applicabile soltanto alle organizzazioni statunitensi che si sono autocertificate secondo i requisiti del quadro ("organizzazioni del DPF"). Attualmente ciò è possibile soltanto se rientrano nella competenza giurisdizionale della Commissione federale del commercio ("FTC") o del Dipartimento dei Trasporti ("DoT"). In futuro, altri organi statutari, aventi competenza di supervisione sull'attuazione dei principi del DPF, potrebbero essere aggiunti in un futuro allegato.

9. I principi del DPF spiegano che le condizioni del quadro sono applicabili: i) dalla FTC ai sensi dell'articolo 5 della legge sulla Commissione federale del commercio (*FTC Act*) che vieta atti sleali o ingannevoli nel commercio o che incidono sul commercio[10]; ii) dal DoT ai sensi del Codice degli Stati Uniti d'America, titolo 49, articolo 41712 che proibisce a un vettore o a un agente di vendita di biglietti di adottare una pratica sleale o ingannevole nel trasporto aereo per la vendita o il trasporto aereo; o iii) ai sensi di altre leggi o regolamenti che vietano tali atti.

10. Nei principi del DPF si sottolinea che detti principi non incidono sul GDPR in termini di sua applicazione né limitano gli obblighi esistenti in materia di tutela della vita privata, altrimenti applicati dal diritto statunitense.

1.2 Ambito di applicazione della valutazione dell'EDPB

11. Il progetto di decisione rispecchia la valutazione della Commissione in merito al DPF, frutto di discussioni con il governo statunitense. Ai sensi dell'articolo 70, paragrafo 1, lettera s), GDPR, l'EDPB è tenuto a fornire un parere sulle conclusioni della Commissione in merito all'adeguatezza del livello di protezione in un paese terzo e, se necessario, a formulare proposte per risolvere eventuali questioni.

12. L'EDPB accoglie con favore gli aggiornamenti apportati ai principi del DPF[11], che costituiranno il quadro giuridico vincolante per le organizzazioni del DPF. Tuttavia l'EDPB osserva che i principi del DPF rimangono essenzialmente gli stessi dello scudo per la privacy[12] (su cui si sono basati i riesami congiunti annuali del gruppo di lavoro Articolo 29 ("Gruppo di lavoro") e dell'EDPB). I principi del DPF sono altresì, in larga misura, i medesimi del progetto di scudo per la privacy su cui il Gruppo di lavoro ha basato il suo parere del 2016[13] ("il parere 01/2016 del Gruppo di lavoro"). Per i principi del DPF che sono sostanzialmente invariati, l'EDPB non ritiene necessario ripetere tutte le osservazioni precedentemente formulate dal Gruppo di lavoro. L'EDPB ha deciso di concentrarsi su aspetti specifici

[9] Ibidem.
[10] Codice degli Stati Uniti d'America, titolo 15, articolo 45, lettera a).
[11] Ad esempio, la precisazione che i dati codificati sono dati personali.
[12] Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (GU L 207 dell'1.8.2016, pag. 1).
[13] Gruppo di lavoro, Parere 01/2016 sul progetto di decisione sull'adeguatezza del regime dello scudo UE-USA per la privacy, adottato il 13 aprile 2016 (in appresso: "parere 01/2016 del Gruppo di lavoro").

che ritiene ancora più rilevanti attualmente, in considerazione dell'evoluzione del contesto giuridico e tecnologico.

13. Inoltre, in linea con la giurisprudenza della CGUE[14], una parte molto importante dell'analisi riguarda il regime giuridico dell'accesso da parte di pubbliche amministrazioni ai dati personali trasferiti negli Stati Uniti.

14. Nella sua valutazione, l'EDPB ha tenuto conto del quadro europeo applicabile in materia di protezione dei dati, compresi gli articoli 7, 8 e 47 della Carta, che tutelano rispettivamente il diritto al rispetto della vita privata e della vita familiare, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo e a un giudice imparziale e a un giudice imparziale, e l'articolo 8 della Convenzione europea dei diritti dell'uomo ("CEDU") che tutela il diritto al rispetto della vita privata e familiare. Oltre a quanto sopra, l'EDPB ha preso in considerazione i requisiti del GDPR, la giurisprudenza pertinente e i criteri di riferimento per l'adeguatezza adottati dall'EDPB ("criteri di riferimento per l'adeguatezza ai sensi del GDPR")[15].

15. L'obiettivo di questo esercizio è fornire alla Commissione un parere per la valutazione dell'adeguatezza del livello di protezione fornito dal DPF. Il concetto di "livello di protezione adeguato", che esisteva già nella direttiva 95/46/CE, è stato ulteriormente sviluppato dalla CGUE. Di conseguenza è importante ricordare la norma stabilita dalla CGUE nelle sentenze *Schrems I*[16] (che ha invalidato l'"approdo sicuro") e *Schrems II*[17] (che ha invalidato lo scudo per la privacy).

16. Nella sentenza *Schrems I*, la CGUE ha stabilito che, sebbene il "livello di protezione" nel paese terzo debba essere "sostanzialmente equivalente" a quello garantito nell'UE, *"gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione"*[18]. Pertanto l'obiettivo non è quello di rispecchiare punto per punto la legislazione europea, ma di stabilire le prescrizioni essenziali e centrali della legislazione in esame. L'adeguatezza può essere conseguita anche attraverso una combinazione di diritti degli interessati e obblighi in capo a chi effettua il trattamento dei dati personali o esercita il controllo sul trattamento, uniti al controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono applicabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti a un paese terzo o a un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. La presenza di meccanismi di applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati[19].

17. Nella sentenza *Schrems II*, la CGUE ha ritenuto che le leggi in base alle quali le autorità di intelligence statunitensi possono accedere ai dati personali trasferiti negli Stati Uniti (articolo 702 della

[14] In particolare: sentenza della Corte di giustizia del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner,* C-392/14, ECLI:EU:C:2015:650 e sentenza della Corte di giustizia del 16 luglio 2020, *Data Protection Commissioner/Facebook Ireland Limited e Maximillian Schrems,* C-311/18, ECLI:EU:C:2020:559.

[15] Gruppo di lavoro, Criteri di riferimento per l'adeguatezza, WP 254 rev.01, 28 novembre 2017, come da ultimo rivisti e adottati il 6 febbraio 2018, approvati dall'EDPB il 25 maggio 2018 (in appresso: "criteri di riferimento per l'adeguatezza ai sensi del GDPR").

[16] CGUE, sentenza della Corte di giustizia del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner,* C-392/14, ECLI:EU:C:2015:650 (in appresso: "sentenza *Schrems I* della CGUE").

[17] Sentenza della Corte di giustizia del 16 luglio 2020, *Data Protection Commissione/Facebook Ireland Limited e Maximillian Schrems,* C-311/18, ECLI:EU:C:2020:559 (in appresso "sentenza *Schrems II* della CGUE").

[18] Sentenza *Schrems I* della CGUE, punti 73 e 74.

[19] Criteri di riferimento per l'adeguatezza ai sensi del GDPR, pag. 2.

FISA/decreto presidenziale 12333) limitano in modo sproporzionato i diritti sanciti dagli articoli 7 e 8 della Carta e tali limitazioni non sono inquadrate in modo da corrispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dall'articolo 52, paragrafo 1, seconda frase, della Carta[20].

18. Inoltre, la CGUE ha affermato che il quadro giuridico precedente non forniva garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta, in quanto il meccanismo di mediazione non poteva compensare il fatto che né la direttiva presidenziale 28 (PPD-28) né il decreto presidenziale 12333 garantissero ai cittadini non statunitensi mezzi di ricorso effettivo[21]. Il mediatore mancava di indipendenza nei confronti del potere esecutivo e della facoltà di adottare decisioni vincolanti per i servizi di intelligence statunitensi[22].

19. Il decreto presidenziale 14086, che sostituisce in generale la PPD-28, ha introdotto due nuovi requisiti nel diritto statunitense che riprendono la sentenza *Schrems II* della CGUE: da un lato, il fatto che le attività di intelligence dei segnali saranno condotte soltanto nella misura necessaria a portare avanti una raccolta determinata da una priorità di intelligence convalidata e soltanto nella misura e con modalità proporzionate a detta priorità di intelligence convalidata; e, dall'altro, un meccanismo di ricorso.

20. Nel presente parere, l'EDPB valuta, in particolare, in che misura il DPF e il recente decreto presidenziale 14086 affrontano efficacemente le conclusioni formulate dalla CGUE nella sua sentenza.

1.3 Osservazioni e preoccupazioni generali

1.3.1 Valutazione del diritto interno

21. L'EDPB comprende che la valutazione contenuta nel progetto di decisione fa riferimento ai principi del DPF. Tuttavia l'EDPB gradirebbe ricevere informazioni sul contesto giuridico statunitense in cui operano le organizzazioni del DPF. Ciò consentirebbe di comprendere meglio l'interazione del DPF con il diritto statunitense. Ad esempio, nell'allegato I, sezione 1[23], si stabilisce che i principi del DPF non limitano gli obblighi in materia di tutela della vita privata altrimenti applicabili ai sensi del diritto statunitense, senza descrivere tali obblighi.

1.3.2 Impegni internazionali assunti dagli Stati Uniti

22. A norma dell'articolo 45, paragrafo 2, lettera c), GDPR e dei criteri di riferimento per l'adeguatezza ai sensi del GDPR, nel valutare l'adeguatezza del livello di protezione di un paese terzo la Commissione tiene in considerazione, tra le altre cose, gli impegni internazionali assunti dal paese terzo, o altri obblighi derivanti dalla sua partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali, nonché l'attuazione di tali obblighi.

23. Gli Stati Uniti sono parte di numerosi accordi internazionali che garantiscono il diritto alla tutela della vita privata, come il patto internazionale relativo ai diritti civili e politici (articolo 17), la convenzione sui diritti delle persone con disabilità (articolo 22) e la convenzione sui diritti del fanciullo (articolo 16). Inoltre gli Stati Uniti, in quanto membri dell'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), aderiscono al quadro in materia di tutela della vita privata dell'OCSE, in particolare alle *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*. Il 14 dicembre

[20] Sentenza *Schrems II* della CGUE, punti 184 e 185.
[21] Sentenza *Schrems II* della CGUE, punto 192.
[22] Sentenza *Schrems II* della CGUE, punto 195.
[23] Allegato I, sezione I, ultima frase, del progetto di decisione.

2022, i ministri e i rappresentanti di alto livello dei membri dell'OCSE e dell'Unione europea hanno adottato la *Declaration on Government Access to Personal Data held by Private Sector Entities*. Gli Stati Uniti sono altresì parte della convenzione di Budapest sulla criminalità informatica.

24. Inoltre gli Stati Uniti sono membri del sistema delle norme transfrontaliere in materia di privacy ("CBPR") dei paesi della Cooperazione economica Asia-Pacifico ("APEC"), una certificazione sulla protezione dei dati sostenuta dai governi a cui le imprese possono aderire per dimostrare la conformità a norme in materia di tutela della vita privata riconosciute a livello internazionale. Tali norme in materia di privacy sono state approvate dai leader dell'APEC.

25. L'EDPB prende atto inoltre della partecipazione degli Stati Uniti in veste di Stato osservatore ai lavori del comitato consultivo della convenzione 108 del Consiglio d'Europa.

26. Inoltre l'EDPB prende atto e accoglie con favore il continuo impegno degli organismi statunitensi in seno al consesso istituito di recente nel 2021 della "Tavola rotonda delle autorità del G7 per la protezione dei dati e la tutela della vita privata" (Tavola rotonda del G7 per la protezione dei dati), che riunisce le autorità indipendenti di controllo della protezione dei dati e della tutela della vita privata dei paesi del G7. In tale contesto, gli Stati Uniti hanno sostenuto ad esempio l'ultimo comunicato della Tavola rotonda del G7 per la protezione dei dati[24] adottato l'8 settembre 2022 a Bonn, in Germania, incentrato sul concetto di "Data Free Flow with Trust" (libera circolazione dei dati con fiducia).

1.3.3 Progressi nel settore della legislazione statunitense in materia di protezione dei dati

27. L'EDPB prende atto in particolare degli sviluppi della legislazione in materia di protezione dei dati personali a livello statale negli Stati Uniti. L'EDPB accoglie con favore l'adozione di leggi sulla protezione dei dati che sono entrate in vigore o entreranno in vigore entro il 2023 in cinque Stati (California, Colorado, Connecticut, Virginia e Utah)[25]..

28. L'EDPB rileva inoltre che iniziative corrispondenti per ulteriori leggi statali sono già state avviate in numerosi altri Stati degli Stati Uniti d'America.

29. Inoltre l'EDPB accoglie esplicitamente con favore gli sforzi relativi all'iniziativa bipartisan per una legge federale in materia di protezione dei dati, la legge americana in materia di protezione dei dati e tutela della vita privata (ADPPA, *American Data Privacy and Protection Act*).

1.3.4 Portata del progetto di decisione

30. Ai sensi dell'articolo 1 del progetto di decisione, la Commissione conclude che gli Stati Uniti garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'UE a organizzazioni negli

[24] Tavola rotonda delle autorità del G7 per la protezione dei dati e la tutela della vita privata, *Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces*, 8 settembre 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

[25] Legge sulla protezione dei dati personali dei consumatori della California (*California Consumer Privacy Act*) (2018; in vigore dal 1º gennaio 2020); legge sui diritti alla tutela della vita privata della California (*Califomia Privacy Rights Act*) (2020; pienamente operativo dal 1º gennaio 2023); legge sulla protezione dei dati personali del Colorado (*Colorado Privacy Act*) (2021; in vigore dal 1º luglio 2023); legge sulla protezione dei dati personali del Connecticut (*Connecticut Data Privacy Act*) (2022; in vigore dal 1º luglio 2023); legge sulla protezione dei dati personali dei consumatori della Virginia (*Virginia Consumer Data Protection Act*) (2021; in vigore dal 1º gennaio 2023); legge sulla protezione dei dati personali dei consumatori dello Utah (*Utah Consumer Privacy Act*) (2022; in vigore dal 31 dicembre 2023).

Stati Uniti che sono incluse nell'"Elenco del quadro per la protezione dei dati personali", gestito e reso pubblico dal Dipartimento del Commercio ("DoC") degli Stati Uniti, in conformità con l'allegato I, sezione I, punto 3[26].

31. Il DPF è disponibile per le imprese soggette alla competenza giurisdizionale della FTC o del DoT. Si sottolinea che in futuro potrebbero essere aggiunti altri organi statutari statunitensi con poteri analoghi[27].

1.3.5 Limitazione dell'obbligo di aderire ai principi del DPF

32. Il punto 5, della sezione I, dell'allegato I, prevede che l'adesione ai principi del DPF da parte delle organizzazioni del DPF possa essere limitata, tra l'altro: i) alla misura necessaria per ottemperare all'ordinanza di un organo giurisdizionale o per soddisfare esigenze di interesse pubblico, di contrasto[28] o di sicurezza nazionale[29] (anche nel caso in cui le disposizioni legislative o regolamentari creino obblighi contrastanti); e ii) in base a disposizioni legislative, all'ordinanza di un organo giurisdizionale o a disposizioni regolamentari che creano autorizzazioni esplicite, a condizione che, nell'esercizio di tali autorizzazioni, un'organizzazione del DPF possa dimostrare che la sua inosservanza dei principi del DPF è limitata alla misura in cui ciò sia necessario per soddisfare gli interessi legittimi prevalenti perseguiti da tale autorizzazione.

33. Senza disporre di una conoscenza completa della legislazione statunitense a livello tanto federale quanto statale, è difficile per l'EDPB valutare in dettaglio la portata delle esenzioni elencate in questo paragrafo. Di conseguenza l'EDPB raccomanda che la Commissione includa nel progetto di decisione un chiarimento sulla portata delle esenzioni, comprese le garanzie applicabili ai sensi del diritto statunitense, al fine di individuare meglio l'impatto di tali esenzioni sul livello di protezione degli interessati. L'EDPB sottolinea inoltre che la Commissione dovrebbe essere informata in merito all'applicazione e all'adozione di qualsiasi disposizione legislativa o regolamentare che possa incidere sull'adesione ai principi del DPF, nonché monitorare tali aspetti.

1.3.6 Cambiamenti rispetto allo "scudo per la privacy"

34. L'EDPB accoglie con favore gli sforzi compiuti per rispondere ai requisiti di cui alla sentenza *Schrems II*. Tuttavia l'EDPB avrebbe gradito che un maggior numero di questioni individuate i) nel parere 01/2016 del Gruppo di lavoro e ii) nei passati riesami congiunti[30] fossero state anch'esse affrontate in occasione dei negoziati relativi al DPF.

35. L'EDPB rileva inoltre che, nonostante una serie di modifiche apportate e spiegazioni aggiuntive incluse nei considerando del progetto di decisione, i principi del DPF a cui le organizzazioni del DPF devono

[26] Considerazioni finali, articolo 1, del progetto di decisione (pag. 57). L'EDPB comprende che il progetto di decisione non riguarderà i trasferimenti da soggetti stabiliti al di fuori dell'UE ma tenuti a rispettare il GDPR conformemente all'articolo 3, paragrafo 2, GDPR che si applica a soggetti certificati negli Stati Uniti.

[27] Allegato I, sezione I, punto 2, del progetto di decisione.

[28] Per ulteriori osservazioni sull'uso dei dati personali soggetti all'applicazione del DPF UE-USA per fini di contrasto, cfr. sezione 3.1 del presente parere.

[29] Per ulteriori osservazioni sull'uso dei dati personali soggetti all'applicazione del DPF UE-USA per fini di sicurezza nazionale, cfr. sezione 3.2 del presente parere.

[30] Riesami annuali: scudo UE-USA per la privacy – Primo riesame congiunto annuale, WP255, Relazione del Gruppo di lavoro adottata il 28 novembre 2017 (in appresso: "relazione sul primo riesame congiunto") (solo in EN); scudo UE-USA per la privacy - Secondo riesame congiunto annuale, Relazione dell'EDPB adottata il 22 gennaio 2019 (in appresso: "relazione sul secondo riesame congiunto") (solo in EN); scudo UE-USA per la privacy - Terzo riesame congiunto annuale, Relazione dell'EDPB adottata il 12 novembre 2019 (in appresso: "relazione sul terzo riesame congiunto") (solo in EN).

attenersi rimangono sostanzialmente invariati rispetto a quelli applicabili nel contesto dello scudo per la privacy.

1.3.7 Mancanza di chiarezza nei documenti del DPF

36. L'EDPB osserva che la struttura degli allegati e la loro numerazione rendono le informazioni piuttosto difficili da reperire e da consultare. Ciò contribuisce a una presentazione globalmente complessa del nuovo quadro che raccoglie nei suoi allegati documenti di diverso valore giuridico e può non favorire una buona comprensione dei principi del DPF da parte degli interessati, delle organizzazioni del DPF e delle autorità di protezione dei dati dell'UE.

37. L'EDPB sottolinea inoltre che la terminologia dovrebbe essere utilizzata in modo coerente in tutto il DPF. Attualmente non è così, ad esempio, per la nozione di "trattamento". In effetti alcune parti del DPF enumerano alcuni tipi di trattamenti dei dati anziché utilizzare il termine "trattamento". Ciò può comportare incertezza del diritto e possibili lacune nella protezione[31]

38. L'EDPB accoglie con favore il fatto che le definizioni di alcuni termini utilizzati siano incluse nel DPF[32]. Tuttavia, ciò non è il caso per alcuni altri termini essenziali, quali quanto meno "procuratore" o "responsabile del trattamento", che secondo l'EDPB meritano una definizione chiara e specifica nell'allegato I, sezione I, punto 8, del DPF, e sulla quale concordano tanto gli Stati Uniti quanto l'UE, al fine di evitare confusione in una fase successiva per le organizzazioni del DPF che fanno affidamento al DPF, le autorità di vigilanza e il pubblico in generale.

39. Per quanto riguarda la questione delle interpretazioni divergenti nell'UE e negli USA relative al concetto di dati relativi alle risorse umane (HR), l'EDPB concorda con la relazione della Commissione sul terzo riesame in merito all'obiettivo di proseguire le discussioni con le autorità statunitensi[33].

2 ASPETTI GENERALI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

2.1 Principi sostanziali

2.1.1 Concetti

40. Sulla base dei criteri di riferimento per l'adeguatezza ai sensi del GDPR, le nozioni e/o i principi di base della protezione dei dati devono essere presenti nel quadro giuridico del paese terzo. Sebbene non debbano necessariamente riprendere la terminologia del GDPR, tali nozioni e/o principi dovrebbero rispecchiare ed essere coerenti con le nozioni sancite nel diritto europeo in materia di protezione dei dati. A titolo esemplificativo, il GDPR contiene le seguenti nozioni fondamentali: "dati personali", "trattamento di dati personali", "titolare del trattamento", "responsabile del trattamento", "destinatario" e "dati sensibili". L'EDPB accoglie con favore il fatto che le definizioni dei termini "dati

[31] Ad esempio i) secondo la sezione III, punto 6, lettera f), dell'allegato I, del progetto di decisione, i principi del DPF sarebbero applicabili soltanto quando l'organizzazione "conserva, utilizza o divulga" i dati ricevuti (ossia non per altre operazioni rientranti nel termine "trattamento", quali la raccolta, la registrazione, la modifica, l'estrazione, la consultazione, la cancellazione); e ii) secondo la sezione II, punto 4, lettera a), dell'allegato I, del progetto di decisione, la sicurezza dei dati sarebbe imposta soltanto per la "creazione, il mantenimento, l'utilizzo o la diffusione" di informazioni personali.

[32] Allegato I, sezione I, punto 8, del progetto di decisione.

[33] Relazione sul terzo riesame congiunto, pagg. 5, 15, 16 e 30; cfr. anche il documento di lavoro dei servizi della Commissione che accompagna il documento relazione della Commissione al Parlamento europeo e al Consiglio sul terzo riesame annuale del funzionamento dello scudo UE-USA per la privacy, pagg. 17 e 18.

personali", "trattamento" e "titolare del trattamento" siano incluse nel DPF, come accadeva nello scudo per la privacy.

41. L'EDPB rileva che resta ancora poco chiaro in che misura i principi del DPF siano applicabili alle organizzazioni del DPF che ricevono dati personali dall'Unione a fini esclusivi di trattamento (i cosiddetti "procuratori" o "responsabili del trattamento"). Il DPF non distingue tra principi del DPF applicabili ai procuratori e principi del DPF applicabili ai responsabili del trattamento, mentre numerosi degli obblighi inclusi nei principi del DPF non sono adatti ai procuratori/responsabili del trattamento. Ad esempio un procuratore/responsabile del trattamento non dovrebbe essere in grado di fornire alle persone tutte le indicazioni richieste dal principio sull'informativa (ad esempio le finalità per cui raccoglie e utilizza i dati personali che riguardano dette persone)[34], in quanto un procuratore/responsabile del trattamento non può stabilire in autonomia i mezzi e le finalità del trattamento[35].

2.1.2 Il principio della limitazione della finalità

42. In linea con il GDPR, i criteri di riferimento per l'adeguatezza ai sensi del GDPR prevedono che i dati personali siano trattati per una finalità specifica e successivamente utilizzati esclusivamente nella misura in cui ciò non sia incompatibile con la finalità del trattamento.

43. Il principio sull'integrità dei dati e la limitazione della finalità stabilisce che l'organizzazione non può trattare le informazioni personali in modo incompatibile con le finalità per cui sono state raccolte o con quelle successivamente autorizzate dalla persona[36]. L'EDPB rileva che nel quadro dei principi sull'informativa, sulla scelta e sull'integrità dei dati e sulla limitazione della finalità è utilizzata una terminologia diversa. Come osservato dal Gruppo di lavoro e nonostante gli utili chiarimenti di cui al considerando della bozza di decisione, nel DPF si riscontra l'uso di termini quali "finalità diverse", "finalità materialmente diverse" o "un uso non coerente con" senza fornire una chiara definizione di tali concetti in tale documento e tale circostanza potrebbe determinare incertezza del diritto.

2.1.3 Diritti di accesso, rettifica, cancellazione e opposizione

44. Nel DPF, i diritti degli interessati all'accesso, alla rettifica e alla cancellazione sono disciplinati dal principio dell'accesso[37].

45. Il principio dell'accesso rimane invariato rispetto allo scudo per la privacy. Di conseguenza, alcune preoccupazioni espresse nel parere 01/2016 del Gruppo di lavoro restano valide, come illustrato di seguito.

46. Per quanto concerne il diritto di accesso delle persone, l'EDPB ritiene necessario ribadire che sarebbe meglio inserire i dettagli dell'obbligo di rispondere alle richieste delle persone nel testo principale del principio (tali dettagli sono ancora descritti soltanto in una nota[38]).). Inoltre dovrebbe essere chiaro che l'accesso dovrebbe essere fornito nella misura in cui un'organizzazione del DPF tratta informazioni

[34] Allegato I, sezione II, punto 1, lettera a), del progetto di decisione.
[35] Cfr. anche parere 01/2016 del Gruppo di lavoro, pag. 16.
[36] Allegato I, sezione II, punto 5, del progetto di decisione.
[37] Allegato I, sezione II, punto 6 e sezione III, punto 8, lettera a) sottopunto i), del progetto di decisione.
[38] Allegato I, sezione III, punto 8, lettera a), sottopunto i), numero 1 e nota 14 del progetto di decisione.

personali, non soltanto quando le "conserva"[39]. Secondo l'EDPB, l'attuale formulazione potrebbe portare a un'interpretazione restrittiva del diritto di accesso.

47. Per quanto concerne l'elenco delle eccezioni al diritto di accesso[40], alcune tendono ancora a far propendere l'equilibrio a favore degli interessi delle organizzazioni del DPF. L'EDPB continua a nutrire preoccupazioni circa il fatto che, in tali casi, non sembra esserci alcun obbligo di tenere conto dei diritti e degli interessi della persona fisica[41].

48. Un'altra eccezione, che è stata oggetto di precedenti preoccupazioni da parte del Gruppo di lavoro[42] e che all'EDPB sembra eccessivamente ampia, è l'eccezione al diritto di accesso per le informazioni pubblicamente disponibili e le informazioni provenienti da registri pubblici[43]. L'EDPB ha ripetutamente affermato che, ai sensi del diritto dell'UE, gli interessati hanno sempre il diritto di accedere ai propri dati, indipendentemente dal fatto che tali dati personali siano stati pubblicati o meno. Qualora le richieste di accesso dovessero essere respinte sulla base del fatto che i dati sono stati ottenuti da fonti pubblicamente disponibili o da registri pubblici, le persone perderebbero la possibilità di controllare l'accuratezza dei dati e di controllare se i dati sono stati innanzitutto resi pubblici legalmente.

49. L'EDPB ricorda che il diritto di accesso è sancito dall'articolo 8, paragrafo 2, della Carta. Pur non essendo un diritto assoluto, esso è fondamentale per il diritto alla protezione dei dati personali, in quanto facilita l'esercizio degli altri diritti dell'interessato, quali il diritto di rettifica e il diritto alla cancellazione e il diritto di opposizione[44].

50. Oltre ai diritti di accesso, cancellazione ed eliminazione, gli interessati dovrebbero avere il diritto di opporsi in qualsiasi momento, per motivi legittimi cogenti relativi alla loro situazione particolare, al trattamento dei dati che li riguardano a determinate condizioni previste dalla legislazione del paese terzo[45].

51. Con il principio della scelta, il DPF prevede il diritto di scegliere (facoltà di rifiuto) se le informazioni personali possano essere rivelate a terzi ovvero usate per finalità sostanzialmente diverse[46]. Le persone possono inoltre esercitare in qualunque momento la facoltà di rifiuto in rapporto all'uso delle loro informazioni personali che le riguardano a fini di marketing diretto[47]. Fatta eccezione per il contesto delle finalità di marketing diretto, le modalità, in particolare i tempi, per l'esercizio del diritto di opposizione non sono specificati nel dettaglio. Pertanto l'EDPB invita la Commissione a chiarire come le persone possano esercitare il loro diritto di opposizione.

52. Come indicato nel parere 01/2016 del Gruppo di lavoro, l'EDPB ritiene che il semplice riferimento all'esistenza di tale diritto nella politica della privacy non sia sufficiente. L'opportunità individualizzata di esercitare tale diritto deve essere offerta non soltanto in caso di divulgazione o riutilizzo di informazioni personali. L'EDPB sottolinea che all'interno del DPF dovrebbe essere previsto un diritto generale di opposizione per motivi preminenti e legittimi relativi alla situazione particolare dell'interessato. L'EDPB raccomanda di garantire in qualsiasi momento tale diritto di opposizione e

[39] Allegato I, sezione III, punto 8, lettera d), punto ii), del progetto di decisione.
[40] Allegato I, sezione III, punto 8, lettera e), del progetto di decisione.
[41] Parere 01/2016 del Gruppo di lavoro, punto 2.2.5.
[42] Parere 01/2016 del Gruppo di lavoro, punto 2.2.9.
[43] Allegato I, sezione III, punto 15, lettere d) ed e), del progetto di decisione.
[44] Parere 01/2016 del Gruppo di lavoro, punto 2.2.5.
[45] Capitolo 3, sezione A, punto 8, dei criteri di riferimento per l'adeguatezza in materia di GDPR.
[46] Allegato I, sezione II, punto 2, lettera a), del progetto di decisione.
[47] Allegato I, sezione III, punto 12, lettera a), del progetto di decisione.

raccomanda inoltre di non circoscrivere tale diritto al solo ambito d'uso dei dati per finalità di marketing diretto[48].

53. In relazione ai dati sulle risorse umane, l'EDPB apprezza i chiarimenti della Commissione in merito all'applicazione dei principi di notifica e di scelta nella situazione in cui un'organizzazione statunitense certificata intenda utilizzare i dati relativi alle risorse umane per una finalità diversa, non legata all'occupazione, quali comunicazioni di marketing[49]. Tuttavia l'EDPB sostiene che l'ulteriore trattamento di dati relativi alle risorse umane per finalità non legate all'occupazione sarà considerato nella maggior parte dei casi incompatibile con la finalità originaria e che il consenso sarà raramente prestato in maniera del tutto libera quando viene concesso in un contesto lavorativo.

54. L'EDPB ribadisce inoltre le preoccupazioni del Gruppo di lavoro in relazione all'esenzione dai principi di notifica e di scelta per i dati relativi alle risorse umane "*in quanto e fino a che ciò risulti necessario per non ledere la capacità dell'organizzazione di procedere a promozioni e nomine o prendere decisioni analoghe relative al personale*"[50], che per l'EDPB appare ampia e vaga[51].

2.1.4 Limitazioni ai trasferimenti successivi

55. I trasferimenti successivi di dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento. Il livello di tutela delle persone i cui dati sono trasferiti non deve essere compromesso dal trasferimento successivo. Spetta al primo destinatario dei dati trasferiti dall'UE assicurare che siano previste garanzie adeguate per i trasferimenti successivi dei dati in mancanza di una decisione di adeguatezza. Tali trasferimenti successivi di dati dovrebbero essere possibili soltanto per finalità determinate e limitate e purché sussista una base giuridica per il trattamento[52].

56. Secondo il principio della responsabilizzazione per i trasferimenti successivi di cui al DPF, i trasferimenti successivi possono avvenire soltanto per finalità limitate e specifiche, sulla base di un contratto stipulato tra l'organizzazione del DPF e la terza parte (oppure di un accordo analogo all'interno di un gruppo aziendale) e soltanto se tale contratto prevede che la terza parte fornisca il medesimo livello di protezione garantito dai principi del DPF[53].

57. L'EDPB desidera ribadire le preoccupazioni espresse nel parere 01/2016 del Gruppo di lavoro in merito all'esenzione dall'obbligo di contratto per i trasferimenti tra titolari del trattamento all'interno di un gruppo di società[54]. In relazione ai dati relativi alle risorse umane, l'EDPB continua a non comprendere

[48] Parere 01/2016 del Gruppo di lavoro, punto 2.2.2.
[49] Allegato I, sezione III, punto 9, lettera b), sottopunto i), nonché considerando 15 e nota 27 del progetto di decisione.
[50] Allegato I, sezione III, punto 9, lettera b), sottopunto iv), del progetto di decisione.
[51] Parere 01/2016 del Gruppo di lavoro, punto 2.2.7.
[52] Capitolo 3, sezione A, punto 9, dei criteri di riferimento per l'adeguatezza in materia di GDPR.
[53] Allegato I, sezione II, punto 3, del progetto di decisione.
[54] Allegato I, sezione III, punto 10, lettera b), sottopunto i), del progetto di decisione che fa riferimento a "o altri strumenti infragruppo (ad esempio, programmi di conformità e di controllo") che apparentemente non devono essere vincolanti.

la logica dell'esenzione dall'obbligo di stipulare un contratto con un terzo titolare del trattamento in caso di trasferimenti successivi per "esigenze operative occasionali di natura occupazionale"[55].

58. Inoltre l'EDPB desidera ribadire la richiesta del Gruppo di lavoro[56] secondo la quale, prima di un trasferimento successivo, le organizzazioni vincolate dal quadro dovrebbero valutare che i requisiti obbligatori di cui alla legislazione nazionale del paese terzo applicabile al destinatario non compromettano la continuità della protezione degli interessati i cui dati sono trasferiti[57].

59. L'EDPB sostiene che i trasferimenti successivi di dati personali verso paesi terzi potrebbero comportare interferenze con i diritti fondamentali delle persone e invita la Commissione a chiarire che le garanzie imposte dal destinatario iniziale all'importatore nel paese terzo devono essere efficaci alla luce della legislazione del paese terzo, prima di un trasferimento successivo nel contesto del DPF[58].

2.1.5 Processo decisionale automatizzato, compresa la profilazione

60. Le decisioni basate unicamente sul trattamento automatizzato (processo decisionale automatizzato relativo alle persone fisiche), compresa la profilazione, che producono effetti giuridici che riguardano l'interessato o incidono significativamente sulla sua persona sono ammesse soltanto a determinate condizioni stabilite dal quadro giuridico del paese terzo. Nel quadro europeo tali condizioni comprendono, per esempio, la necessità di ottenere il consenso esplicito dell'interessato o la necessità di tale decisione per la conclusione di un contratto. Se la decisione non è conforme alle condizioni stabilite dal quadro giuridico del paese terzo, l'interessato dovrebbe avere il diritto di non essere sottoposto alle sue prescrizioni. Il diritto del paese terzo dovrebbe, in ogni caso, prevedere le necessarie garanzie, compreso il diritto a essere informato sui motivi particolari sottesi alla decisione e sulla sua logica, a rettificare informazioni inaccurate o incomplete e a contestare la decisione qualora questa sia stata adottata sulla base di un fondamento di fatto errato[59].

61. Il DPF non prevede garanzie giuridiche specifiche nel caso in cui le persone siano sottoposte a decisioni che producono effetti giuridici o abbiano effetti significativi nei loro confronti fondate esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della loro personalità, quali il rendimento professionale, il credito, l'affidabilità o il comportamento.

62. Come già considerato nel parere 01/2016 del Gruppo di lavoro e dall'EDPB nei suoi precedenti pareri sulle decisioni di adeguatezza relative al Giappone e alla Corea del Sud[60], l'EDPB ritiene che i rapidi

[55] Allegato I, sezione III, punto 9, lettera e), sottopunto i), del progetto di decisione, che fa riferimento ad esempi quali la copertura assicurativa.

[56] Parere 01/2016 del Gruppo di lavoro, punto 2.2.3, pag. 21.

[57] Alla luce della sentenza *Schrems II*, l'EDPB ha chiarito ulteriormente gli obblighi per gli esportatori e gli importatori di dati in relazione a trasferimenti successivi in una serie di orientamenti e raccomandazioni: cfr. EDPB, raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE (versione 2.0, adottate il 18 giugno 2021); raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza (adottate il 10 novembre 2020); linee guida 4/2021 sui codici di condotta come strumento per i trasferimenti (versione 2.0, adottate il 22 febbraio 2022); raccomandazioni 1/2022 relative alla domanda di omologazione e agli elementi e ai principi che devono essere presenti nelle norme vincolanti d'impresa dei titolari del trattamento (solo in EN) (adottate il 14 novembre 2022); linee guida 07/2022 relative alla certificazione come strumento per i trasferimenti (solo in EN) (adottate in seguito a consultazione pubblica il 14 febbraio 2023).

[58] Parere 01/2016 del Gruppo di lavoro, punto 2.2.3, pag. 21.

[59] Capitolo 3, sezione B, punto 3, dei criteri di riferimento per l'adeguatezza in materia di GDPR.

[60] EDPB, parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali in Giappone, adottato il 5 dicembre 2018; EDPB, parere 32/2021

sviluppi nel settore del processo decisionale automatizzato e della profilazione, sempre più spesso ricorrendo all'uso di tecnologie di intelligenza artificiale, richiedano particolare attenzione a questo proposito[61].

63. L'EDPB prende atto delle argomentazioni della Commissione, secondo cui è improbabile che l'assenza di norme specifiche sul processo decisionale automatizzato nel DPF incida sul livello di protezione dei dati personali raccolti nell'Unione (dato che qualsiasi decisione basata sul trattamento automatizzato verrebbe di norma presa dal titolare del trattamento nell'Unione che ha un rapporto diretto con l'interessato in questione)[62].. Tuttavia, secondo l'EDPB, non si può escludere che un titolare del trattamento stabilito negli Stati Uniti possa utilizzare un processo decisionale automatizzato sui dati trasferiti ai sensi del progetto di decisione (ad esempio nel contesto di un rapporto di lavoro, per valutare il rendimento sul lavoro, l'assicurazione, l'alloggio).

64. L'EDPB accoglie con favore i riferimenti della Commissione alle garanzie specifiche previste dal diritto statunitense in settori diversi[63]. Tuttavia, secondo l'EDPB, il livello di protezione per le persone sembra variare a seconda delle norme settoriali specifiche, laddove esistano, che si applicano alla situazione in questione. Esiste il rischio che alcune situazioni non siano incluse in quanto non rientrano nell'ambito di applicazione degli atti a cui si fa riferimento. Inoltre il contenuto dei diritti individuali in relazione al processo decisionale automatizzato è descritto in modo diverso nei vari atti.

65. In tale contesto l'EDPB ritiene che, al fine di fornire garanzie sufficienti, siano necessarie norme specifiche nel DPF sul processo decisionale automatizzato, tra cui il diritto della persona fisica di conoscere la logica applicata, di contestare la decisione e di ottenere l'intervento umano quando la decisione la riguarda in modo significativo[64].

2.2 Meccanismi di procedura e applicazione

66. L'EDPB rileva che il DPF continua a basarsi su un sistema di autocertificazione, anche se la Commissione lo definisce un sistema di "certificazione".

67. L'EDPB ricorda i miglioramenti ottenuti nel corso dei precedenti riesami congiunti. Ad esempio, per quanto riguarda il ruolo del DoC, sul processo di (ri)autocertificazione [...], sul monitoraggio della conformità delle società ai principi del DPF (ad esempio attraverso controlli a campione, l'uso di questionari di conformità) e sull'individuazione e sulla risoluzione di false dichiarazioni di partecipazione (ad esempio attraverso ricerche su internet).

68. Allo stesso tempo, il Gruppo di lavoro e l'EDPB hanno espresso preoccupazioni in relazione a una certa mancanza di vigilanza sul rispetto dei requisiti dello scudo per la privacy[65]. In particolare l'EDPB concorda con le conclusioni della Commissione dopo il terzo riesame annuale dello scudo per la privacy, secondo cui, nel contesto dello scudo per la privacy, verifiche casuali condotte dal DoC tendevano a essere circoscritte ai requisiti formali, evidenziando ad esempio la mancata risposta da

relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nella Repubblica di Corea, adottato il 24 settembre 2021.

[61] Cfr., tra l'altro, domanda di pronuncia pregiudiziale nella causa C-634/21, *OQ/Land Hesse (SCHUFA Holding e altri)* (pendente).

[62] Considerando 33 e 34 del progetto di decisione.

[63] Considerando 35 del progetto di decisione.

[64] Cfr. anche relazione sul terzo riesame congiunto, punto 76.

[65] Relazione sul terzo riesame congiunto, punto 7.

parte del referente nominato o l'assenza di una politica della privacy dell'impresa consultabile in rete)[66]. L'EDPB ritiene che i controlli di conformità in merito a requisiti più sostanziali siano fondamentali.

69. L'EDPB ricorda altresì l'importanza di una vigilanza efficace (anche per quanto concerne il rispetto dei requisiti sostanziali) e dell'applicazione del DPF. Tale aspetto sarà monitorato attentamente dall'EDPB, anche nel contesto dei riesami periodici.

70. Per quanto concerne le attività di contrasto, l'EDPB prende atto dei rinnovati impegni contenuti nelle lettere della FTC[67] e del DoT[68] di dare priorità alle indagini sulle presunte violazioni del DPF, di adottare le opportune misure di contrasto nei confronti dei soggetti che rilasciano dichiarazioni false o ingannevoli di partecipazione al quadro, di monitorare i provvedimenti coercitivi relativi alle violazioni del DPF e di collaborare con le autorità di protezione dei dati dell'UE. A questo proposito, l'EDPB riconosce altresì che la FTC ha dichiarato che prevede di concentrare ulteriormente i propri sforzi in materia di contrasto sulle violazioni sostanziali del DPF e che intende indagare (anche) di propria iniziativa. Tali aspetti saranno monitorati attentamente dall'EDPB, anche nel contesto dei riesami periodici.

2.3 Meccanismi di ricorso

71. L'EDPB accoglie con favore la chiara presentazione, nel progetto di decisione, dei sette mezzi di ricorso offerti agli interessati dell'UE in caso di trattamento dei loro dati personali in violazione del DPF[69].

72. Tali diversi meccanismi di ricorso sono stabiliti in conformità con i requisiti del principio di ricorso, controllo e responsabilità e del principio supplementare 11 sulla "risoluzione delle controversie e modalità di controllo dell'applicazione" emanato dal DoC e menzionato nell'allegato I del progetto di decisione[70].

73. Come sottolineato dalla Commissione nel suo progetto di decisione, "*all'interessato dovrebbero essere riconosciuti mezzi di ricorso effettivi in sede amministrativa e giudiziaria*"[71]. Ciò riprende il requisito di cui all'articolo 45, paragrafo 2, lettera a), GDPR secondo il quale, nel valutare l'adeguatezza del livello di protezione garantito da un paese terzo, la Commissione deve prendere in considerazione in particolare "un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento"[72]. Tale requisito è richiamato anche dai criteri di riferimento per l'adeguatezza ai sensi del GDPR[73].

74. L'EDPB rileva che tali meccanismi di ricorso sono i medesimi inclusi nel precedente scudo per la privacy, che erano stati oggetto di osservazioni da parte del Gruppo di lavoro[74].

---

[66] Relazione della Commissione al Parlamento europeo e al Consiglio sul terzo riesame annuale del funzionamento dello scudo UE-USA per la privacy (COM(2019) 495 final del 23.10.2019), pag. 4.
[67] Allegato IV del progetto di decisione.
[68] Allegato V del progetto di decisione.
[69] Considerando 67 del progetto di decisione.
[70] Allegato I, sezione II, punto 7 e sezione III, punto 11, nonché allegato I dell'allegato I, del progetto di decisione.
[71] Considerando 64 del progetto di decisione.
[72] Cfr. anche considerando 141 GDPR che fa riferimento all'articolo 47 della Carta per il diritto a un ricorso giurisdizionale effettivo nell'UE.
[73] Criteri di riferimento per l'adeguatezza ai sensi del GDPR, pag. 8.
[74] Cfr. in particolare il parere 01/2016 del Gruppo di lavoro, sezione 2.2.6, lettera a).

75. Per quanto concerne il meccanismo di arbitrato, l'EDPB osserva che tale opzione non è disponibile per quanto riguarda le eccezioni ai principi del DPF[75] e pertanto rimanda alla sua osservazione di cui al punto 33.

76. Per quanto concerne gli ulteriori mezzi di ricorso giudiziario previsti dalla legislazione statunitense, l'EDPB accoglierebbe altresì con favore ricevere ulteriori dettagli sulla legislazione citata[76] e rimanda alla sua osservazione di cui al punto 21.

77. Inoltre l'EDPB accoglie con favore la lettera della FTC che descrive la sua intenzione di lavorare a stretto contatto con le autorità di protezione dei dati dell'UE[77]. L'EDPB accoglie inoltre con favore l'attribuzione di priorità ai reclami da parte della FTC, anche se ciò potrebbe non dare certezza all'interessato che i suoi reclami saranno trattati in tutti i casi.

78. Per quanto concerne la possibilità, in alcuni casi, offerta alle persone di presentare i loro reclami presso un'autorità di protezione dei dati dell'UE, l'EDPB gradirebbe ulteriori informazioni: i) in merito all'eventualità o meno che la possibilità per le autorità di protezione dei dati dell'UE di fornire consulenza in merito a misure correttive o compensative possa includere la raccomandazione di sanzioni pecuniarie o l'uso di poteri investigativi; e ii) in merito alla misura in cui l'azione di un'autorità di protezione dei dati dell'UE verrebbe presa in considerazione come prova per un'azione di contrasto da parte della FTC o del DoT[78].

79. L'efficacia dei meccanismi di ricorso sarà monitorata attentamente dall'EDPB, anche nel contesto dei riesami periodici.

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

3.1 Accesso e utilizzo per finalità di contrasto penale

3.1.1 L'accesso delle autorità di contrasto ai dati personali dovrebbe essere basato su norme chiare, precise e accessibili

80. L'EDPB accoglie con favore le informazioni e le spiegazioni più dettagliate, rispetto alla precedente decisione di adeguatezza, fornite nel progetto di decisione per quanto concerne l'accesso e l'uso di dati personali da parte delle autorità pubbliche statunitensi per finalità di contrasto penale. L'allegato VI del progetto di decisione contiene altresì una lettera della Divisione penale del Dipartimento della Giustizia degli Stati Uniti nella quale è fornita "una breve panoramica dei principali strumenti investigativi usati negli USA per ottenere dalle imprese dati commerciali e altre informazioni a fini di applicazione della normativa penale o per scopi (civili e regolamentari) d'interesse pubblico, corredata delle limitazioni di accesso che si applicano ai relativi poteri". Secondo tale lettera, tutte le procedure giuridiche descritte nella lettera sono utilizzate per ottenere informazioni da società negli Stati Uniti, senza tener conto della nazionalità o del luogo di residenza dell'interessato e derivano direttamente dalla costituzione degli Stati Uniti (quarto emendamento), dalla legislazione e dal diritto processuale oppure dagli orientamenti e dalle politiche del Dipartimento della Giustizia. Tale panoramica non tratta

[75] Allegato I dell'allegato I, sezione A, del progetto di decisione.
[76] Considerando 85 del progetto di decisione.
[77] Allegato IV del progetto di decisione.
[78] Allegato I, sezione III, punto 5, lettera b), punto iii), del progetto di decisione.

degli strumenti investigativi di sicurezza nazionale utilizzati dalle forze dell'ordine nelle indagini in materia di terrorismo e nelle indagini concernenti altri aspetti della sicurezza nazionale[79].

81. L'EDPB osserva che il progetto di decisione e l'allegato VI si occupano principalmente delle autorità federali preposte all'applicazione della legge e di quelle di regolamentazione[80] e non fanno riferimento specifico a normative ai sensi del diritto degli Stati federati che prevedono il ricorso a tali procedure per ottenere informazioni. L'allegato VI menziona anche che "secondo il settore specifico in cui opera e la tipologia di dati che detiene, l'impresa può addurre altre basi giuridiche per contestare la richiesta di dati presentata dall'ente amministrativo" e offre vari esempi non esaustivi, quali la legge sul segreto bancario e i suoi regolamenti attuativi[81], la legge sull'informativa corretta nel credito[82] e la legge sul diritto alla privacy finanziaria[83]. L'EDPB osserva che la base giuridica applicabile a una determinata domanda di accesso dipende dalla natura dei dati richiesti, dal tipo di impresa, dalla natura delle procedure giuridiche (penale, amministrativa, relativa ad altro interesse pubblico) e dal tipo di ente che chiede l'accesso. Poiché tutte le norme applicabili che limitano l'accesso delle autorità di contrasto ai dati trasferiti negli Stati Uniti si basano sulla costituzione, sulla legge e su politiche trasparenti del Dipartimento della Giustizia, l'EDPB riconosce l'accessibilità di tali norme e invita la Commissione a tenere conto di tale aspetto nel progetto di decisione. Dall'allegato VI si desume che tali normative si applicano indipendentemente dalla nazionalità o dal luogo di residenza dell'interessato e, in generale, integrano i requisiti del quarto emendamento (anche se spesso vanno oltre e includono ulteriori protezioni).

82. In conclusione, l'EDPB prende atto della valutazione più dettagliata contenuta nel progetto di decisione rispetto alla precedente decisione di adeguatezza per quanto riguarda l'accesso da parte delle autorità federali di contrasto. Per quanto concerne l'accesso da parte delle autorità di contrasto degli Stati federati, l'EDPB prende atto del fatto che, ai sensi dell'allegato VI, le tutele previste dal diritto statale devono essere almeno equivalenti a quelle di cui alla costituzione degli Stati Uniti, compreso, a titolo esemplificativo ma non esaustivo, il quarto emendamento. L'EDPB invita la Commissione a valutare ulteriormente l'aspetto della protezione offerta dal diritto degli Stati federati nei futuri riesami.

3.1.2 Devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti

83. L'EDPB rileva che la richiesta di accesso ai dati per finalità di contrasto può essere considerata, in generale, una richiesta che persegue un obiettivo legittimo. Tuttavia, allo stesso tempo, tali ingerenze sono accettabili solo se necessarie e proporzionate[84].

---

[79] Allegato VI, nota 1, del progetto di decisione.
[80] Cfr. considerando da 90 a 93 del progetto di decisione.
[81] Codice degli Stati Uniti d'America, titolo 31, articolo 5318; codice dei regolamenti federali, titolo 31, capitolo X.
[82] Codice degli Stati Uniti d'America, titolo 15, articolo 1681b.
[83] Codice degli Stati Uniti d'America, titolo 12, articoli da 3 401 a 3 423.
[84] Cfr. sentenza della Corte di giustizia del 6 ottobre 2020, *La Quadrature du Net e a./Premier ministre e a.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791 (in appresso "sentenza *La Quadrature du Net* della CGUE"), punto 140. Cfr. anche garante europeo della protezione dei dati (GEPD), Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: un pacchetto di strumenti (solo in EN), 11 aprile 2017 e GEPD, Linee guida sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale (solo in EN), 19 dicembre 2019.

84. Secondo una costante giurisprudenza della CGUE, il principio di proporzionalità esige che le misure legislative che introducono ingerenze nei diritti al rispetto della vita privata e alla protezione dei dati personali siano idonee "a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non superino i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi"[85]. Pertanto, in linea di massima, la valutazione della necessità e proporzionalità è sempre effettuata in relazione a una misura specifica contemplata dalla legislazione.

85. Nell'allegato VI le autorità statunitensi precisano che i procuratori federali e gli inquirenti federali hanno facoltà di accesso ai documenti e ad altre informazioni detenute dalle organizzazioni attivando "varie procedure giuridiche obbligatorie, tra cui citazioni dinanzi al grand jury, citazioni amministrative e mandati di perquisizione" e possono acquisire altre comunicazioni "in virtù dei poteri di intercettazione delle comunicazioni e dei dati informativi conferiti per le indagini penali federali"[86]. Inoltre gli enti che hanno competenze civili o di regolamentazione possono citare le organizzazioni ingiungendo loro di trasmettere "documenti aziendali, informazioni conservate su supporto elettronico o altri beni materiali"[87]. I processi stessi sono spiegati anche nei considerando da 90 a 93 del progetto di decisione. A questo proposito l'EDPB prende atto di un'evoluzione positiva, citata nel progetto di decisione, della giurisprudenza statunitense relativa alle informazioni conservate elettronicamente[88].

86. L'allegato VI precisa inoltre che tali procedure giuridiche sono non discriminatorie e seguite in generale per ottenere informazioni dalle "imprese" presenti negli USA, indipendentemente dal fatto che siano certificate o meno ai sensi del quadro UE-USA per la protezione dei dati personali, e "a prescindere dalla cittadinanza o dal luogo di residenza dell'interessato".

87. Inoltre l'allegato VI contiene conclusioni relative alle garanzie offerte dal quarto emendamento della costituzione degli Stati Uniti, secondo cui le perquisizioni e i sequestri da parte delle autorità di contrasto sono soggette principalmente all'ottenimento di un mandato rilasciato da un organo giurisdizionale, previa dimostrazione del motivo plausibile e dei requisiti di particolarità, e fa riferimento al fatto che, in casi eccezionali nei quali il requisito del mandato non si applica, l'attività di contrasto è soggetta a una verifica della ragionevolezza ai sensi del quarto emendamento[89]. Una persona soggetta a perquisizione o i cui beni sono soggetti a perquisizione può chiedere la cancellazione delle prove ottenute o derivate da una perquisizione illegale se tali prove vengono presentate contro tale persona durante un processo penale[90].

88. In conclusione, l'EDPB rileva che il sistema di strumenti investigativi usati per ottenere dati commerciali e altre informazioni dalle imprese presenti negli Stati Uniti per finalità di contrasto penale o di interesse

---

[85] Cfr. sentenza della Corte di giustizia dell'8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238 (in appresso: "sentenza *Digital Rights Ireland* della CGUE"), punto 46 e giurisprudenza ivi citata.

[86] Allegato VI del progetto di decisione, pag. 2.

[87] Allegato VI del progetto di decisione, pag. 4.

[88] Cfr. nota 146 del progetto di decisione. In una sentenza del 2018, la Corte Suprema degli Stati Uniti ha confermato che le autorità di contrasto necessitano di un mandato di perquisizione o di un'eccezione al mandato anche per l'accesso a registrazioni storiche dell'ubicazione del sito a livello di cella, che forniscono una panoramica completa dei movimenti di un utente e che l'utente può nutrire una ragionevole aspettativa di tutela della vita privata rispetto a tali informazioni (*Timothy Ivory Carpenter c. Stati Uniti d'America*, n. 16-402, 585 U.S. (2018)).

[89] Cfr. allegato VI del progetto di decisione, pag. 2.

[90] Cfr. considerando 90 del progetto di decisione.

pubblico, comprese le limitazioni e le garanzie relative all'accesso, rappresenta un sistema completo ma anche complesso di misure che rispecchia, tra l'altro, la natura federale del governo degli Stati Uniti.

89. Di conseguenza il sistema di misure investigative di contrasto negli Stati Uniti può essere considerato in genere conforme ai requisiti di necessità e proporzionalità in relazione ai diritti fondamentali al rispetto della vita privata e alla protezione dei dati.

3.1.3 Dovrebbe esistere un meccanismo di controllo indipendente

90. L'EDPB prende debita nota del fatto che la maggioranza delle procedure descritte nel progetto di decisione e nell'allegato VI presuppone che un organo giurisdizionale emetta una decisione prima che le autorità siano autorizzate ad accedere ai dati (ad esempio ordinanze di un organo giurisdizionale relative ai dispositivi d'intercettazione dei dati informativi della comunicazione in entrata e in uscita[91], ordinanze di un organo giurisdizionale che dispongono la sorveglianza a norma della legge federale sulle intercettazioni[92], mandati di perquisizione – articolo 41 del regolamento federale di procedura penale[93]). Tuttavia sembra che non tutte le procedure richiedano il previo intervento di un organo giurisdizionale. Ad esempio le autorità che hanno competenze civili o di regolamentazione "possono citare" le imprese[94]. In tali casi esiste tuttavia la possibilità di un controllo giurisdizionale ex post sulla ragionevolezza della citazione, giacché "[i]l destinatario della citazione amministrativa può contestarne l'esecuzione in sede giudiziaria"[95].

91. Inoltre il progetto di decisione descrive la vigilanza sulle agenzie federali di contrasto penale da parte di vari organi, dal controllo interno da parte degli addetti alla tutela della vita privata e alle libertà civili fino al controllo esterno effettuato dall'ispettore generale e da specifiche commissioni in seno al Congresso degli Stati Uniti[96]. La Commissione europea fornisce informazioni articolate e dettagliate e in genere giunge a conclusioni comprensibili. Pertanto l'EDPB si astiene dal riprodurre constatazioni e valutazioni fattuali nel presente parere.

92. Sulla base delle informazioni disponibili, l'EDPB rileva che, riguardo all'accesso delle autorità di contrasto ai dati detenuti da imprese presenti negli Stati Uniti, esiste un meccanismo di vigilanza indipendente piuttosto solido.

3.1.4 La persona fisica deve poter accedere a mezzi di ricorso efficaci

93. Secondo la giurisprudenza della CGUE, una persona fisica deve disporre di un ricorso effettivo per soddisfare i propri diritti quando ritiene che non siano o non siano stati rispettati. Nella sentenza *Schrems I* la CGUE ha spiegato che "una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione

[91] Cfr. considerando 92 del progetto di decisione.
[92] Cfr. allegato VI del progetto di decisione, pag. 3.
[93] Cfr. considerando 90 e allegato VI, pag. 3, del progetto di decisione.
[94] Cfr. allegato VI, pag. 4 e considerando 91 del progetto di decisione.
[95] Cfr. allegato VI, pag. 4 e considerando 91 del progetto di decisione.
[96] Cfr. considerando da 103 a 106 del progetto di decisione.

siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo"[97].

94. Il progetto di decisione[98] e il suo allegato VI contengono ulteriori indicazioni riguardo alle possibilità di ricorso offerte dal diritto positivo alle persone quando le autorità pubbliche ottengono illegalmente accesso ai loro dati.

95. A questo proposito, secondo la Commissione[99], il Codice degli Stati Uniti d'America, titolo 5, articolo 702 (legge sulla procedura amministrativa (APA, *Administrative Procedure Act*)) stabilisce che una chiunque subisca un illecito, un inconveniente o un torto a causa dell'azione di un ente pubblico, ai sensi di una disposizione pertinente, ha diritto di ricorrere al sindacato giurisdizionale.

96. Inoltre la legge sulle comunicazioni conservate, (SCA, *Stored Communications Act*) (emanata come titolo II della legge sulla privacy nelle comunicazioni elettroniche) stabilisce che, chiunque subisca un pregiudizio in ragione di una violazione di tale capitolo, nel contesto del quale la condotta che costituisce la violazione sia stata posta in essere consapevolmente o intenzionalmente, può, nel contesto di un'azione civile, ottenere dalla persona o dal soggetto che ha commesso tale violazione, diversa/o dagli Stati Uniti, il risarcimento più idoneo[100]. Inoltre chiunque subisca un pregiudizio in ragione di una violazione intenzionale di tale capitolo o del capitolo 119 può intentare un'azione dinanzi la Corte distrettuale degli Stati Uniti nei confronti degli Stati Uniti al fine di ottenere un risarcimento in denaro[101].

97. Inoltre il progetto di decisione contiene altresì informazioni sul diritto di ottenere accesso a registrazioni delle agenzie federali a norma della legge sulla libertà d'informazione (FOIA, *Freedom of Information Act*)[102] e a diverse altre normative che garantiscono alle persone il diritto di promuovere una causa contro un'autorità pubblica o un funzionario degli Stati Uniti in relazione al trattamento dei loro dati personali, quali la legge sulle intercettazioni (*Wiretap Act*), la legge sulle frodi e gli abusi informatici (*Computer Fraud and Abuse Act*), la legge federale sulle rivendicazioni per fatti illeciti (*Federal Torts Claim Act*), la legge sul diritto alla privacy finanziaria (*Right to Financial Privacy Act*) e la legge sull'informativa corretta nel credito (*Fair Credit Reporting Act*)[103].

98. L'EDPB accoglie quindi con favore i chiarimenti forniti dalla Commissione sul numero di mezzi di ricorso su cui le persone possono fare affidamento. L'EDPB invita inoltre la Commissione a chiarire ulteriormente se tali mezzi di ricorso consentano all'interessato di "accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati", come richiesto dalla CGUE.

3.1.5 Ulteriore utilizzo delle informazioni raccolte

3.1.5.1 Ulteriore utilizzo dei dati trasferiti a cui le autorità di contrasto all'interno degli Stati Uniti hanno accesso

99. L'EDPB rileva positivamente che il progetto di decisione valuta l'ulteriore utilizzo dei dati a cui hanno accesso le autorità di contrasto negli Stati Uniti. Tuttavia l'EDPB si rammarica che venga fornito

[97] Sentenza *Schrems I* della CGUE, punto 95.
[98] Cfr. considerando da 107 a 112 del progetto di decisione.
[99] Cfr. considerando 109 del progetto di decisione.
[100] Codice degli Stati Uniti d'America, titolo 18, articolo 2707.
[101] Codice degli Stati Uniti d'America, titolo 18, articolo 2712.
[102] Cfr. considerando 111 del progetto di decisione.
[103] Cfr. considerando 112 del progetto di decisione.

soltanto un esempio dei motivi per cui le informazioni possono essere ulteriormente diffuse[104]. A questo proposito, l'EDPB raccomanda alla Commissione di includere nel progetto di decisione ulteriori chiarimenti sui principi e sulle garanzie applicabili all'ulteriore utilizzo dei dati, come quelli inclusi nella legge sulla privacy (Codice degli Stati Uniti d'America, titolo 5, articolo 552a)[105].

3.1.5.2 Trasferimenti successivi al di fuori degli Stati Uniti

100. L'EDPB rileva inoltre che la Commissione europea ha fatto riferimento altresì ai trasferimenti successivi dalle autorità di contrasto statunitensi alle autorità di paesi terzi, ma anche in questo caso soltanto in riferimento al documento *Attorney General Guidelines for Domestic FBI Operations AGG-DOM*[106]. L'EDPB ritiene che tali informazioni e valutazioni siano fondamentali per consentire una valutazione completa del livello di protezione offerto dal quadro legislativo e dalle pratiche degli Stati Uniti in relazione alla divulgazione a livello internazionale e all'ulteriore utilizzo. Dato che la Commissione ha fornito soltanto un esempio, peraltro limitato, sulla questione dei trasferimenti successivi al di fuori degli Stati Uniti nel loro complesso, l'EDPB invita la Commissione a chiarire ulteriormente le norme e le garanzie applicabili ai trasferimenti successivi, all'utilizzo ulteriore e alla divulgazione di informazioni personali raccolte per finalità di contrasto negli Stati Uniti e successivamente trasferite a paesi terzi, anche attraverso accordi internazionali.

3.2 Accesso e utilizzo per finalità di sicurezza nazionale

101. Come osservazione generale, l'EDPB riconosce che agli Stati è concesso un ampio margine di discrezionalità in materia di sicurezza nazionale, riconosciuto anche dalla Corte CEDU. L'EDPB ricorda inoltre che, come sottolineato nelle sue raccomandazioni aggiornate sulle garanzie essenziali europee per le misure di sorveglianza[107], l'articolo 6, paragrafo 3, del trattato sull'Unione europea stabilisce che i diritti fondamentali sanciti dalla CEDU costituiscono principi generali del diritto dell'UE. Tuttavia, come ricorda la CGUE nella sua giurisprudenza, la CEDU non costituisce, finché l'UE non vi abbia aderito, un atto giuridico formalmente integrato nell'ordinamento giuridico dell'Unione[108]. Pertanto il livello di tutela dei diritti fondamentali richiesto dall'articolo 45 GDPR deve essere determinato sulla base delle disposizioni di tale regolamento, lette alla luce dei diritti fondamentali sanciti dalla Carta. Ciò detto, ai sensi dell'articolo 52, paragrafo 3, della Carta, i diritti in essa contenuti che corrispondono ai diritti garantiti dalla CEDU hanno lo stesso significato e la stessa portata di quelli previsti da quest'ultima convenzione. Di conseguenza, come ricordato dalla CGUE, occorre tener conto della giurisprudenza della Corte CEDU in materia di diritti previsti anche dalla Carta, in quanto livello minimo di protezione per interpretare i corrispondenti diritti della Carta[109]. Secondo l'ultimo comma dell'articolo 52, paragrafo 3, della Carta, tuttavia, "*[l]a presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa*".

102. Pertanto, nella valutazione che segue, l'EDPB ha tenuto conto della giurisprudenza della Corte CEDU, nella misura in cui la Carta, come interpretata dalla CGUE, non preveda un livello di protezione più elevato che prescriva requisiti diversi dalla giurisprudenza della Corte CEDU.

---

[104] Cfr. considerando 102 del progetto di decisione.
[105] Cfr. *Attorney General Guidelines for Domestic FBI Operations* (AGG-DOM), pag. 36, p. B (1)(g).
[106] Cfr. considerando 102 del progetto di decisione.
[107] Cfr. EDPB, Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza.
[108] Cfr. sentenza *Schrems II* della CGUE, punto 98.
[109] Cfr. sentenza *La Quadrature du Net* della CGUE, punto 124.

103. Nel contesto del quadro giuridico statunitense diversi strumenti giuridici prevedono la possibilità per le agenzie di intelligence degli Stati Uniti di raccogliere dati e di accedervi e trattarli ulteriormente.

104. Come ricordato dalla Commissione europea nel suo progetto di decisione, le agenzie di intelligence statunitensi possono chiedere l'accesso a dati personali che sono stati trasferiti a organizzazioni situate negli Stati Uniti per finalità di sicurezza nazionale soltanto nella misura consentita dalle normative in vigore, in particolare ai sensi della legge relativa alla vigilanza sull'intelligence esterna (FISA) o a disposizioni di legge che autorizzano l'accesso attraverso cosiddette National Security Letters (NSL)[110]. Ai sensi del decreto presidenziale 12333 le agenzie di intelligence statunitensi hanno altresì la possibilità di raccogliere dati personali al di fuori degli Stati Uniti, che possono includere dati personali in transito tra l'Unione e gli Stati Uniti[111].

105. Per quanto riguarda i regimi specifici di raccolta di dati, in particolare l'articolo 702 della FISA e il decreto presidenziale 12333, il decreto presidenziale 14086 prevede ora norme nuove destinate a migliorare le garanzie per le attività di intelligence dei segnali degli Stati Uniti. Tali norme generali si applicano orizzontalmente e devono essere ulteriormente attuate attraverso politiche e procedure delle agenzie che le traducano in indicazioni concrete per le operazioni quotidiane[112]. Il decreto presidenziale 14086 ha sostituito in gran parte la precedente direttiva presidenziale 28 ("PPD-28")[113].

106. Al fine di valutare il quadro giuridico che si applica alla raccolta, all'accesso e all'ulteriore trattamento dei dati per finalità di sicurezza nazionale, è quindi importante esaminare il quadro giuridico specifico che disciplina la raccolta dei dati all'interno e all'esterno degli Stati Uniti, ossia l'articolo 702 della FISA e il decreto presidenziale 12333, che, in quanto tali, non sono cambiati rispetto al precedente riesame dello scudo per la privacy, tenendo conto del fatto che il nuovo decreto presidenziale 14086 prevede garanzie da attuare anche nel contesto della raccolta dei dati sulla base di testi specifici quali l'articolo 702 della FISA e il decreto presidenziale 12333.

3.2.1 Garanzia A - Il trattamento dovrebbe essere conforme alla legge e basato su norme chiare, precise e accessibili

107. Per la sua valutazione dell'assetto generale della raccolta dei dati per finalità di sicurezza nazionale, l'EDPB desidera richiamare la prima delle quattro cosiddette "garanzie essenziali europee", secondo la quale il "trattamento dovrebbe basarsi su norme chiare, precise e accessibili" [114].

108. Conformemente alla giurisprudenza costante della CGUE, qualsiasi limitazione nell'esercizio del diritto alla protezione dei dati personali deve essere prevista dalla legge e implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato[115]. La CGUE ha ricordato altresì che tale "normativa dev'essere giuridicamente

[110] Cfr. considerando 115 del progetto di decisione.
[111] Cfr. considerando 117 del progetto di decisione.
[112] Cfr. considerando 120 del progetto di decisione.
[113] Questo decreto presidenziale revoca la PPD-28, fatta eccezione per gli articoli 3 e 6 di tale direttiva e per l'allegato classificato della stessa, che rimangono in vigore. Cfr. memorandum presidenziale sulla sicurezza nazionale del 7 ottobre 2022.
[114] Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020. Cfr. punti 175 e 180 della sentenza *Schrems II*, il parere 1/15 (accordo PNR UE-Canada) del 26 luglio 2017, punto 139 e la giurisprudenza citata.
[115] Cfr. sentenza *Schrems II* della CGUE, punti 174 e 175 e giurisprudenza ivi citata. Cfr. anche, per quanto concerne l'accesso da parte delle autorità pubbliche degli Stati membri, la sentenza *Privacy International*,

vincolante nell'ambito dell'ordinamento nazionale"[116]. A questo proposito, la giurisprudenza della Corte CEDU chiarisce che il termine "ordinamento" deve essere inteso nel suo senso sostanziale e non formale. Può includere le promulgazioni di atti di rango inferiore e misure di regolamentazione adottate da organismi di regolamentazione professionale in virtù di poteri normativi indipendenti delegati loro dal Parlamento e persino leggi non scritte. Per essere considerata parte dell'"ordinamento", una norma deve essere quanto meno adeguatamente accessibile e formulata con sufficiente precisione[117].

109. Il grado di precisione richiesto deve essere misurato in relazione all'entità della limitazione del diritto[118]. Inoltre per quanto concerne la "prevedibilità" della legge, la Corte CEDU ha ricordato nella sentenza *Zakharov* che nel contesto delle misure segrete di sorveglianza, quali l'intercettazione delle comunicazioni, "la prevedibilità non può significare che una persona debba essere in grado di prevedere quando le autorità potrebbero intercettare le sue comunicazioni in modo da poter adattare il suo comportamento di conseguenza". Tuttavia norme chiare e dettagliate sulle misure di sorveglianza segreta sono essenziali per prevenire i rischi di arbitrarietà quando un potere conferito all'esecutivo viene esercitato in segreto. "Il diritto nazionale deve essere sufficientemente chiaro da fornire ai cittadini un'indicazione adeguata in merito alle circostanze in cui e alle condizioni alle quali le autorità pubbliche possono ricorrere a tali misure"[119].

110. Inoltre la CGUE ha chiarito che la valutazione del diritto applicabile dei paesi terzi dovrebbe concentrarsi sulla possibilità riconosciuta alle persone di invocarlo e azionarlo dinnanzi a un organo giurisdizionale. In particolare i diritti concessi agli interessati dovrebbero essere azionabili e le persone devono disporre di diritti opponibili alle autorità pubbliche[120], cosa che non avveniva nel contesto della precedente PPD-28. Il decreto presidenziale 14086, che, a quanto risulta all'EDPB, nell'ordinamento giuridico statunitense ha lo stesso effetto giuridico della PPD-28 (ossia è vincolante per l'esecutivo), prevede ora diritti azionabili opponibili alle autorità pubbliche. Una valutazione dettagliata dei nuovi diritti azionabili degli interessati è fornita nella sezione dedicata ai mezzi di ricorso.

111. I considerando da 114 a 152 del progetto di decisione e l'allegato VII offrono una sintesi di alcuni aspetti della disciplina giuridica vigente, delle limitazioni applicabili alla raccolta, delle limitazioni applicabili alla conservazione e alla divulgazione, della garanzia della conformità e vigilanza, della trasparenza e dei mezzi di ricorso. L'ordinamento giuridico statunitense per le attività di intelligence è costituito da una serie di documenti diversi, tra cui relazioni, politiche e procedure delle singole agenzie. A tale riguardo la valutazione dell'EDPB si è concentrata su un numero limitato di questioni che ritiene fondamentali.

112. Secondo i considerando da 115 a 119 del progetto di decisione, l'accesso ai dati personali trasferiti da parte delle autorità di sicurezza nazionale statunitensi può avvenire soltanto ai sensi della FISA, di altre disposizioni di legge (Codice degli Stati Uniti d'America, titolo 12, articolo 3414, titolo 15, articoli da 1681u a 1681v e titolo 18, articolo 2709) oppure, in relazione a dati personali in transito, sulla base

C-623/17, ECLI:EU:C:2020:790 (in appresso: "sentenza Privacy International della CGUE"), punto 65; e la sentenza *La Quadrature du Net* della CGUE, punto 175.

[116] Sentenza *Privacy International* della CGUE, punto 68.

[117] Corte CEDU, *Sunday Times c. Regno Unito* (n. 1), 26 aprile 1979, CE:ECHR:1979:0426JUD000653874 (in appresso: "sentenza *Sunday Times c. Regno Unito* n. 1 della Corte CEDU"), punto 49.

[118] Sentenza *Sunday Times c. Regno Unito* n. 1 della Corte CEDU, punto 49.

[119] Corte CEDU, *Zakharov c. Russia*, 4 dicembre 2015 (in appresso: "sentenza *Zakharov* della Corte CEDU"), punto 229.

[120] Sentenza *Schrems II* della CGUE, punto 181.

del decreto presidenziale 12333. Dai considerando 116 e 118 del progetto di decisione si evince che la Commissione concentra la sua valutazione, in relazione all'accesso ai dati personali da parte delle autorità di sicurezza nazionale statunitensi, sugli articoli 105, 302, 402, 501 e 702 della FISA (attività di intelligence esterne che hanno come obiettivo cittadini non statunitensi situati al di fuori degli Stati Uniti) e sul decreto presidenziale 12333 (attività di intelligence estere su dati personali in transito), essendo i più rilevanti. Il parere dell'EDPB si limita pertanto alla valutazione di tali disposizioni effettuata dalla Commissione, tenendo conto delle limitazioni e delle garanzie stabilite nel decreto presidenziale 14086[121].

113. A questo proposito, occorre osservare che tutti gli strumenti giuridici citati nel progetto di decisione sono accessibili al grande pubblico (negli Stati Uniti e al di fuori degli stessi) e disponibili online. Inoltre i requisiti stabiliti nel decreto presidenziale sono vincolanti per l'intera comunità dell'intelligence[122] e si applicano in modo trasversale a tutte le attività aventi finalità di intelligence esterna.

114. Il concetto di "intelligence dei segnali" non è definito nel decreto presidenziale 14086. Quest'ultimo fa riferimento alle definizioni di cui al decreto presidenziale 12333 per stabilire l'ambito di applicazione dell'intelligence e del controspionaggio esterni, che sono definiti in modo ampio. A questo proposito, anche se è stato sostenuto che, dopo l'introduzione della FISA, il decreto presidenziale 12333 può essere utilizzato soltanto per la raccolta di dati al di fuori del territorio degli Stati Uniti, l'EDPB ricorda che il decreto presidenziale 12333 stesso, che rimane intatto, manca di dettagli sufficienti per quanto concerne il suo ambito di applicazione geografico, la misura in cui i dati possono essere raccolti, conservati o ulteriormente diffusi, la natura dei reati che possono dare origine alla sorveglianza o il tipo di informazioni che possono essere raccolte o utilizzate. In linea di principio, tutta la raccolta di dati per finalità di intelligence esterna rientranti nell'ambito di applicazione del decreto presidenziale 12333 può avvenire a discrezione del presidente degli Stati Uniti[123]. Tuttavia l'EDPB è dell'avviso che lo scopo principale del decreto presidenziale 14086 sia quello di prescrivere le limitazioni applicabili alla raccolta e al trattamento dei dati personali nel contesto dell'intelligence esterna, indipendentemente dal programma di sorveglianza utilizzato e dal luogo di ottenimento dei dati. L'EDPB ritiene pertanto che le garanzie supplementari previste dal decreto presidenziale 14086 si applichino anche nel contesto dei programmi di sorveglianza applicabili ai dati personali in transito ai sensi del decreto presidenziale 12333[124].

115. A questo proposito, il decreto presidenziale 14086 elenca 12 obiettivi legittimi che dovrebbero essere perseguiti quando si effettua la raccolta di intelligence dei segnali e 5 obiettivi per i quali la raccolta di intelligence dei segnali non può essere condotta[125], oltre a 6 obiettivi legittimi per l'uso dei dati raccolti in blocco[126]. Mentre alcuni di essi sono piuttosto dettagliati (ad esempio "salvataggio di ostaggi"), altri sono più generici (ad esempio "sicurezza globale"). Il decreto presidenziale 14086 stabilisce altresì un elenco di obiettivi proibiti che include in particolare la soppressione o la restrizione dei "legittimi

[121] Questo decreto presidenziale revoca la PPD-28, fatta eccezione per gli articoli 3 e 6 di tale direttiva e per l'allegato classificato della stessa, che rimangono in vigore. Cfr. memorandum presidenziale sulla sicurezza nazionale del 7 ottobre 2022.
[122] Cfr. considerando 120 del progetto di decisione.
[123] Ai sensi dell'articolo II della costituzione degli Stati Uniti, la competenza per garantire la sicurezza nazionale, compresa in particolare la raccolta di intelligence esterna, spetta all'autorità del presidente in veste di comandante in capo delle forze armate.
[124] Cfr. considerando 134 del progetto di decisione.
[125] Cfr. articolo 2, lettera b), punto ii), lettera A), sottopunti da 1 a 5, del decreto presidenziale 14086.
[126] Cfr. considerando 134 del progetto di decisione e articolo 2, lettera c), punto ii), del decreto presidenziale 14086.

interessi alla tutela della vita privata"[127]. Il decreto presidenziale 14086 prevede altresì la possibilità per il presidente degli Stati Uniti di aggiungere altri obiettivi all'elenco per i quali è consentita la raccolta, che potrebbero, su decisione del presidente, non essere resi pubblici qualora il presidente ritenga che ciò rappresenti un rischio per la sicurezza nazionale degli Stati Uniti[128]. Tali aggiornamenti possono essere autorizzati soltanto "alla luce di nuovi motivi imperativi di sicurezza nazionale".

116. Gli obiettivi non possono essere utilizzati dalle agenzie di intelligence dei segnali, ma devono essere ulteriormente concretizzati, per fini operativi, in priorità più concrete per le quali è possibile raccogliere intelligence dei segnali. Il decreto presidenziale 14086 descrive in dettaglio la procedura per la convalida delle priorità per le quali è possibile raccogliere intelligence dei segnali[129]. L'EDPB comprende che il processo di definizione delle priorità di intelligence convalidate si basa in linea di principio sul direttore della comunità dell'intelligence e riconosce che di norma dovrebbe coinvolgere la valutazione dell'addetto alla tutela della vita privata e alle libertà civili (CLPO) dell'Ufficio del direttore dell'intelligence nazionale (*ODNI, Office of the Director of National Intelligence*), con il quale il direttore può essere in disaccordo, nel qual caso quest'ultimo includerà la valutazione dell'addetto alla tutela della vita privata e i punti di vista del direttore quando presenterà il quadro delle priorità d'intelligence nazionale al presidente (NIPF, *National Intelligence Priorities Framework*)[130].

117. Tuttavia l'EDPB rileva altresì che, secondo la definizione di "*priorità di intelligence convalidata*", per "*la maggior parte delle attività di raccolta di intelligence dei segnali degli Stati Uniti*"[131] tali priorità corrispondono a una priorità convalidata ai sensi dell'articolo 2, lettera b), punto iii), del decreto presidenziale (descritto al punto precedente). Il processo di convalida può in alcuni casi differire da questo processo in "*circostanze ristrette*", nel qual caso il presidente o il capo di un servizio della comunità dell'intelligence può stabilire una priorità, "*nella misura in cui ciò sia fattibile*", secondo i criteri stabiliti dal medesimo articolo 2, lettera b), punto iii), lettera A), sottopunti da 1 a 3, che include il requisito di un'adeguata considerazione della tutela della vita privata e delle libertà civili di tutte le persone, ma senza il coinvolgimento del CLPO.

118. Il decreto presidenziale 14086 sottolinea inoltre che le attività di raccolta di intelligence dei segnali devono essere il più possibile mirate per portare avanti una priorità di intelligence convalidata, e che la comunità dell'intelligence deve considerare la disponibilità, la fattibilità e l'adeguatezza di altre fonti meno intrusive. Tale decreto definisce inoltre i requisiti generali di necessità e proporzionalità[132].

119. Inoltre, conformemente all'articolo 5, lettera h), il decreto presidenziale 14086 crea il diritto di presentare reclami qualificati al CLPO e di ottenere il riesame delle decisioni di quest'ultimo da parte del Tribunale del riesame in materia di protezione dei dati, conformemente al meccanismo di ricorso di cui all'articolo 3 di tale decreto.

120. Il testo della FISA sembra essere più chiaro e preciso rispetto a quello del decreto presidenziale 12333 in merito al tipo di operazioni di intelligence che possono essere autorizzate. La FISA e il decreto presidenziale 12333 devono ora essere applicati alla luce del decreto presidenziale 14086 e in particolare tenendo conto, tra l'altro, dei principi di necessità e proporzionalità.

[127] Cfr. articolo 2, lettera b), punto ii), lettera A), sottopunto 2, del decreto presidenziale 14086.
[128] Cfr. articolo 2, lettera b), punto i), lettera B), del decreto presidenziale 14086.
[129] Cfr. considerando 129 del progetto di decisione.
[130] Cfr. articolo 2, lettera b), punto iii), lettera B), del decreto presidenziale 14086.
[131] Cfr. articolo 4, lettera n), del decreto presidenziale 14086.
[132] Cfr. articolo 2, lettera c), punto i), lettere A) e B), del decreto presidenziale 14086.

121. I requisiti stabiliti nel decreto presidenziale 14086 devono essere ulteriormente attuati attraverso politiche e procedure dell'agenzia che li recepiscano traducendoli in indicazioni concrete per le operazioni quotidiane. A questo proposito, il decreto presidenziale 14086 concede alle agenzie di intelligence statunitensi un anno al massimo per aggiornare le politiche e le procedure esistenti (ossia entro il 7 ottobre 2023) per renderle conformi ai requisiti di tale decreto presidenziale. Tali politiche e procedure aggiornate devono essere sviluppate in consultazione con il procuratore generale, il CLPO e la PCLOB e devono essere rese pubbliche nella massima misura possibile[133].

122. L'EDPB auspicherebbe che non solo l'entrata in vigore ma anche l'adozione della decisione siano subordinate, tra l'altro, all'adozione di politiche e procedure aggiornate per l'attuazione del decreto presidenziale 14086 da parte di tutte le agenzie di intelligence statunitensi. L'EDPB raccomanda alla Commissione di valutare tali politiche e procedure aggiornate e di condividere tale valutazione con l'EDPB.

123. Infine, in relazione alla conservazione dei dati trasferiti una volta raccolti per finalità di sicurezza nazionale, l'EDPB rileva che il decreto presidenziale 14086 garantisce che le norme applicabili ai dati personali di cittadini statunitensi siano applicabili anche ai dati personali di cittadini non statunitensi[134]. Dal progetto di decisione sembra che tali norme siano previste dall'articolo 309 della legge autorizzativa dell'intelligence per l'esercizio finanziario 2015 (*Intelligence Authorization Act for Fiscal Year 2015*)[135], che stabilisce, in linea di principio, un periodo massimo di conservazione di 5 anni per qualsiasi comunicazione telefonica o elettronica non pubblica acquisita senza il consenso della persona. A questo proposito, l'EDPB raccomanda che la Commissione fornisca maggiore chiarezza sulla sua valutazione delle norme di conservazione applicabili ai dati personali di cittadini statunitensi nella decisione.

3.2.2 Garanzia B - Devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti

3.2.2.1 Garanzie orizzontali previste dal nuovo decreto presidenziale 14086 – Necessità e proporzionalità

124. Il nuovo decreto presidenziale 14086, che sostituisce in generale la PPD-28, mira a stabilire norme destinate a migliorare le garanzie per le attività di intelligence dei segnali degli Stati Uniti, che dovranno essere ulteriormente attuate dai servizi della comunità dell'intelligence nelle loro politiche e procedure interne.

125. Il decreto presidenziale 14086 introduce due nuovi requisiti nel diritto statunitense che rispecchiano quelli ricordati dalla CGUE nella sentenza *Schrems II*, ossia requisiti secondo cui le attività di intelligence dei segnali devono essere condotte soltanto nella misura necessaria a portare avanti una raccolta determinata da una priorità di intelligence convalidata e soltanto nella misura e con modalità proporzionate a detta priorità di intelligence convalidata[136].

126. L'EDPB ritiene che tali aspetti siano stati inclusi per rispecchiare i principi di necessità e proporzionalità previsti dal diritto dell'UE e dalla giurisprudenza della CGUE e relativa alla CEDU, che mirano a garantire che la raccolta e il trattamento dei dati siano limitati a quanto necessario e proporzionato.

[133] Cfr. articolo 2, lettera c), punto iv), lettere B) e C), del decreto presidenziale 14086.
[134] Considerando 150 del progetto di decisione.
[135] Cfr. nota 272 del progetto di decisione.
[136] Cfr. articolo 2, lettera a), punto ii), lettere A) e B), del decreto presidenziale 14086.

127. A questo proposito, l'EDPB ricorda il processo previsto per la convalida delle priorità d'intelligence e la possibile deroga (cfr. punti 116 e 117).

128. Inoltre l'EDPB rileva che tali principi di necessità e proporzionalità previsti dal decreto presidenziale dovranno essere resi operativi e attuati entro un anno nelle politiche e nelle procedure di ogni servizio della comunità dell'intelligence[137].

3.2.2.2 Garanzie specifiche per la raccolta di intelligence dei segnali

129. L'EDPB rileva inoltre che il decreto presidenziale 14086 prevede limitazioni relative agli obiettivi per i quali i dati personali possono o non possono essere raccolti, nel contesto della raccolta dell'intelligence dei segnali[138].

130. L'EDPB accoglie con favore il fatto che il decreto presidenziale preveda che si privilegi la raccolta mirata rispetto alla raccolta in blocco di dati[139]. Nel contesto della raccolta di intelligence dei segnali, il decreto presidenziale prevede un elenco di 12 obiettivi per i quali è possibile raccogliere dati, che devono essere ulteriormente motivati nel contesto di priorità di intelligence (cfr. punto 117), nonché un elenco di 5 obiettivi per i quali le attività di raccolta di intelligence dei segnali non possono essere condotte[140]. In linea di principio, tali disposizioni costituiscono una garanzia per assicurare la necessità della raccolta dei dati.

131. Tuttavia l'EDPB ricorda che il decreto presidenziale 14086 prevede anche la possibilità per il presidente degli Stati Uniti di aggiungere altri obiettivi all'elenco (cfr. punti 114 e 115)[141].

3.2.2.3 Garanzie specifiche per la raccolta in blocco di dati

132. Nella sentenza *Schrems I*, la CGUE ha sottolineato che "*la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario*"[142] e ha stabilito che "*[i]n particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta*".

133. Nella causa *Schrems II*[143], per quanto riguarda l'analisi della raccolta in blocco in relazione alla lettura correlata del decreto presidenziale 12333 e della PPD-28, in particolare dei punti da 183 a 185, la CGUE ha sottolineato, come ricordato in precedenza, che la possibilità di raccolta in blocco, "*che consente, nell'ambito dei programmi di sorveglianza basati sull'E.O. 12333, di accedere a dati in transito verso gli Stati Uniti senza che tale accesso sia oggetto di un qualsivoglia controllo giudiziario, non circoscrive, in ogni caso, in modo sufficientemente chiaro e preciso la portata di siffatta raccolta in blocco di dati personali*".

134. L'EDPB rileva quindi che la CGUE non ha escluso, in linea di principio, la raccolta in blocco, ma ha ritenuto, nella sua sentenza *Schrems II*, che affinché tale raccolta in blocco avvenga legittimamente, debbano essere previsti limiti sufficientemente chiari e precisi per delimitarne la portata.

---

[137] Cfr. articolo 2, lettera c), punto iv), lettera B), del decreto presidenziale 14086.
[138] Cfr. articolo 2, lettera b), punto i), lettera A), sottopunti da 1 a 12, del decreto presidenziale 14086.
[139] Cfr. articolo 2, lettera c), punto ii), lettera A), del decreto presidenziale 14086.
[140] Cfr. articolo 2, lettera b), punto ii), lettera A), sottopunti da 1 a 5, del decreto presidenziale 14086.
[141] Cfr. articolo 2, lettera b), punto i), lettera B), del decreto presidenziale 14086.
[142] Sentenza *Schrems II* della CGUE, punto 92.
[143] Cfr. sentenza *Schrems II* della CGUE.

135. L'EDPB riconosce inoltre che, pur sostituendo la PPD-28, il decreto presidenziale 14086 prevede garanzie e limiti nuovi per la raccolta e l'utilizzo di dati raccolti al di fuori degli Stati Uniti, in quanto non si applicano le limitazioni della FISA o di altre leggi statunitensi più specifiche.

136. Per quanto concerne la raccolta in blocco di dati, l'EDPB prende atto del fatto che il decreto presidenziale 14086 prevede che tale raccolta continui a essere consentita. In effetti l'EDPB sottolinea che la definizione di raccolta in blocco di dati rimane la stessa della precedente PPD-28, dato che con raccolta dati 'in blocco' nell'ambito dell'intelligence dei segnali si intende la raccolta autorizzata di grandi quantità di dati di intelligence dei segnali che, in base a considerazioni tecniche o operative, è effettuata senza il filtro di discriminanti (ad esempio senza l'uso di dispositivi specifici o selettori)[144].

137. Dopo la sentenza *Schrems II*, la Corte non ha specificato con precisione le garanzie necessarie per l'attuazione della raccolta in blocco di dati. Tuttavia l'EDPB ricorda che la Corte CEDU ha emesso importanti decisioni riguardanti la raccolta in blocco di dati e le relative garanzie in questo contesto.

138. L'EDPB ricorda che la raccolta in blocco, consentendo la raccolta di grandi quantità di dati senza discriminazioni, presenta rischi più elevati per le persone[145] rispetto alla raccolta mirata e richiede quindi l'adozione di garanzie supplementari.

139. L'EDPB rileva inoltre che la CGUE ha sviluppato un'ulteriore giurisprudenza relativa alla conservazione dei dati sul traffico e sull'ubicazione e al successivo accesso a tali dati conservati dagli operatori di telecomunicazioni, anche a fini di sicurezza nazionale, che, sebbene non possa essere considerata direttamente applicabile in questo contesto, in una certa misura potrebbe essere rilevante nell'ambito della presente valutazione della raccolta in blocco nel contesto del decreto presidenziale 12333.

1) <u>Limitazione della finalità</u>

140. Il decreto presidenziale prevede che la raccolta in blocco avvenga soltanto dopo aver stabilito che le informazioni necessarie per portare avanti una priorità di intelligence convalidata non possono essere ragionevolmente ottenute mediante una raccolta mirata[146] e che il servizio della comunità dell'intelligence applicherà metodi ragionevoli e misure tecniche al fine di limitare i dati raccolti esclusivamente a quelli necessari per portare avanti una priorità di intelligence convalidata, riducendo nel contempo al minimo la raccolta di informazioni non pertinenti[147]. Oltre a queste garanzie, l'EDPB riconosce anche che l'uso dei dati raccolti in blocco deve essere utilizzato per perseguire uno o più dei sei obiettivi elencati[148]. L'EDPB sottolinea inoltre che, sebbene tali obiettivi siano più dettagliati rispetto a quelli previsti dalla precedente PPD-28, in genere sostituita dal decreto presidenziale 14086, la portata di tali possibilità di raccolta rimane potenzialmente ampia, ossia comprende grandi volumi di dati.

141. Anche in questo caso l'EDPB ricorda che il decreto presidenziale 14086 prevede altresì la possibilità per il presidente degli Stati Uniti di aggiungere altri obiettivi all'elenco (cfr. punto 115)[149].

---

[144] Cfr. articolo 4, lettera b), del decreto presidenziale 14086.
[145] Cfr. ad esempio la sentenza della Corte CEDU (Grande Camera), *Big Brother Watch e altri c. Regno Unito*, 25 maggio 2021 (di seguito "sentenza *Big Brother Watch* della Corte CEDU"), punto 363, nella quale la Corte afferma di non essere persuasa del fatto che l'acquisizione di dati relativi alle comunicazioni attraverso l'intercettazione massiva sia necessariamente meno intrusiva dell'acquisizione di contenuti.
[146] Articolo 2, lettera c), punto ii), lettera A), del decreto presidenziale 14086.
[147] Articolo 2, lettera c), punto ii), lettera A), del decreto presidenziale 14086.
[148] Articolo 2, lettera c), punto ii), lettera B), del decreto presidenziale 14086.
[149] Cfr. articolo 2, lettera c), punto ii), lettera C), del decreto presidenziale 14086.

2) Autorizzazione indipendente preventiva

142. L'EDPB sottolinea che la Corte CEDU dedica un'importanza significativa all'autorizzazione indipendente preventiva nel contesto della raccolta in blocco di dati per finalità di sicurezza nazionale. Infatti la Corte CEDU ha stabilito in particolare che al fine di ridurre al minimo il rischio di abuso della facoltà di intercettazione massiva, la Corte ritiene che il processo debba essere soggetto a "garanzie da punto a punto (*end-to-end*)", il che significa che: a livello nazionale, in ogni fase del processo, dovrebbe essere effettuata una valutazione della necessità e della proporzionalità delle misure adottate; che l'intercettazione massiva dovrebbe essere soggetta a un'autorizzazione indipendente in via preliminare, nel momento in cui vengono definiti l'oggetto e l'ambito di applicazione dell'operazione; e che tale operazione dovrebbe essere soggetta a un controllo e a un riesame indipendente a posteriori. Secondo la Corte, si tratta di garanzie fondamentali che costituiranno l'elemento portante di qualsiasi regime di intercettazione massiva conforme all'articolo 8[150].

143. L'EDPB rileva altresì il punto della sentenza della Grande Camera (di cui in nota), nel quale la Corte di Strasburgo sottolinea che concorda con la Camera quando afferma che l'autorizzazione giudiziaria, pur essendo una garanzia importante contro l'arbitrio, non costituisce un requisito necessario (cfr. punti da 318 a 320 della sentenza della Camera). Tuttavia l'intercettazione massiva dovrebbe essere autorizzata da un organismo indipendente; ossia un organo indipendente dall'esecutivo[151].

144. In questo contesto l'EDPB rileva che la legge non prevede un'autorizzazione indipendente preventiva per la raccolta in blocco di dati e che ciò non è previsto nemmeno dal decreto presidenziale 12333 (cfr. sezione successiva sul decreto presidenziale 12333).

3) Norme in materia di conservazione

145. L'EDPB ricorda che un'altra importante serie di garanzie è costituita dalle norme concernenti la durata della raccolta e della conservazione dei dati. A questo proposito, la Corte CEDU ha sottolineato che il diritto nazionale dovrebbe stabilire un limite alla durata dell'intercettazione, la procedura da seguire per l'esame, l'uso e la conservazione dei dati ottenuti, le precauzioni da adottare quando si comunicano i dati ad altre parti e le circostanze nelle quali i dati intercettati possono o devono essere cancellati o distrutti[152], in quanto tali garanzie sono parimenti rilevanti ai fini dell'intercettazione massiva[153].

146. A questo proposito l'EDPB ritiene che il decreto presidenziale preveda norme in materia di conservazione dei dati per i dati personali raccolti tramite l'intelligence dei segnali, anche in blocco[154]. L'EDPB osserva che, conformemente all'articolo 2, lettera c), punto iii), lettera A), del decreto presidenziale 14086, ogni servizio della comunità dell'intelligence che gestisce informazioni personali raccolte attraverso l'intelligence dei segnali deve stabilire e applicare politiche e procedure destinate a ridurre al minimo la diffusione e la conservazione delle informazioni personali raccolte attraverso l'intelligence dei segnali. Tuttavia tali norme non prevedono un periodo di conservazione specifico, ma fanno piuttosto riferimento in generale alle stesse norme applicabili per la conservazione dei dati relativi a cittadini statunitensi e alle situazioni nelle quali non è stata presa una decisione definitiva in materia di conservazione. L'EDPB esprime quindi preoccupazione circa il fatto che tali periodi di conservazione, come per la raccolta mirata (cfr. punto 122), non sono chiaramente definiti nel decreto

[150] Cfr. sentenza *Big Brother Watch* della Corte CEDU, punto 350.
[151] Cfr. sentenza *Big Brother Watch* della Corte CEDU, punto 351.
[152] Cfr. sentenza *Big Brother Watch* della Corte CEDU, punto 348.
[153] Cfr. sentenza *Big Brother Watch* della Corte CEDU, punto 348.
[154] Cfr. articolo 2, lettera c), punto iii), lettera A), sottopunto 2), lettere da a) a c), del decreto presidenziale 14086.

presidenziale in questione per quanto riguarda i dati raccolti in blocco. Invita la Commissione a condividere la sua valutazione sulla necessità e sulla proporzionalità dei periodi di conservazione applicabili ai cittadini statunitensi e le informazioni disponibili sui periodi di conservazione nella pratica, laddove non sia stata presa una decisione definitiva in materia di conservazione ai sensi del diritto statunitense, poiché nella sua versione attuale, il progetto di decisione si limita a richiamare tale norma generale in un unico breve paragrafo[155] e in una nota[156] che non consente di stabilire se tali periodi di conservazione siano necessari e proporzionati. Dato che, come sottolineato dalla Corte CEDU, si tratta di una garanzia fondamentale per consentire agli interessati di esercitare i propri diritti in un contesto in cui innanzitutto viene adottata una misura particolarmente invasiva per raccogliere i loro dati, l'EDPB invita la Commissione europea a fornire ulteriori chiarimenti in merito ai diversi periodi di conservazione nella pratica.

4) Garanzie relative alla "diffusione"

147. L'EDPB ricorda inoltre che per garantire l'efficacia della necessità e della proporzionalità e il principio di limitazione della finalità, la Corte CEDU ha riconosciuto altresì l'importanza delle norme previste dalla legge per quanto riguarda l'ulteriore diffusione dei dati raccolti, anche nel contesto della raccolta in blocco[157].

148. L'articolo 2, lettera c), punto iii), lettera A), sottopunto 1), lettera c), del decreto presidenziale 14086 stabilisce che le informazioni su cittadini non statunitensi raccolte attraverso attività di intelligence possono essere diffuse soltanto se una persona autorizzata che ha ricevuto un'adeguata formazione nutre la ragionevole convinzione che le informazioni personali saranno adeguatamente protette e che il destinatario ha la necessità di conoscere le informazioni in questione.

149. Tenendo conto di ciò, l'EDPB ritiene che le disposizioni relative alla diffusione ai sensi del decreto presidenziale 14086 non prevedano un esplicito divieto di diffusione per finalità diverse da quelle di sicurezza nazionale quando si tratta di diffusione ad autorità competenti degli Stati Uniti[158]. L'EDPB invita la Commissione a chiarire ulteriormente le norme e le garanzie applicabili in questo caso.

150. L'EDPB teme quindi che i dati acquisiti dalle autorità competenti della comunità dell'intelligence possano essere diffusi alle autorità competenti degli Stati Uniti per finalità di lotta alla criminalità, compresi reati gravi, nel contesto di indagini penali, fornendo così alle autorità di contrasto, senza ulteriori restrizioni specifiche, la possibilità di ottenere dati che sarebbe stato loro vietato raccogliere direttamente e invita quindi la Commissione a valutare ulteriormente questo aspetto.

151. Nel contesto specifico dei trasferimenti successivi (diffusione a destinatari esterni al governo degli Stati Uniti, compreso un governo straniero o un'organizzazione internazionale[159]), l'EDPB ricorda che ritiene che la protezione dei dati debba essere mantenuta anche nel contesto dei trasferimenti successivi, anche nel settore della sicurezza nazionale[160].

---

[155] Cfr. punto 150 del progetto di decisione.
[156] Cfr. nota 271 del progetto di decisione.
[157] Cfr. sentenza *Big Brother Watch* della Corte CEDU, punto 348.
[158] Cfr. articolo 2, lettera c), punto iii), lettera A), sottopunto 1), del decreto presidenziale 14086.
[159] Cfr. in particolare articolo 2, lettera c), punto iii), lettera A), sottopunto 1), lettera d), del decreto presidenziale 14086.
[160] Cfr. ad esempio, EDPB, Parere 14/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nel Regno Unito, adottato il 13 aprile 2021, sezioni 4.3.2.1 e 4.3.2.2.

152. A questo proposito, il decreto presidenziale prevede alcune garanzie, in particolare l'obbligo, prima della diffusione, di tenere in debita considerazione la finalità della diffusione (pur senza richiedere espressamente che la finalità della diffusione sia anch'essa la protezione della sicurezza nazionale) la natura e la portata delle informazioni personali diffuse e il potenziale impatto dannoso sulla persona o sulle persone interessate.

153. Pur riconoscendo che alcune di tali garanzie, in particolare la considerazione del "*potenziale impatto dannoso*"[161] sugli interessati in questione, rispecchiano alcuni requisiti di cui alla CEDU, l'EDPB sottolinea che la Corte di Strasburgo richiede inoltre un obbligo giuridicamente vincolante che impone di analizzare e determinare se il destinatario straniero dell'intelligence offra un livello minimo accettabile di garanzie[162], che l'EDPB non ritrova espressamente nelle disposizioni del decreto presidenziale relative alla diffusione a destinatari stranieri. L'EDPB invita pertanto la Commissione a valutare ulteriormente questo aspetto.

154. L'EDPB rileva altresì che la Commissione europea non ha preso in considerazione, nel contesto della sua valutazione di adeguatezza, l'esistenza di accordi internazionali conclusi con paesi terzi od organizzazioni internazionali che possano prevedere disposizioni specifiche per il trasferimento internazionale di dati personali da parte dei servizi di intelligence a paesi terzi. L'EDPB ritiene che la conclusione di accordi bilaterali o multilaterali con paesi terzi per finalità di cooperazione in materia di intelligence possa incidere sul quadro giuridico della protezione dei dati, come valutato.

155. L'EDPB invita pertanto la Commissione europea a chiarire se tali accordi esistono, a quali condizioni possono essere conclusi e a valutare se le disposizioni degli accordi internazionali possono incidere sul livello di protezione garantito ai dati personali trasferiti dallo Spazio economico europeo (SEE) mediante il quadro legislativo e le prassi in materia di trasferimenti successivi per finalità di sicurezza nazionale.

5) <u>Raccolta temporanea in blocco a sostegno della fase tecnica iniziale di una raccolta mirata</u>

156. L'EDPB ricorda che, nel contesto dell'ultimo riesame congiunto dello scudo per la privacy, le discussioni si sono concentrate principalmente sull'interpretazione e sull'applicazione del motivo ulteriore (situazione/scenario) per la raccolta in blocco previsto dalla prima frase della nota 5 dell'articolo 2 della PPD-28, che stabilisce che le limitazioni contenute in tale articolo non si applicano ai dati di intelligence dei segnali acquisiti temporaneamente per facilitare la raccolta mirata. Le autorità statunitensi hanno spiegato all'epoca il significato di "*dati di intelligence dei segnali acquisiti temporaneamente per facilitare una raccolta mirata*". Da tali discussioni l'EDPB ha compreso che tale nota significa che i dati possono essere raccolti in blocco, e indipendentemente dalle sei finalità previste, qualora siano raccolti temporaneamente, al fine di stabilire un identificatore per un obiettivo definito. Si tratterebbe quindi di un motivo in più per raccogliere dati in blocco, e in questo caso si applicherebbero ancora soltanto i principi generali dell'articolo 1 della PPD-28. Come ricordato in precedenza, nella sentenza *Schrems II*, la CGUE ha ritenuto che il decreto presidenziale 12333 in combinato disposto con la PPD-28 per quanto riguarda la raccolta in blocco di dati non "*circoscrive[sse] [...] in modo sufficientemente chiaro e preciso la portata di siffatta raccolta in blocco di dati personali*"[163].

[161] Cfr. articolo 2, lettera c), punto iii), lettera A), sottopunto 1), lettera d), del decreto presidenziale 14086.
[162] Cfr. Corte CEDU (Grande Camera), Centrum För Rättvisa c. Svezia, 25 maggio 2021, punto 326.
[163] Sentenza *Schrems II* della CGUE, punto 183.

157. L'EDPB osserva che una deroga che consente questo tipo di raccolta in blocco è ancora prevista nel decreto presidenziale 14086[164]; tuttavia, l'EDPB accoglie con favore il fatto che tale deroga sia stata ridotta rispetto alla PPD-28 e che siano previste ulteriori garanzie nel contesto del decreto presidenziale 14086.

158. L'EDPB è consapevole del fatto che il nuovo decreto presidenziale 14086 prevede garanzie che rimangono applicabili nel contesto di questo tipo di raccolta tecnica temporanea in blocco, in particolare i principi generali di necessità e proporzionalità in relazione alla priorità di intelligence convalidata quando i dati sono acquisiti senza discriminanti prima che avvenga la raccolta mirata (articolo 2, lettere a) e b) e articolo 2, lettera c), punto i), del decreto presidenziale 14086). L'EDPB ritiene inoltre che tale raccolta in blocco a sostegno di una successiva raccolta mirata di intelligence dei segnali sia soggetta anche alle garanzie supplementari previste dal punto 2, lettera c), iii) in poi[165].

159. Tuttavia l'EDPB ricorda altresì (cfr. punto 117) che la definizione di "*priorità di intelligence convalidata*" prevede una procedura di deroga che non coinvolge il CLPO dell'ODNI.

160. Tuttavia l'EDPB rileva comunque che le garanzie di cui alla disposizione relativa alla raccolta in blocco non si applicano alla raccolta in blocco temporanea utilizzata per sostenere la fase tecnica iniziale dell'attività di raccolta mirata di intelligence dei segnali, come indicato all'articolo 2, lettera c), punto ii), lettera D), del decreto presidenziale 14086, il che significa in particolare che in tale contesto i dati raccolti in blocco possono essere utilizzati per finalità diverse da quelle elencate all'articolo 2, lettera c), punto ii). L'EDPB accoglierebbe con favore l'inclusione nel progetto di decisione di chiarimenti circa le finalità per le quali possono essere utilizzati i dati raccolti in blocco in tale contesto, nonché l'applicazione delle limitazioni di cui all'articolo 2, lettera c), punto i), per la raccolta di intelligence dei segnali in generale (ossia soltanto per gli obiettivi legittimi ivi elencati) nel contesto della raccolta temporanea in blocco.

161. Per concludere l'EDPB sottolinea altresì che la deroga in questione per la raccolta temporanea in blocco in vista della raccolta mirata e le restanti garanzie da applicare rimangono poco chiare, in particolare per quanto concerne quali garanzie del decreto presidenziale 14086 si applicherebbero a quale fase (raccolta in blocco, ulteriore raccolta mirata) e invita la Commissione a valutare ulteriormente tali aspetti e a valutarli anche nella pratica nel contesto dei futuri riesami congiunti.

162. Inoltre anche se l'EDPB si rammarica ulteriormente del fatto che, sebbene il concetto di "temporanea" sia stato leggermente più dettagliato nel decreto presidenziale rispetto alla PPD-28, a suo avviso sembra ancora significare che finché l'obiettivo non è stato identificato, la raccolta in blocco può continuare. A questo proposito l'EDPB ricorda la necessità di disporre di norme chiare e precise e sottolinea anche in questo caso la garanzia fondamentale che tali norme costituiscono per gli interessati.

163. In conclusione, per quanto concerne le garanzie applicabili alla raccolta di dati in blocco, l'EDPB continua a esprimere preoccupazione circa il fatto che, nonostante le garanzie supplementari previste dal decreto presidenziale 14086, la possibilità di raccogliere dati in blocco, ossia in assenza di discriminanti, è ancora prevista, senza garanzie fondamentali quali l'autorizzazione preventiva alla raccolta di tali dati (anche nella situazione derogatoria della raccolta tecnica temporanea di dati in blocco) tenendo conto anche della necessità di ulteriori chiarimenti e delle preoccupazioni espresse in merito a una rigorosa limitazione delle finalità per l'accesso successivo ai dati, a norme chiare e

[164] Cfr. articolo 2, lettera c), punto ii), lettera D), del decreto presidenziale 14086 e nota 226 del progetto di decisione.

[165] Per ulteriori dettagli su queste disposizioni cfr. sezioni precedenti.

rigorose in materia di conservazione dei dati e a garanzie più rigorose per quanto riguarda la diffusione dei dati raccolti in blocco, anche nel contesto di trasferimenti successivi.

164. In generale l'EDPB sottolinea che la suddetta sentenza della Corte CEDU dimostra ancora una volta l'importanza di un controllo completo da parte di autorità di controllo indipendenti. L'EDPB sottolinea che un controllo indipendente in tutte le fasi del processo di accesso da parte delle amministrazioni pubbliche per finalità di sicurezza nazionale costituisce una garanzia importante contro misure di sorveglianza arbitrarie e quindi ai fini della valutazione di un livello adeguato di protezione dei dati. La garanzia di indipendenza delle autorità di controllo ai sensi dell'articolo 8, paragrafo 3, della Carta mira a garantire un controllo efficace e affidabile del rispetto delle norme in materia di protezione delle persone in relazione al trattamento dei dati personali. Ciò vale in particolare nei casi in cui, a causa della natura della sorveglianza segreta, alla persona in questione viene impedito di chiedere un riesame o di partecipare direttamente a qualsiasi procedimento di riesame prima o durante l'esecuzione della misura di sorveglianza.

165. L'EDPB ricorda di essere del parere che la valutazione dell'adeguatezza dipenda da tutte le circostanze del caso, in particolare dall'efficacia della vigilanza ex post e dei mezzi di ricorso giuridici previsti dal quadro giuridico.

3.2.2.4 Quadro giuridico che organizza la raccolta specifica per finalità di sicurezza nazionale da parte dei servizi della comunità dell'intelligence all'interno e all'esterno del territorio degli Stati Uniti

166. Nella sentenza *Schrems II*, la CGUE ha sottolineato, in relazione all'articolo 702 della FISA, che tale testo "*non fa emergere in alcun modo l'esistenza di limitazioni all'autorizzazione che esso comporta per l'attuazione dei programmi di sorveglianza ai fini dell'intelligence esterna, né l'esistenza di garanzie per i cittadini stranieri potenzialmente oggetto di tali programmi*"[166]. Ciò ha portato la Corte ha ritenere che "*[i]n tali circostanze [...] tale articolo non è idoneo a garantire un livello di tutela sostanzialmente equivalente a quello garantito dalla Carta [...], secondo cui, per soddisfare il principio di proporzionalità, una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura e impongano requisiti minimi*"[167].

167. In relazione al decreto presidenziale 12333, a seguito dell'analisi delle condizioni in cui la raccolta in blocco potrebbe avvenire in base a tale decreto, in combinato disposto con la PPD-28, la CGUE ha osservato che "*tale decreto [non] conferisce diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici*"[168] e ha altresì concluso che "*nell'ambito dei programmi di sorveglianza basati sull'E.O. 12333, [la possibilità] di accedere a dati in transito verso gli Stati Uniti senza che tale accesso sia oggetto di un qualsivoglia controllo giudiziario, non circoscrive, in ogni caso, in modo sufficientemente chiaro e preciso la portata di siffatta raccolta in blocco di dati personali*"[169].

168. Per quanto riguarda questi specifici regimi di raccolta dei dati, il decreto presidenziale 14086 prevede ora norme nuove.

[166] Cfr. sentenza *Schrems II* della CGUE, punto 180.
[167] Cfr. sentenza *Schrems II* della CGUE, punto 180.
[168] Cfr. sentenza *Schrems II* della CGUE, punto 182.
[169] Cfr. sentenza *Schrems II* della CGUE, punto 183.

3.2.2.4.1 Raccolta di dati per finalità di sicurezza nazionale a norma dell'articolo 702

169. L'EDPB ricorda che, nella sua ultima relazione, la PCLOB aveva accolto con favore le conclusioni sull'articolo 702 della FISA[170], secondo le quali nella pratica anche i cittadini stranieri beneficiano delle restrizioni applicabili all'accesso ai dati e alla loro conservazione che sono previste dalle procedure attuate dai diversi enti per rendere mirata e/o ridurre al minimo la raccolta dati, dato che considerati i costi e le difficoltà associati all'individuazione e alla cancellazione di informazioni concernenti cittadini statunitensi o residenti negli USA all'interno di un ampio corpus di dati, solitamente l'intero insieme di dati è trattato nel rispetto dei massimi standard di tutela applicabili ai cittadini statunitensi.

170. Secondo tali conclusioni, il programma non opera raccogliendo comunicazioni in blocco. Le relazioni *Statistical Transparency Report* pubblicate dall'ODNI nel 2014 e nel 2021 confermano tale constatazione. Sempre secondo la relazione della PCLOB, per rendere mirata l'attività di sorveglianza si utilizzano selettori attivati, quali gli indirizzi di posta elettronica o i numeri di telefono.

171. Tuttavia l'EDPB ricorda altresì che, allo stesso tempo, nel contesto dell'articolo 702, è stato chiarito durante l'ultimo riesame dello scudo per la privacy che il concetto di "persona" da identificare come obiettivo potrebbe riferirsi a più persone che utilizzano il medesimo identificatore, a condizione che tutte queste persone siano cittadini stranieri (non statunitensi) e soddisfino i criteri applicabili per essere individuati come obiettivi. L'EDPB ricorda inoltre che durante il terzo riesame congiunto annuale dello scudo per la privacy del 2019 sono stati richiesti ulteriori chiarimenti nel contesto del programma UPSTREAM al fine di escludere che si verifichi un accesso massiccio e indiscriminato a dati personali di persone non statunitensi[171].

172. Inoltre l'EDPB ricorda che il fatto che la raccolta sia giustificata ai sensi dell'articolo 702 della FISA dal perseguimento di una delle finalità rilevanti dell'acquisizione, che dev'essere quello di ottenere informazioni di intelligence esterna, continua a lasciare un certo margine di incertezza quanto alla limitazione della finalità e alla necessità della raccolta stessa. L'EDPB osserva tuttavia che, ai sensi dell'articolo 2, lettera a), lettere A) e B), del decreto presidenziale 14086, le attività di intelligence dei segnali saranno condotte soltanto dopo aver stabilito che le attività sono necessarie per portare avanti una priorità convalidata e soltanto nella misura e secondo modalità proporzionate a tale priorità e che saranno il più possibile mirate per portare avanti la priorità convalidata, tenendo in debita considerazione fattori pertinenti quali l'intrusività della raccolta, la sensibilità dei dati e un impatto non sproporzionato sulla tutela della vita privata e sulle libertà civili. L'EDPB si aspetta ancora ulteriori chiarimenti circa le modalità con cui ciò verrà concretamente attuato e reso operativo, anche nel contesto dell'applicazione dell'articolo 702 della FISA.

173. A questo proposito, in assenza di un accesso diretto a tali informazioni, l'EDPB ha chiesto una valutazione indipendente sulla necessità e sulla proporzionalità della definizione di "obiettivi" e del concetto di "intelligence esterna" ai sensi dell'articolo 702 della FISA (anche nel contesto del programma UPSTREAM) in seguito al suo rinnovo. L'EDPB ritiene pertinente la sua precedente richiesta di un'ulteriore valutazione indipendente del processo di applicazione dei selettori in casi specifici ("attivazione di selettori") e di ulteriori chiarimenti nel contesto del programma UPSTREAM. Di conseguenza, tenendo conto del nuovo decreto presidenziale 14086, l'EDPB chiede ulteriori informazioni per valutare e monitorare anche in che modo e in che misura i principi di necessità e proporzionalità recentemente introdotti saranno applicati nella pratica in questo contesto e si aspetta che ciò sarà valutato anche nel contesto dei futuri riesami congiunti.

[170] Cfr. relazione della PCLOB sul programma di sorveglianza gestito a norma dell'articolo 702 della FISA, pag. 100.
[171] Cfr. relazione sul terzo riesame congiunto, pag. 17, punto 83.

174. L'EDPB accoglie con favore il fatto che l'Autorità per la tutela della vita privata e delle libertà civili (PCLOB), un'agenzia di vigilanza indipendente e pienamente funzionante, abbia deciso di condurre un progetto di controllo per esaminare il programma di sorveglianza che il ramo esecutivo gestisce ai sensi dell'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna (FISA), in previsione della data di scadenza per tale articolo 702, prevista per il mese di dicembre del 2023, e dell'imminente esame pubblico e congressuale della sua ri-autorizzazione[172]. L'EDPB accoglie altresì con favore il fatto che tale riesame riguardi settori principali di indagine selezionati, tra cui, a titolo esemplificativo non esaustivo, le interrogazioni di cittadini statunitensi sulle informazioni raccolte a norma dell'articolo 702 e la raccolta "a monte" condotta a norma dell'articolo 702[173] e comprenda altresì l'esame del valore e dell'efficacia passati e previsti del programma, nonché dell'adeguatezza delle garanzie esistenti in materia di tutela della vita privata e libertà civili[174]. L'EDPB sottolinea quindi che necessiterebbe dell'accesso alle conclusioni della PCLOB incluse in tale relazione sull'articolo 702 al fine di valutare in modo adeguato e completo le garanzie in materia di tutela della vita privata fornite e applicate nel contesto del programma di sorveglianza in questione.

175. Tenendo conto del nuovo decreto presidenziale 14086, l'EDPB chiede altresì ulteriori informazioni per valutare e monitorare anche in che modo e in che misura i principi di necessità e proporzionalità recentemente introdotti, nonché altre garanzie previste in tale atto, saranno applicati nella pratica in questo contesto.

3.2.2.4.2 Raccolta di dati per finalità di sicurezza nazionale a norma del decreto presidenziale 12333

176. Come riconosciuto dalla CGUE nella sentenza *Schrems II*, l'analisi delle leggi del paese terzo per il quale si prende in considerazione l'adeguatezza non deve limitarsi alle leggi e alle pratiche che consentono la sorveglianza all'interno dei confini fisici di tale paese, ma dovrebbe includere altresì un'analisi dei fondamenti giuridici dell'ordinamento di tale paese terzo che gli consentono di condurre attività di sorveglianza al di fuori del suo territorio per quanto riguarda i dati dell'UE. Le limitazioni necessarie all'accesso ai dati da parte di pubbliche amministrazioni dovrebbero estendersi ai dati personali "in transito" verso il paese per il quale è riconosciuta l'adeguatezza.

177. L'EDPB accoglie con favore la relazione pubblica redatta dalla PCLOB sul decreto presidenziale 12333 e pubblicata nell'aprile del 2021, ma osserva che tale relazione rimane generica in quanto la maggior parte delle conclusioni sono classificate.

178. In tale contesto, ancora una volta, data l'incertezza e la mancanza di chiarezza sulle modalità di applicazione del decreto presidenziale 12333 e considerata l'importanza di chiarire come quest'ultimo sarà applicato alla luce del nuovo decreto presidenziale 14086, l'EDPB sottolinea l'importanza delle attese relazioni della PCLOB in merito a questo testo[175]. Tuttavia è consapevole del fatto che la maggior parte del contenuto di tali relazioni rimarrà probabilmente classificato e che quindi non saranno disponibili né per il pubblico né per l'EDPB ulteriori informazioni sul funzionamento concreto del decreto presidenziale 12333 e sulla sua necessità e proporzionalità.

---

[172] Cfr. *NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)*.

[173] Cfr. sopra.

[174] Cfr. sopra.

[175] La relazione generale sul decreto presidenziale 12333 è rimasta per lo più classificata: soltanto una breve versione pubblica è stata resa pubblica, così come la relazione e le raccomandazioni sulle attività antiterrorismo della CIA condotte ai sensi del decreto presidenziale 12333, anch'essi solo parzialmente declassificati.

179. L'EDPB accoglierebbe quindi con particolare favore la declassificazione della relazione della PCLOB sull'applicazione del decreto presidenziale 14086 e la sua piena messa a disposizione una volta completata, anche per quanto concerne le parti che valutano come le garanzie del decreto presidenziale 14086 saranno applicate alla raccolta di dati a norma del decreto presidenziale 12333. L'EDPB invita inoltre la Commissione a prestare particolare attenzione a questo aspetto nel contesto dei futuri riesami congiunti.

180. In generale, per quanto concerne i diversi strumenti giuridici che prevedono la possibilità per le agenzie di intelligence statunitensi, nel quadro giuridico degli Stati Uniti, di raccogliere e di accedere e trattare ulteriormente dati, l'EDPB gradirebbe chiarimenti in merito alla loro interazione con il nuovo decreto presidenziale 14086 e si aspetta assicurazioni circa il fatto che le preoccupazioni espresse nei precedenti pareri dell'EDPB al riguardo siano risolti mediante l'adozione di tali nuove garanzie.

181. L'EDPB invita inoltre la Commissione a prestare particolare attenzione a tali aspetti nel contesto dei futuri riesami congiunti.

3.2.2.4.3 Relazione della PCLOB

182. L'EDPB accoglie con favore il fatto che il decreto presidenziale 14086 preveda anche l'obbligo per la PCLOB di redigere una relazione sull'attuazione di tale decreto. L'EDPB sottolinea che tale relazione dovrebbe includere una valutazione della specifica possibilità in questione offerta dal decreto presidenziale di raccogliere dati, per le finalità elencate per la raccolta mirata, così come in blocco, anche per motivi tecnici, al fine di comprendere meglio i termini chiave del decreto presidenziale 14086 e il modo in cui vengono praticamente compresi e applicati nei diversi programmi di sorveglianza. Tale relazione sarebbe altresì necessaria per valutare come il decreto presidenziale sarà attuato nelle procedure e nelle politiche interne dei servizi della comunità dell'intelligence.

3.2.3 Garanzia C - Vigilanza

3.2.3.1 Introduzione

183. Le attività di intelligence degli Stati Uniti sono soggette a un processo di vigilanza a più livelli. La struttura di vigilanza negli Stati Uniti può essere suddivisa in vigilanza interna ed esterna. Tutti i servizi della comunità dell'intelligence hanno funzionari addetti alla vigilanza e alla conformità che effettuano una vigilanza periodica delle attività di intelligence dei segnali, nonché addetti alla tutela della vita privata e alle libertà civili e ispettori generali. Esistono inoltre organi di vigilanza esterni, quali l'Autorità per la tutela della vita privata e delle libertà civili (PCLOB) e l'*Intelligence Oversight Board* (IOB, Autorità di vigilanza sull'intelligence).

184. L'EDPB ricorda che un'ingerenza avviene al momento della raccolta dei dati, ma anche al momento dell'accesso ai dati da parte di un'autorità pubblica in vista di un trattamento ulteriore. La Corte CEDU ha specificato più volte che qualsiasi ingerenza nel diritto al rispetto della vita privata e alla protezione dei dati deve essere soggetta a un sistema di vigilanza efficace, indipendente e imparziale che deve essere previsto da un giudice o da un altro organo indipendente[176] (ad esempio un'autorità amministrativa o un organo parlamentare).

[176] Corte CEDU, *Klass e altri c. Germania*, 6 settembre 1978 (in appresso: "sentenza *Klass* della Corte CEDU"), punti 17 e 51.

185. Sebbene la Corte CEDU abbia espresso la propria preferenza per la responsabilità di un giudice ai fini del mantenimento della vigilanza, non ha escluso che un altro organismo possa essere responsabile, a condizione che tale autorità sia sufficientemente indipendente dall'esecutivo[177] e dalle autorità che effettuano la vigilanza e sia dotata di poteri e competenze sufficienti per esercitare un controllo efficace e continuo[178].

186. La Corte CEDU ha aggiunto che le modalità di nomina e lo status giuridico dei membri dell'organismo di controllo[179] devono essere presi in considerazione nel valutare l'indipendenza.

187. La Corte CEDU ha affermato altresì che occorre esaminare se le attività dell'organismo di controllo sono aperte al pubblico. Ad esempio tale obiettivo potrebbe essere conseguito se l'organismo di controllo riferisce annualmente al governo, ossia le relazioni pubbliche sono presentate al Parlamento e sono discusse da quest'ultimo[180].

188. Il controllo indipendente sull'attuazione delle misure di sorveglianza è stato preso in considerazione anche dalla CGUE nella sentenza *Schrems II*, nella quale si afferma che "*[...] il controllo esercitato dalla Corte FISA mira quindi a verificare se tali programmi di sorveglianza corrispondano all'obiettivo di ottenere informazioni in materia di intelligence esterna, ma non verte sulla questione 'se la persona costituisca un obiettivo adatto per acquisire informazioni di intelligence esterna'*"[181].

3.2.3.2 Vigilanza interna

3.2.3.2.1 Ispettori generali

189. L'EDPB riconosce che agli ispettori generali è affidata un'ampia serie di autorizzazioni, necessarie per monitorare le attività di intelligence. In particolare gli ispettori generali hanno accesso a tutte le informazioni necessarie per valutare la conformità generale del lavoro delle agenzie rispetto alla legislazione, anche, ma non solo, rispetto alle leggi relative alla tutela della vita privata e alla protezione dei dati, e possono emettere citazioni e ricevere dichiarazioni giurate da qualsiasi persona in relazione alle indagini degli ispettori generali.

190. Sulla base di quanto sopra, l'EDPB ritiene che gli ispettori generali abbiano in genere ampi poteri investigativi. Tuttavia non dispongono di alcun potere correttivo vincolante e si limitano a formulare raccomandazioni non vincolanti[182].

191. L'EDPB riconosce che, in linea di principio, agli ispettori generali non può essere impedito o vietato di avviare, svolgere o portare a termine una verifica o un'indagine o di emettere una citazione nel corso di una verifica o di un'indagine[183]. In tale contesto l'EDPB osserva tuttavia che gli ispettori generali sono soggetti all'autorità, alla direzione e al controllo del rispettivo capo dipartimento, che può vietare loro l'accesso a informazioni, l'avvio di un'indagine e, tra l'altro, l'emissione di una citazione nei casi in cui il capo dipartimento stabilisca che tale divieto è necessario al fine di preservare gli interessi nazionali.

---

[177] Sentenza *Zakharov* della Corte CEDU, punto 258; Corte CEDU, Iordachi e altri c. Moldova, 10 febbraio 2009, punti 40 e 51; Corte CEDU, Dumitru Popescu c. Romania, 26 aprile 2007, punti da 70 a 73.
[178] Sentenza *Klass* della Corte CEDU, punto 56.
[179] Sentenza *Zakharov* della Corte CEDU, punto 278.
[180] Sentenza *Zakharov* della Corte CEDU, punto 283; Corte CEDU, L. c. Norvegia, 9 giugno 1990; Corte CEDU, Kennedy c. Regno Unito, 18 maggio 2010, punto 166.
[181] Sentenza *Schrems II* della CGUE, punto 179.
[182] Considerando 105 del progetto di decisione.
[183] Legge sugli ispettori generali (*Inspector General Act*) del 1978, articolo 3, lettera a).

Tuttavia il capo del dipartimento deve informare le commissioni competenti del Congresso degli Stati Uniti dell'esercizio di tale autorità[184].

192. L'EDPB osserva che la nomina degli ispettori generali può essere revocata soltanto dal presidente degli Stati Uniti, che deve comunicare al Congresso le motivazioni di tale rimozione.

193. L'EDPB rileva che non sono state apportate modifiche significative al meccanismo di vigilanza interna dopo i pareri del Gruppo di lavoro e successivamente dell'EDPB. Di conseguenza l'EDPB conclude, in linea con il parere 01/2016 del Gruppo di lavoro[185], che in generale sono in atto sufficienti meccanismi di vigilanza interna.

3.2.3.3 Vigilanza esterna

194. L'EDPB osserva che, oltre agli organismi citati di seguito, vari altri organismi del governo degli Stati Uniti supervisionano le attività delle agenzie di intelligence statunitensi, quali l'Autorità di vigilanza sull'intelligence (IOB) o le commissioni del Congresso. Queste ultime possono svolgere le proprie indagini e pubblicare le proprie relazioni.

3.2.3.3.1 Autorità per la tutela della vita privata e delle libertà civili (PCLOB)

195. L'EDPB riconosce il ruolo di controllo globale della PCLOB per quanto concerne il nuovo meccanismo di ricorso e l'attuazione del decreto presidenziale 14086.

196. Innanzitutto le sue nuove funzioni prevedono la consultazione con il procuratore generale in merito alla nomina dei giudici del DPRC e degli avvocati speciali. In secondo luogo, la PCLOB riesaminerà annualmente il processo di ricorso, ossia l'elaborazione dei reclami qualificati da parte del meccanismo di ricorso. Rientra in tale contesto la verifica dell'eventualità che il CLPO e il DPRC abbiano trattato i reclami qualificati in modo tempestivo, stiano ottenendo o meno pieno accesso alle informazioni necessarie e operino in conformità con il decreto presidenziale 14086, nonché la verifica della conformità della comunità dell'intelligence rispetto alle decisioni prese dal CLPO e dal DPRC.

197. Inoltre la PCLOB deve essere consultata quando le agenzie di intelligence aggiornano le loro politiche e procedure interne ai fini dell'attuazione del decreto presidenziale 14086. La PCLOB effettuerà inoltre un riesame delle politiche e delle procedure aggiornate e ne valuterà la conformità rispetto al decreto presidenziale 14086[186]. Sebbene i risultati della PCLOB non siano vincolanti in senso stretto, il capo di ciascun servizio della comunità dell'intelligence è tenuto a considerare attentamente e ad attuare o a trattare altrimenti tutte le raccomandazioni contenute in tale riesame, in conformità con il diritto applicabile[187]. L'EDPB invita la Commissione a prestare particolare attenzione all'eventualità e alle modalità con cui le raccomandazioni della PCLOB sono state attuate a livello di agenzia nei riesami futuri, in caso di adozione del progetto di decisione.

198. L'EDPB ricorda che la PCLOB, essendo indipendente, è "incoraggiata" a verificare, ma non è tenuta a farlo, se le garanzie previste dal decreto presidenziale 14086 sono state prese in considerazione in

[184] Cfr. ad esempio la legge sugli ispettori generali del 1978, articolo 8 (per il Dipartimento della Difesa); articolo 8E (per il Dipartimento di Giustizia), articolo 8G, lettera d), punto 2), lettere A) e B) (per l'Agenzia nazionale per la sicurezza (*National Security Agency* (NSA); Codice degli Stati Uniti d'America, titolo 50, articolo 403q, lettera b) (per la CIA); legge autorizzativa dell'intelligence per l'esercizio finanziario 2010, articolo 405, lettera f) (per la comunità dell'intelligence).
[185] Parere 01/2016 del Gruppo di lavoro.
[186] Articolo 2, lettera c), punto iv) e articolo 2, lettera c), punto v), del decreto presidenziale 14086.
[187] Articolo 2, lettera c), punto v), lettera B), del decreto presidenziale 14086.

modo adeguato e se la comunità dell'intelligence ha rispettato pienamente i requisiti del processo di ricorso. Tuttavia l'EDPB è a conoscenza del fatto che la PCLOB ha dichiarato, nella sua spiegazione aggiuntiva all'EDPB e in pubblico[188], che assumerà il ruolo previsto dal decreto presidenziale 14086.

199. Inoltre l'EDPB accoglie con favore il fatto che i risultati delle relazioni della PCLOB siano destinati ad essere resi pubblici. Tenendo conto del fatto che i vari organismi nel contesto del meccanismo di ricorso e quelli della comunità dell'intelligence devono in linea di principio attuare le raccomandazioni contenute nelle relazioni della PCLOB o affrontarle in altro modo, l'EDPB riconosce che tali raccomandazioni svolgono un ruolo importante nel garantire la tutela della vita privata.

200. L'EDPB osserva che l'accesso della PCLOB alle informazioni è limitato se il presidente degli Stati Uniti autorizza la conduzione di "azioni segrete"[189] da parte di dipartimenti, agenzie o soggetti del governo degli Stati Uniti[190].

201. In linea con i suoi precedenti pareri, l'EDPB ritiene che la PCLOB sia un organo indipendente, le cui raccomandazioni sono state un importante contributo alle riforme negli Stati Uniti e le cui relazioni sono state una fonte particolarmente utile per comprendere il funzionamento dei vari programmi di sorveglianza, un aspetto essenziale della struttura di vigilanza.

202. Tuttavia nel suo terzo riesame congiunto annuale del precedente scudo UE-USA per la privacy, l'EDPB si è rammaricato del fatto che la PCLOB abbia fornito all'EDPB soltanto le stesse informazioni fornite al pubblico in generale. Inoltre è motivo di rammarico il fatto che la PCLOB non abbia pubblicato ulteriori relazioni sulla PPD-28 per dare seguito alla sua prima relazione, al fine di fornire ulteriori elementi sulle modalità di applicazione delle garanzie di cui alla PPD-28, nonché una relazione generale aggiornata sull'articolo 702 della FISA.

203. Di conseguenza l'EDPB accoglie con favore l'annuncio della PCLOB indirizzato all'EDPB, secondo cui nel prossimo futuro si può prevedere la pubblicazione di una relazione di seguito sull'articolo 702 della FISA. Inoltre l'EDPB è soddisfatto del fatto che la PCLOB abbia informato del suo impegno a consentire la pubblicità delle sue relazioni relative al decreto presidenziale 14086. Tuttavia l'EDPB ricorda che la pubblicazione di relazioni non classificati è disciplinata dal diritto statunitense e deve essere coordinata con le agenzie della comunità di intelligence e non può essere decisa dalla PCLOB di propria iniziativa.

204. Pertanto, in caso di adozione del progetto di decisione, l'EDPB ricorda che nei futuri riesami del quadro UE-USA di protezione dei dati, gli esperti con nulla osta di sicurezza dell'EDPB dovrebbero essere in grado di esaminare documenti aggiuntivi e discutere ulteriori elementi classificati, se necessario, al fine di garantire che le informazioni contenute nelle relazioni possano essere adeguatamente valutate, tenendo conto al contempo dei pertinenti interessi di sicurezza nazionale e delle protezioni applicabili in materia di tutela della vita privata.

---

[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

[189] Ai sensi del Codice degli Stati Uniti d'America, titolo 50, articolo 3093, lettera e), punto 1, per "azione segreta" si intende una o più attività del governo degli Stati Uniti destinate a influenzare le condizioni politiche, economiche o militari all'estero, nel contesto delle quali è inteso che il ruolo del governo degli Stati Uniti non deve essere evidente o riconosciuto pubblicamente, ma non comprende: 1) le attività la cui finalità principale è l'acquisizione di informazioni di intelligence, lo svolgimento di attività tradizionali di controspionaggio [...].

[190] Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee, lettera g), punto 5; Codice degli Stati Uniti, titolo 50, articolo 3093, lettera a).

205. L'EDPB accoglie con favore l'indipendenza e la vigilanza della PCLOB nei confronti della comunità nazionale dell'intelligence, che deve conformarsi alle raccomandazioni della PCLOB o affrontarle in altro modo, come sarà indicato nella relazione della PCLOB al Congresso degli Stati Uniti.

206. Tenendo conto dei requisiti sanciti dalla Corte CEDU in materia di controllo pubblico[191], secondo cui le relazioni di un organismo di controllo devono essere presentate e discusse dal Parlamento, l'EDPB ritiene sufficiente che la PCLOB presenti le sue relazioni non meno di una volta a semestre al presidente degli Stati Uniti e in particolare alle commissioni congressuali del Senato e della Camera dei Rappresentanti[192], che sono gli organi parlamentari degli Stati Uniti.

3.2.3.3.2 Corte di vigilanza sull'intelligence esterna (Corte FISA)

207. La Corte di vigilanza sull'intelligence esterna (Corte FISA, *Foreign Intelligence Surveillance Court*) è competente per il controllo della raccolta di dati personali a norma dell'articolo 702 della FISA[193] e le decisioni emesse dalla Corte FISA possono essere impugnate adendo la Corte di controllo della vigilanza sull'intelligence esterna (FISCR, *Foreign Intelligence Surveillance Court of Review*).

208. La Corte FISA vigila sul processo di certificazione per la raccolta di informazioni di intelligence esterna a norma dell'articolo 702 della FISA e autorizza la sorveglianza elettronica, le perquisizioni fisiche e altre misure investigative per finalità di intelligence esterna[194]. La Corte FISA autorizza altresì le procedure di individuazione, minimizzazione e interrogazione dei certificati, che sono legalmente vincolanti per le agenzie di intelligence statunitensi[195]. Se la Corte FISA ritiene che i requisiti non siano stati soddisfatti, può negare la certificazione in toto o in parte e richiedere la modifica delle procedure.

209. Qualora vengano individuate violazioni delle procedure di individuazione, la Corte FISA può ordinare all'agenzia di intelligence pertinente di adottare misure correttive[196]. Tali misure correttive potranno spaziare da misure individuali a misure strutturali, ad esempio dalla cessazione dell'acquisizione di dati e dalla cancellazione di dati ottenuti illecitamente fino alla modifica delle pratiche di raccolta, anche per quanto riguarda gli orientamenti e la formazione del personale.

210. L'EDPB riconosce che il decreto presidenziale 14086 prevede che il CLPO e il DPRC segnalino le violazioni all'assistente del procuratore generale per la sicurezza nazionale, che le segnalerà alla Corte FISA[197].

211. Come ha osservato la CGUE nella sentenza *Schrems II*, la Corte FISA non autorizza misure di sorveglianza individuali; piuttosto, autorizza programmi di sorveglianza[198]. Di conseguenza l'EDPB ribadisce la propria preoccupazione secondo la quale la Corte FISA non fornirebbe un controllo giudiziario efficace sull'individuazione di persone non statunitensi, preoccupazione che non sembra essere stata risolta dal nuovo decreto presidenziale 14086.

---

[191] Sentenza *Zakharov* della Corte CEDU, punto 283, Corte CEDU, L. c. Norvegia, 9 giugno 1990; Corte CEDU, Kennedy c. Regno Unito, 18 maggio 2010, punto 166.
[192] Codice degli Stati Uniti d'America, titolo 42, articolo 2000ee, lettera e).
[193] Codice degli Stati Uniti d'America, titolo 50, articolo 1881, lettera a).
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.
[195] Codice degli Stati Uniti d'America, titolo 50, articolo 1881a, lettera i).
[196] Codice degli Stati Uniti d'America, titolo 50, articolo 1803, lettera h).
[197] Articolo 3, lettera c), punto i), lettera D), del decreto presidenziale 14086. Articolo 3, lettera d), punto i), lettera F), del decreto presidenziale 14086.
[198] Sentenza *Schrems II* della CGUE, punto 179.

212. Per quanto concerne l'autorizzazione indipendente preventiva[199] della sorveglianza a norma dell'articolo 702 della FISA, l'EDPB si rammarica del fatto che, a quanto risulta dal progetto di decisione[200] e dalle spiegazioni fornite dal governo dagli Stati Uniti, la Corte FISA non sembra essere vincolata dalle garanzie supplementari di cui al decreto presidenziale 14086, quando certifica i programmi che autorizzano l'individuazione di persone non statunitensi. Secondo l'EDPB, le garanzie supplementari contenute in tale decreto dovrebbero comunque essere prese in considerazione in questo contesto. L'EDPB ricorda che le relazioni della PCLOB sarebbero particolarmente utili per valutare le modalità di attuazione delle garanzie di cui al decreto presidenziale 14086 e le modalità di loro applicazione quando i dati sono raccolti a norma dell'articolo 702 della FISA.

3.2.4 Garanzia D - Necessità di mettere a disposizione della persona mezzi di ricorso efficaci

213. L'EDPB ricorda che diritti effettivi ed azionabili della persona sono di importanza fondamentale per concludere che sussiste un livello adeguato di protezione dei dati in un paese terzo. Gli interessati devono disporre di un rimedio efficace per soddisfare i loro diritti quando ritengono che questi non siano o non siano stati rispettati. Nelle sentenze *Schrems I e II* la CGUE ha spiegato che "una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta"[201].

214. Il sistema statunitense relativo ai ricorsi giurisdizionali contiene un limite importante che rende molto difficile intentare un'azione legale contro le misure di sorveglianza attuate dal governo statunitense adendo gli organi giurisdizionali ordinari. La costituzione degli Stati Uniti impone a una persona di dimostrare la propria legittimazione ad agire, ossia di dimostrare di aver subito un pregiudizio concreto, specifico ed effettivo o imminente[202]. Nei casi di sorveglianza, tale requisito sembra essere annullato dalla mancanza di notifica alle persone sottoposte a sorveglianza anche dopo la cessazione di tali misure.

215. In tale contesto l'EDPB accoglie con favore il fatto che il decreto presidenziale 14086 stabilisca un meccanismo di ricorso specifico per gestire e risolvere i reclami di persone non statunitensi, riguardanti le attività di intelligence dei segnali attuate dagli Stati Uniti. Nel contesto di tale nuovo meccanismo, l'obbligo della legittimazione ad agire non è applicabile: conformemente all'articolo 4, lettera k), punto ii), del decreto presidenziale 14086, il richiedente non deve dimostrare che i suoi dati sono stati effettivamente oggetto di attività di intelligence dei segnali attuate dagli Stati Uniti. Gli interessati possono quindi invocare le garanzie previste dal decreto presidenziale 14086, comprese quelle previste da altre leggi e disposizioni pertinenti di cui all'articolo 4, lettera d), punto iii), del decreto presidenziale 14086[203]. A questo proposito, il nuovo meccanismo aggiunge un mezzo di ricorso che altrimenti non esisterebbe.

216. Il nuovo meccanismo è composto da due livelli: nel contesto del primo livello, le persone possono promuovere un reclamo presso l'addetto alla tutela della vita privata e alle libertà civili (CLPO)

[199] Per quanto riguarda la raccolta di dati in blocco a norma del decreto presidenziale 12333, per la quale la Corte FISA non è competente, l'EDPB è preoccupato per il fatto che non esiste un processo di autorizzazione preventiva per la raccolta di dati in blocco (cfr. anche garanzia B).
[200] Considerando 165 del progetto di decisione.
[201] Sentenza *Schrems I* della CGUE, punto 95; sentenza *Schrems II* della CGUE, punto 187.
[202] Clapper c. Amnesty International USA, 568 U.S. 398 (2013) II. pag. 10.
[203] L'articolo 5, lettera h), del decreto presidenziale 14086, crea esplicitamente il diritto per gli interessati di presentare reclami conformemente al meccanismo di ricorso.

dell'Ufficio del direttore dell'intelligence nazionale. Nell'ambito del secondo livello, le persone hanno la possibilità di impugnare la decisione del CLPO adendo un organo di nuova istituzione, il cosiddetto Tribunale del riesame in materia di protezione dei dati (DPRC). Le sezioni che seguono si concentrano principalmente sul secondo livello del meccanismo di ricorso. L'EDPB ritiene che il CLPO, in qualità di funzionario governativo facente funzione, non sia dotato di un sufficiente grado di indipendenza dall'esecutivo e non possa quindi, di per sé, soddisfare adeguatamente le prescrizioni derivanti dall'articolo 47 della Carta. Tale valutazione è stata confermata dalla Commissione in diverse occasioni.

3.2.4.1 L'istituzione del DPRC sulla base di un decreto presidenziale può essere di per sé sufficiente?

217. Il DPRC non è un organo giurisdizionale ordinario istituito dal Congresso ai sensi dell'articolo III della costituzione degli Stati Uniti, ma si basa su un decreto presidenziale emesso dal presidente degli Stati Uniti. Sebbene l'EDPB sia consapevole della considerazione sottostante, ossia evitare l'obbligo di dimostrare la legittimazione ad agire (cfr. anche il punto 215), e in generale accolga con favore tale considerazione, ciò solleva una questione fondamentale: tale meccanismo di ricorso può soddisfare (realmente) le prescrizioni di cui all'articolo 47 della Carta? Ai sensi di tale disposizione, ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice precostituito per legge.

218. Sebbene la formulazione italiana dell'articolo 47 della Carta faccia riferimento a un "giudice", altre versioni linguistiche privilegiano il termine "organo giurisdizionale"[204]. Nella sentenza *Schrems II* la CGUE ha ribadito che "i singoli devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati"[205]. Tuttavia, nello stesso contesto di valutazione dell'adeguatezza del livello di protezione dei dati, la CGUE ritiene che una tutela giurisdizionale effettiva contro tali interferenze possa essere assicurata non soltanto da un organo giurisdizionale, ma anche da un organismo che offra garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta[206]. Analogamente, la CEDU stabilisce che "ogni persona i cui diritti e le cui libertà siano stati violati, [ha] diritto a un ricorso effettivo davanti a un'istanza nazionale"[207] che, come ha costantemente affermato la Corte CEDU, non deve necessariamente essere un'autorità giudiziaria[208]. Piuttosto i poteri e le garanzie procedurali di cui dispone un'autorità, in particolare il fatto che sia indipendente dall'esecutivo e che garantisca l'equità del procedimento, sono pertinenti ai fini della valutazione dell'efficacia del ricorso dinanzi a tale autorità[209]. Sembra che entrambi gli organi giurisdizionali non basino la loro valutazione su criteri puramente formalistici, ma considerino decisive le garanzie sostanziali.

219. Nella sentenza *Schrems II* la CGUE ha prestato particolare attenzione all'efficacia del ricorso nel settore dell'accesso ai dati personali da parte dei soggetti preposti alla sicurezza nazionale. L'EDPB prende atto del fatto che la CGUE, nel procedere in tal senso, non ha discusso l'aspetto del "precostituito per legge" di cui all'articolo 47 della Carta, sebbene anche il meccanismo del mediatore dello scudo per la privacy non fosse basato sul diritto statunitense. Anziché affrontare questa questione, la CGUE ha valutato aspetti diversi per la sua verifica dell'adeguatezza, quali la mancanza di poteri correttivi. Pertanto, la

[204] Ad esempio "Gericht" nella versione in lingua tedesca.
[205] Sentenza *Schrems II* della CGUE, punto 194.
[206] Cfr. sentenza *Schrems II* della CGUE, punto 197.
[207] Articolo 13 CEDU.
[208] Sentenza *Klass* della Corte CEDU, punto 67; sentenza *Big Brother Watch* della Corte CEDU, punto 359.
[209] Sentenza *Klass* della Corte CEDU, punto 67; sentenza *Big Brother Watch* della Corte CEDU, punto 359.

sentenza *Schrems II* non fornisce alcuna indicazione sulla valutazione di "precostituito per legge" ai sensi dell'articolo 47 della Carta. Tuttavia esistono altre sentenze nelle quali la CGUE si è espressa in merito. Rispecchiando la giurisprudenza consolidata della Corte CEDU a questo proposito, la CGUE ha ricordato nelle cause C-487/19 e C-132/20 che la ragione dell'introduzione dell'espressione "precostituito per legge" è garantire che l'organizzazione del sistema giudiziario non sia lasciata alla discrezione dell'esecutivo e fare in modo che tale materia sia disciplinata da una legge adottata dal potere legislativo in modo conforme alle norme che disciplinano l'esercizio della sua competenza[210]. Come si evince da questa affermazione, il diritto a un giudice precostituito per legge è strettamente legato alla garanzia di indipendenza.

220. In questo contesto l'EDPB conclude che, nel contesto della valutazione dell'adeguatezza del livello di protezione, il meccanismo di ricorso specifico creato dal decreto presidenziale 14086 rispetto al ricorso agli organi giurisdizionali di cui all'articolo III non è di per sé insufficiente. L'analisi del livello di protezione in questo senso dipende dal fatto che le garanzie previste dal decreto presidenziale 14086 e integrate dal regolamento sul procuratore generale garantiscano in maniera sufficiente l'indipendenza del DPRC rispetto agli altri poteri.

221. La Commissione dovrebbe monitorare costantemente se le norme stabilite nel decreto presidenziale 14086 e le sue disposizioni aggiuntive, in particolare quelle destinate a promuovere l'indipendenza del DPRC, siano pienamente attuate e funzionino efficacemente nella pratica. Inoltre qualsiasi modifica del quadro dovrebbe essere esaminata attentamente per verificarne l'impatto sulla valutazione della Commissione in base al progetto di decisione. A questo proposito l'EDPB rileva che le modifiche apportate al decreto presidenziale 14086 e al regolamento sul procuratore generale possono determinare l'adozione di atti di esecuzione immediatamente applicabili che sospendono, abrogano o modificano la decisione di adeguatezza[211].

3.2.4.2 Indipendenza sufficiente rispetto all'esecutivo

222. Nella sentenza *Schrems II*, la CGUE ha sottolineato che l'indipendenza del giudice o dell'organo deve essere assicurata, in particolare nei confronti del potere esecutivo, con tutte le garanzie necessarie, anche per quanto riguarda le condizioni di revoca o annullamento della nomina. Più specificamente, la CGUE ha criticato il fatto che il mediatore fosse nominato dal segretario di Stato e riferisse direttamente a quest'ultimo. Il mediatore è stato ritenuto parte integrante del Dipartimento di Stato degli Stati Uniti. La CGUE ha inoltre riscontrato l'assenza di garanzie specifiche per la revoca o l'annullamento della nomina del mediatore, una circostanza che mina quindi l'indipendenza di quest'ultimo dall'esecutivo.

223. L'EDPB riconosce che le disposizioni di cui al decreto presidenziale 14086 e il regolamento supplementare sul procuratore generale non impongono al DPRC l'obbligo di riferire al procuratore generale, come avverrebbe in una relazione tra superiore e subordinato. Il DPRC non è nemmeno soggetto al controllo quotidiano del procuratore generale[212]. Tali garanzie rappresentano un miglioramento significativo rispetto allo scudo per la privacy. Tuttavia il DPRC è istituito all'interno del ramo esecutivo, ossia il Dipartimento della Giustizia. Per questo motivo, in particolare, l'attuazione e l'effettivo funzionamento delle garanzie nella pratica saranno fondamentali al fine di determinare se il DPRC, pur non essendo parte integrante del Dipartimento della Giustizia, in quanto soggetto

[210] Cfr. CGUE, sentenza della Corte di giustizia del 6 ottobre 2021, *W.Ż.*, C-487/19, ECLI:EU:C:2021:798, punto 129 e sentenza della Corte di giustizia del 29 marzo 2022, *Getin Noble Bank S.A.*, C-132/20, ECLI:EU:C:2022:235, punto 121.
[211] Considerando 212 del progetto di decisione.
[212] Articolo 201.7, lettera d), del regolamento sul procuratore generale.

comunque collocato all'interno dell'esecutivo, possa essere considerato sufficientemente indipendente nella pratica. L'EDPB invita la Commissione a monitorare attentamente se tali garanzie si rispecchino pienamente nella pratica. Inoltre l'EDPB suggerisce di chiarire l'espressione "controllo quotidiano" affinché i "giudici" del DPRC non siano soggetti a nessun tipo di controllo. La Commissione ha confermato che il controllo quotidiano va inteso in questo senso.

224. Oltre alle garanzie di cui sopra, il DPF UE-USA prevede alcune garanzie per quanto riguarda la nomina e la revoca della nomina dei "giudici" del DPRC. Pur essendo nominati dal procuratore generale, la loro nomina si basa sui criteri utilizzati per valutare i candidati ai posti di giudice federale e prevede la consultazione della PCLOB. La revoca della nomina a "giudice" prima della scadenza del mandato corrispondente o in relazione a un procedimento in corso è possibile soltanto in circostanze ben definite, che, a quanto risulta all'EDPB, sono modellate sulle disposizioni applicabili ai giudici federali[213]. L'applicazione di tali norme rappresenta un ulteriore progresso verso il rafforzamento della posizione indipendente del DPRC per il quale, ancora una volta, l'attuazione pratica sarà fondamentale. Tuttavia dal progetto di decisione non è chiaro se e in che modo il rispetto di tali prescrizioni sarà osservato negli Stati Uniti. Sulla base di ulteriori spiegazioni fornite dalla Commissione e dal governo degli Stati Uniti, l'EDPB ha appreso che la PCLOB può affrontare le disposizioni di cui sopra nel suo riesame annuale del processo di ricorso e che la competenza per il monitoraggio e la garanzia del rispetto di tutte le prescrizioni legali dell'ispettore generale in seno al Dipartimento della Giustizia comprende le prescrizioni di cui al decreto presidenziale 14086 e ai regolamenti che istituiscono il DPRC. L'EDPB invita la Commissione a chiarire questo aspetto nel progetto di decisione. Detto questo, la Commissione dovrebbe tenere conto di queste garanzie quando monitora la pratica effettiva del trattamento dei dati personali come valutato nel progetto di decisione.

225. Il progetto di decisione non affronta la questione se, e in caso affermativo, a quali condizioni il presidente degli Stati Uniti abbia l'autorità per annullare o revocare la nomina a "giudice" dal DPRC. L'EDPB ritiene che tale autorità non esista, come è stato spiegato dalla Commissione europea e confermato dai rappresentanti del governo degli Stati Uniti. L'EDPB suggerisce di chiarire questo aspetto nella decisione di adeguatezza.

226. I "giudici" del DPRC sono nominati per mandati quadriennali rinnovabili e, al momento della nomina iniziale, non devono essere stati impiegati nel ramo esecutivo nei due anni antecedenti[214]. Durante il periodo di nomina a "giudice" del DPRC, essi non dovranno avere altri incarichi o impieghi ufficiali in seno al governo degli Stati Uniti[215]. Tuttavia, a differenza dei giudici federali statunitensi, possono partecipare ad attività extragiudiziarie, tra cui attività commerciali, attività finanziarie, attività di raccolta fondi senza scopo di lucro, attività fiduciarie e all'esercizio della professione forense, a condizione che tali attività non interferiscano con l'esercizio imparziale delle loro funzioni o con l'efficacia o l'indipendenza del DPRC[216]. L'indipendenza della magistratura non deriva soltanto dalla libertà da istruzioni, ma anche dall'indipendenza personale. In questo contesto, sono rilevanti fattori quali la durata del mandato, la possibilità di essere riconfermati e il potenziale di conflitto di interessi. La durata di quattro anni prevista dal decreto presidenziale 14086 e rispettivamente dal regolamento sul procuratore generale, pur essendo più breve dei mandati dei giudici della CGUE (sei anni con possibilità di riconferma) e della Corte CEDU (nove anni senza possibilità di riconferma), non desta

[213] Articolo 3, lettera d), punto iv), del decreto presidenziale 14086; articolo 201.7 del regolamento sul procuratore generale.
[214] Articolo 201.3, lettera a), del regolamento sul procuratore generale.
[215] Articolo 201.3, lettera c, del regolamento sul procuratore generale.
[216] Articolo 201.7, lettera c, del regolamento sul procuratore generale.

gravi preoccupazioni in quanto tale. L'EDPB non è a conoscenza di alcuna giurisprudenza che imponga una durata minima del mandato a questo proposito[217]. L'EDPB riconosce inoltre che la possibilità di intraprendere attività extragiudiziali è soggetta alla condizione che, semplificando, tali attività non determinino conflitti di interesse che compromettono i doveri del DPRC. Dalle spiegazioni aggiuntive fornite dal governo degli Stati Uniti, l'EDPB ha appreso che anche tali prescrizioni sono soggette a riesame e monitoraggio da parte della PCLOB e dell'ispettore generale del Dipartimento della Giustizia (cfr. punto 226). Anche le modalità di applicazione e dimostrazione pratica di questa prescrizione dovrebbero essere affrontate nell'ambito dei riesami congiunti.

227. Ai sensi dell'articolo 3, lettera d), punto i), lettera B), del decreto presidenziale 14086, tutti i "giudici" del DPRC devono essere in possesso di nulla osta di sicurezza per poter accedere a informazioni classificate, ossia per svolgere la loro funzione effettiva di pronunciarsi in merito a cause in materia di sicurezza nazionale[218]. Alcune leggi e alcuni regolamenti europei in materia di nulla osta di sicurezza esentano invece i giudici dall'obbligo di un tale nulla osta nella misura in cui essi svolgono funzioni giudiziarie, ritenendo tale controllo dettagliato potenzialmente in conflitto con l'indipendenza giudiziaria[219]. Secondo le spiegazioni del governo degli Stati Uniti, mentre un candidato alla nomina a giudice in un organo giurisdizionale degli Stati Uniti è sottoposto a un esame approfondito, dopo la nomina a giudice federale nel contesto di un organo giurisdizionale degli Stati Uniti, un giudice federale non è tenuto a ottenere un nulla osta di sicurezza per accedere a documenti classificati pertinenti per una causa.

228. Secondo l'EDPB, dalle circostanze sopra descritte emergono in parte differenze tra la posizione e lo status di un giudice federale degli Stati Uniti e un "giudice" del DPRC. Tuttavia le garanzie fornite non danno motivo di dubitare dell'indipendenza del DPRC. L'EDPB esorta la Commissione a fare in modo che, in caso di adozione del progetto di decisione, le suddette garanzie costituiscano una priorità durante il primo riesame congiunto del DPF UE-USA. Inoltre l'EDPB si aspetta che la Commissione dia seguito all'impegno di sospendere, abrogare o modificare la decisione, laddove adottata, nel caso in cui l'esecutivo degli Stati Uniti decida di limitare le garanzie incluse nel decreto presidenziale[220].

3.2.4.3 Poteri del DPRC

3.2.4.3.1 Accesso alle informazioni

229. Una tutela giuridica efficace richiede che un organo giurisdizionale disponga di poteri investigativi sufficienti per riesaminare la misura contestata. Nella causa *Kadi II* la CGUE ha stabilito, in relazione all'articolo 47 della Carta, che i giudici dell'Unione europea devono assicurare che una decisione si fondi su una base di fatto sufficientemente solida[221]. La CGUE afferma che "spetta al giudice dell'Unione procedere a detto esame, chiedendo, se necessario, all'autorità competente dell'Unione

[217] Cfr. anche, mutatis mutandis, Corte CEDU (Grande Camera), Centrum För Rättvisa c. Svezia, 25 maggio 2021, punto 346.
[218] Cfr. articolo 201.11, lettera b), del regolamento sul procuratore generale e il considerando 177 del progetto di decisione.
[219] Ad esempio articolo 2, terzo comma, della legge tedesca sui nulla osta di sicurezza.
[220] Considerando 212 del progetto di decisione.
[221] CGUE, sentenza della Corte di giustizia del 18 luglio 2013, *Commissione europea e altri/Yassin Abdullah Kadi,* cause riunite C-584/10 P, C-593/10 P e C-595/10 P, ECLI:EU:C:2013:518 (in appresso: "sentenza *Kadi II* della CGUE"), punto 119.

di produrre informazioni o elementi probatori, riservati o meno, pertinenti per un siffatto esame"[222], nel qual caso "non possono essere opposti il segreto o la riservatezza di [...] informazioni o elementi"[223].

230. Ai sensi del considerando 181 del progetto di decisione, il DPRC riesamina le decisioni prese dal CLPO basandosi, quanto meno, sulle registrazioni dell'indagine svolta da quest'ultimo, nonché su tutte le informazioni e su tutti i documenti forniti dal reclamante, dall'avvocato speciale o da un'agenzia di intelligence. Il progetto di decisione afferma inoltre che il DPRC ha accesso a tutte le informazioni necessarie, che può ottenere tramite il CLPO. Ciò si basa sulla disposizione di cui all'articolo 201.9, lettera b), del regolamento sul procuratore generale, che autorizza il DPRC a richiedere che il CLPO dell'ODNI integri il fascicolo con specifiche informazioni esplicative o chiarificatrici e che il CLPO dell'ODNI formuli ulteriori constatazioni fattuali, ove necessario, al fine di consentire al collegio di giudici del DPRC di condurre il proprio esame. L'EDPB ritiene che la valutazione effettuata dal DPRC non sia in alcun modo limitata alle risultanze ottenute dal CLPO al primo livello del nuovo meccanismo di ricorso. Al contrario, il DPRC può richiedere sia ulteriori informazioni giuridiche e, soprattutto, ulteriori informazioni sulle circostanze di fatto al fine di analizzare se si sia verificata una violazione rientrante nell'ambito di applicazione della normativa in questione. Allo stesso tempo, l'EDPB rileva altresì che tali poteri investigativi generalmente ampi non si estendono all'accesso diretto ai dati detenuti in merito alla persona fisica di cui trattasi. La Commissione ha spiegato che il CLPO fungerà sempre da intermediario quando il DPRC richiederà ulteriori informazioni. Di conseguenza l'accesso del DPRC alle informazioni necessarie per valutare in modo indipendente una domanda di riesame si basa, in una certa misura, sul fatto che il CLPO fornisca le informazioni necessarie. L'EDPB riconosce che il CLPO è tenuto a fornire tutto il sostegno necessario al DPRC e le agenzie di intelligence sono tenute a fornire al CLPO accesso alle informazioni necessarie ai fini della conduzione dell'esame del DPRC[224]. Tuttavia l'EDPB rileva altresì che il CLPO stesso non è indipendente e conduce l'indagine iniziale di un reclamo nella prima fase della procedura di ricorso. Pertanto l'EDPB accoglie con favore il fatto che la PCLOB verifichi, durante i suoi riesami annuali del meccanismo di ricorso, se il DPRC ha ottenuto pieno accesso a tutte le informazioni necessarie[225]. Inoltre l'EDPB invita la Commissione a includere questo aspetto nei riesami congiunti, qualora il progetto di decisione venga adottato, al fine di esaminare le implicazioni di tale sistema nella pratica.

3.2.4.3.2 Poteri correttivi

231. Una delle principali carenze dello scudo per la privacy che ha portato alla sua invalidazione da parte della CGUE nella sentenza *Schrems II* è stata la mancanza di poteri correttivi vincolanti riconosciuti al mediatore. La CGUE ha rilevato che "non [vi è] [...] alcuna indicazione che tale Mediatore sia autorizzato ad adottare decisioni vincolanti nei confronti dei suddetti servizi"[226]. Il semplice impegno (politico) da parte del governo degli Stati Uniti a fare sì che la comunità dell'intelligence ponga rimedio a qualsiasi violazione delle norme applicabili rilevata dal mediatore non era sufficiente ad assicurare un livello di protezione sostanzialmente equivalente a quello garantito dall'articolo 47 della Carta.

232. Nel contesto del nuovo meccanismo di ricorso, invece, le decisioni adottate dal CLPO e dal DPRC hanno effetto vincolante[227]. L'EDPB riconosce, da un lato, che questa autorità non si limita a misure specifiche,

[222] Sentenza *Kadi II* della CGUE, punto 120.
[223] Sentenza *Kadi II* della CGUE, punto 125.
[224] Articolo 3, lettera c), punto i), lettera H, e articolo 3, lettera d), punto iii), del decreto presidenziale 14086.
[225] Articolo 3, lettera e), punto i), del decreto presidenziale 14086.
[226] Sentenza *Schrems II* della CGUE, punto 196.
[227] Rispettivamente articolo 3, lettera c), punto ii), e articolo 3, lettera d), punto ii), del decreto presidenziale 14086.

ma consente una "riparazione adeguata" al fine di "porre pienamente rimedio" a una violazione individuata rientrante nell'ambito di applicazione della normativa in questione. Nello specifico l'articolo 4, lettera a), del decreto presidenziale 14086 menziona esplicitamente la cancellazione dei dati raccolti illegalmente. Di contro, l'EDPB osserva che la formulazione dell'articolo 4, lettera a), del decreto presidenziale 14086 crea qualche incertezza sul processo di determinazione di tale "riparazione adeguata". Se da un lato una misura deve essere concepita per porre pienamente rimedio a una violazione, dall'altro occorre prendere in considerazione le modalità con cui una violazione del tipo individuato è stata abitualmente affrontata[228]. Il significato e l'effetto di tale prescrizione non sono chiari. Pertanto l'EDPB invita la Commissione a monitorare attentamente le misure di riparazione adottate nella pratica.

3.2.4.4 Presentazione di un reclamo nel contesto del nuovo meccanismo di ricorso

233. Il meccanismo di ricorso istituito ai sensi del decreto presidenziale 14086 è applicabile solo ai reclami qualificati trasmessi dall'autorità pubblica competente in uno Stato qualificato in merito alle attività di intelligence dei segnali degli Stati Uniti per qualsiasi violazione rientrante nell'ambito di applicazione della normativa in questione[229]. Di conseguenza per avvalersi di tale tutela giuridica, devono essere soddisfatte diverse condizioni.

3.2.4.4.1 Designazione come Stato qualificato

234. Innanzitutto, il paese o l'organizzazione regionale d'integrazione economica da cui i dati sono stati trasferiti negli Stati Uniti deve essere stato designato/a come Stato qualificato prima del trasferimento dei dati oggetto del reclamo[230]. Chiaramente è essenziale che il meccanismo di ricorso previsto sia disponibile quando la decisione di adeguatezza entra in vigore. Di conseguenza il considerando 196 del progetto di decisione stabilisce che l'entrata in vigore della decisione è subordinata, tra l'altro, alla designazione dell'Unione come soggetto qualificato ai fini del meccanismo di ricorso. In realtà la Commissione sembra presumere che la designazione avverrà prima dell'adozione della decisione, in quanto il progetto include già un segnaposto per la designazione dell'UE da parte del procuratore generale[231] (anziché includere la designazione come condizione sospensiva nel dispositivo del progetto di decisione).

3.2.4.4.2 Incidenza negativa sugli interessi di tutela della vita privata e delle libertà civili e sulla "legittimazione ad agire"

235. Un "reclamo qualificante" deve basarsi su una presunta "violazione rientrante nell'ambito di applicazione della normativa in questione", che a sua volta richiede l'esistenza di una violazione che incida negativamente sugli interessi individuali alla tutela della vita privata e alle libertà civili del reclamante[232]. L'EDPB ritiene, sulla base di ulteriori spiegazioni della Commissione, che l'espressione "incida negativamente" non implichi alcuna forma di restrizione all'ammissibilità di un reclamo. Piuttosto, come ha dichiarato la Commissione, tale effetto negativo riguarderebbe qualsiasi reclamo relativo al trattamento di dati personali per attività di intelligence dei segnali in violazione delle disposizioni di cui all'articolo 4, lettera d), punto iii), ad esempio le garanzie di cui al decreto presidenziale 14086. L'EDPB si rammarica che ciò non sia specificato nel testo del progetto di decisione e invita la Commissione a chiarire ulteriormente il concetto di "incida negativamente", al fine di

[228] Articolo 4, lettera a), del decreto presidenziale 14086.
[229] Articolo 3, lettera a), del decreto presidenziale 14086.
[230] Articolo 4, lettera d), punto i) e lettera k), punto i) del decreto presidenziale 14086.
[231] Cfr. nota 320 del progetto di decisione.
[232] Articolo 4, lettera k), punto i), e articolo 4, lettera d), punto ii), del decreto presidenziale 14086.

garantire che qualsiasi violazione dei diritti degli interessati sia valutata e vi sia posto rimedio e che non vi sia un livello di "gravità" da dimostrare per avere accesso a un ricorso e a una riparazione adeguata.

236. Come già menzionato, un reclamo a norma del decreto presidenziale 14086 non richiede che il ricorrente dimostri di essere legittimato (cfr. punto 215)[233]. L'EDPB accoglie con favore il chiarimento contenuto all'articolo 4, lettera k), del decreto presidenziale 14086, secondo cui verrà applicata una verifica del livello di "convinzione" e non è necessario dimostrare che i dati del denunciante sono stati effettivamente consultati attraverso attività di intelligence dei segnali. L'istituzione del meccanismo di ricorso costituisce un passo importante, poiché il requisito della legittimazione ad agire rende molto difficile contestare le misure di sorveglianza dinanzi agli organi giurisdizionali ordinari negli Stati Uniti.

237. Sulla base di quanto sopra, l'EDPB non ritiene che il ricorso agli organi giurisdizionali ordinari, a cui fa riferimento anche il progetto di decisione[234], offra un livello di protezione adeguato[235]. A questo proposito, l'EDPB ricorda le preoccupazioni già più volte espresse in relazione all'obbligo della legittimazione ad agire dinanzi agli organi giurisdizionali ordinari[236]. Inoltre, sulla base di ulteriori dichiarazioni formulate dal governo degli Stati Uniti, l'EDPB ritiene che, sebbene il decreto presidenziale 14086 non precluda il ricorso agli organi giurisdizionali aventi giurisdizione generale, non è certo come tali organi giurisdizionali applicherebbero tale decreto. La questione potrebbe essere approfondita nel contesto dei futuri riesami, in caso di adozione del progetto di decisione.

3.2.4.4.3 La procedura di reclamo

238. L'EDPB approva in linea di principio la procedura di indirizzamento di un reclamo attraverso le autorità di controllo degli Stati membri e continua a ritenere che l'identificazione del reclamante debba avvenire nel territorio dell'UE. Tuttavia, come nel caso del meccanismo del mediatore dello scudo per la privacy, la proposta di decisione prevede che l'interessato che desideri promuovere un reclamo di questo tipo debba presentarlo a un'autorità di controllo di uno Stato membro dell'UE competente per la vigilanza di servizi di sicurezza nazionali e/o del trattamento di dati personali da parte di autorità pubbliche[237]. A questo proposito l'EDPB ricorda le preoccupazioni già espresse nel parere del Gruppo di lavoro sullo scudo per la privacy, ad esempio le potenziali difficoltà per le persone di individuare l'autorità competente data la varietà dei meccanismi di controllo dei servizi di sicurezza nazionali negli Stati membri[238]. Tenendo conto del coinvolgimento delle autorità nazionali di protezione dei dati nell'applicazione e nella vigilanza in merito al DPF UE-USA, è più appropriato indirizzare i reclami attraverso di esse.

3.2.4.5 La decisione del DPRC

239. Al termine dell'esame della domanda del denunciante, il DPRC non deve rivelare se il denunciante sia stato o meno oggetto di attività di intelligence dei segnali da parte di soggetti degli Stati Uniti. Al contrario, il reclamante viene informato che l'esame non ha individuato alcuna violazione rientrante nell'ambito di applicazione della normativa in questione o che il Tribunale del riesame in materia di

[233] Clapper c. Amnesty International USA, 568 U.S. 398 (2013) II. pag. 10.
[234] Considerando 187 e seguenti del progetto di decisione.
[235] Cfr. anche sentenza *Schrems II* della CGUE, punti 191 e 192.
[236] Cfr. parere 01/2016 del Gruppo di lavoro, pag. 43.
[237] Considerando 169 del progetto di decisione.
[238] Parere 01/2016 del Gruppo di lavoro, pagg. 48 e 49.

protezione dei dati ha emesso una decisione che richiede una riparazione adeguata[239]. Questa risposta standard serve allo scopo in genere legittimo di proteggere informazioni sensibili sulle attività di intelligence svolte dagli Stati Uniti. Tuttavia l'EDPB è preoccupato per il fatto che il decreto presidenziale 14086 non prevede alcuna esenzione alla risposta standard del DPRC.

240. Nella causa *Kadi II*, la CGUE ha dovuto affrontare gli interessi contrastanti del segreto di Stato da un lato e di un procedimento equo e, per quanto possibile, in contraddittorio, dall'altro. La CGUE ha stabilito che in circostanze nelle quali considerazioni imperative riguardanti la sicurezza nazionale ostano alla comunicazione all'interessato di informazioni o elementi probatori, spetta comunque al giudice attuare tecniche che consentano di conciliare legittime preoccupazioni di sicurezza relative alla natura e alle fonti di informazione e la necessità di garantire adeguatamente all'interessato il rispetto dei suoi diritti processuali, quali il diritto ad essere sentito e il principio del contraddittorio[240]. La CGUE ha specificato ulteriormente che spetta al giudice, nell'esaminare il complesso degli elementi di diritto e di fatto forniti dall'autorità competente dell'Unione, verificare la fondatezza delle ragioni fatte valere da tale autorità per opporsi a siffatta comunicazione[241]. Qualora risulti che le ragioni addotte dall'autorità competente dell'Unione effettivamente ostano alla comunicazione all'interessato di informazioni o elementi probatori, sarà comunque necessario bilanciare adeguatamente le esigenze imposte dal diritto a una tutela giurisdizionale effettiva con quelle derivanti dalla sicurezza nazionale[242]. Per procedere ad un siffatto bilanciamento è ammissibile avvalersi di possibilità quali la comunicazione di una sintesi del contenuto delle informazioni o degli elementi probatori in questione[243]. Sebbene le conclusioni dell'organo giurisdizionale non impongano prescrizioni per la decisione emessa da un organo giurisdizionale, ma facciano piuttosto riferimento alla decisione dell'autorità competente e allo svolgimento del procedimento giudiziario, tali conclusioni forniscono indicazioni sul bilanciamento degli interessi di cui sopra nel contesto del diritto a una tutela giuridica efficace. Per ulteriori indicazioni, si può fare riferimento anche alla causa Big Brother Watch, nel contesto della quale la Corte CEDU, alludendo all'equità del procedimento e in particolare al principio del contraddittorio, ha stabilito che le decisioni di un organo giudiziario o comunque indipendente devono essere motivate[244].

241. L'EDPB riconosce che le decisioni del DPRC sono effettivamente motivate. Il DPRC è espressamente tenuto a emettere una decisione scritta che illustri le proprie determinazioni e la specificazione di qualsiasi riparazione adeguata[245]. Inoltre l'EDPB rileva che la persona sarà informata se le informazioni relative a un riesame da parte del DPRC sono state declassificate[246]. L'EDPB riconosce anche il ruolo degli avvocati speciali previsti nel nuovo meccanismo di ricorso, che include la difesa dell'interesse del reclamante nella questione[247]. Tuttavia, alla luce delle implicazioni della giurisprudenza della CGUE e della Corte CEDU di cui sopra e tenendo conto del fatto che la decisione del DPRC non può essere impugnata ma è definitiva[248], l'EDPB nutre preoccupazioni circa l'applicazione generale della risposta standard del DPRC. L'EDPB ricorda che la PCLOB esaminerà in modo indipendente il funzionamento del

[239] Articolo 3, lettera d), punto i), lettera H), del decreto presidenziale 14086. Tale articolo del decreto presidenziale 14086 prevede la medesima risposta anche per il CLPO.
[240] Sentenza *Kadi II* della CGUE, punto 125.
[241] Sentenza *Kadi II* della CGUE, punto 126.
[242] Sentenza *Kadi II* della CGUE, punto 128.
[243] Sentenza *Kadi II* della CGUE, punto 129.
[244] Sentenza *Big Brother Watch* della Corte CEDU, punto 359.
[245] Articolo 201.9, lettera g), del regolamento sul procuratore generale.
[246] Articolo 3, lettera d), punto v), del decreto presidenziale 14086.
[247] Articolo 201.8, lettera g), del regolamento sul procuratore generale.
[248] Articolo 201.9, lettera g), del regolamento sul procuratore generale.

nuovo meccanismo di ricorso e invita la Commissione a prestare particolare attenzione a tale questione, compresa qualsiasi valutazione relativa a questo aspetto da parte della PCLOB, durante i futuri riesami della decisione, laddove adottata.

4 ATTUAZIONE E MONITORAGGIO DEL PROGETTO DI DECISIONE

242. Per quanto riguarda il monitoraggio e il riesame del progetto di decisione, l'EDPB rileva che secondo la giurisprudenza della CGUE, "alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione di adeguatezza in forza dell'[articolo 45 GDPR], verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo"[249].

243. Inoltre l'EDPB rileva che la lettera del DoC prevede che quest'ultimo e altre agenzie degli Stati Uniti, a seconda dei casi, tengano riunioni periodiche con la Commissione, le autorità di protezione dei dati dell'UE interessate e i rappresentanti appropriati dell'EDPB[250].

244. L'EDPB ritiene che la protezione del diritto a livello statale in relazione all'accesso da parte delle autorità di contrasto, alla deroga per la raccolta temporanea in blocco in vista della raccolta mirata da parte delle autorità di sicurezza nazionale statunitensi, all'applicazione pratica dei principi di necessità e proporzionalità di recente introduzione, anche nel contesto del programma UPSTREAM, all'interazione tra il decreto presidenziale 14086 e i diversi strumenti giuridici statunitensi che consentono alle agenzie di intelligence di raccogliere e trattare ulteriormente dati personali, alle politiche e alle procedure interne di attuazione, al modo in cui tali garanzie saranno prese in considerazione anche nel contesto della vigilanza condotta dalla Corte FISA e al modo in cui il meccanismo di ricorso funzionerà in effetti, nonché alla questione dei trasferimenti successivi, alle decisioni automatizzate, alla vigilanza e l'applicazione sostanziali ed efficaci dei principi del DPF, così come all'efficacia dei ricorsi meriteranno un'attenzione specifica nel corso dei prossime riesami periodici.

245. L'EDPB rileva che il riesame dell'accertamento di adeguatezza avrà luogo dopo un anno dalla data di notifica della decisione di adeguatezza agli Stati membri e successivamente almeno ogni quattro anni[251]. Al fine di rafforzare ulteriormente il monitoraggio continuo della decisione di adeguatezza, l'EDPB invita la Commissione a effettuare i successivi riesami almeno ogni tre anni.

246. Per quanto concerne il coinvolgimento pratico dell'EDPB e dei suoi rappresentanti nella preparazione e nello svolgimento dei futuri riesami periodici, l'EDPB ribadisce che qualsiasi documentazione pertinente dovrebbe essere condivisa per iscritto con l'EDPB, compresa la corrispondenza, con sufficiente anticipo rispetto ai riesami. Come nel caso dei riesami effettuati nel contesto dello scudo per la privacy, l'EDPB raccomanda che, al più tardi tre mesi prima dello svolgimento del riesame, la Commissione, l'amministrazione statunitense e l'EDPB stabiliscano e concordino le modalità per lo svolgimento del riesame.

247. Inoltre l'EDPB rileva e accoglie con favore il fatto che il considerando 212 del progetto di decisione fornisca esempi di modifiche che compromettono il livello di protezione e che possono giustificare

[249] Sentenza *Schrems I* della CGUE, punto 76. Cfr. anche articolo 3, paragrafo 4, del progetto di decisione.
[250] Allegato III del progetto di decisione.
[251] Articolo 3, paragrafo 4, del progetto di decisione.

l'avvio di una "procedura di abrogazione d'emergenza", incentrata sulle modifiche che potrebbero verificarsi in relazione al decreto esecutivo 14086 e al relativo regolamento sul procuratore generale.

Per il Comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)