Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

Rapporto sul secondo riesame dello Swiss-US Privacy Shield (2019)

I. Introduzione

Il 14 settembre 2019 si è svolto a Washington D.C. il secondo riesame annuale congiunto dello scudo Svizzera-USA per la privacy (*CH-US Privacy Shield Review*) tra la delegazione svizzera e il Governo statunitense.

Dal 17 aprile 2017, da quando cioè è entrato in vigore il regime dello scudo Svizzera-USA per la privacy, oltre 3300 imprese hanno aderito a questo programma e dall'ultimo riesame (ottobre 2018) il numero di imprese certificate è aumentato di 1000 unità. La cerchia degli aderenti è composta per oltre il 70 per cento da PMI provenienti da diversi settori, in particolare da quello delle tecnologie dell'informazione e della comunicazione, dei servizi commerciali e professionali, dei media, dell'intrattenimento e della formazione. Sono tuttora certificate ai sensi dello scudo per la privacy anche grandi aziende come Facebook Inc. e Google LLC.

L'IFPDT è l'organo di contatto per le persone interessate in Svizzera e per le imprese.

Per quanto riguarda la parte commerciale dello scudo Svizzera-USA per la privacy, nell'anno in esame l'IFPDT ha ricevuto un solo caso da trasmettere al *Department of Commerce* (DoC). Si trattava di una «falsa dichiarazione» (*false claim*), ossia del caso di un'impresa che pur non essendolo aveva dichiarato di essere certificata ai sensi dello scudo per la privacy. Il caso ha potuto essere risolto in collaborazione con il DoC (cfr. anche il n. 1.4.).

Inoltre, sono stati presentati una decina di reclami legittimi contro imprese certificate a organi privati indipendenti per la composizione alternativa delle controversie (*alternative dispute resolution, ADR*) riguardanti il regime Svizzera-USA. Non sono pervenuti né reclami relativi a imprese certificate che hanno scelto l'IFPDT come organo di ricorso indipendente, né reclami in merito a dati dei dipendenti raccolti nell'ambito del diritto del lavoro (vigilanza obbligatoria da parte dell'IFPDT). L'IFPDT è invece stato consultato più volte da imprese con sede in Svizzera in merito ad ambiguità riguardanti il trasferimento dei dati verso gli Stati Uniti.

Dall'entrata in vigore del regime, all'IFPDT non è stato sottoposto alcun caso riguardante l'accesso ai dati personali da parte delle autorità statunitensi per motivi di sicurezza nazionale.

Rimane difficile valutare le ragioni per cui gli strumenti giuridici disponibili sono poco utilizzati dalle persone interessate in Svizzera. Una delle spiegazioni potrebbe essere la complessità del regime e la difficoltà di individuare eventuali violazioni della protezione dei dati. Come già menzionato, l'IFPDT è a disposizione come organo di contatto per le persone interessate in Svizzera e per le imprese. D'altro canto va ricordato che prima di rivolgersi a un'eventuale ADR/IFPDT bisogna contattare l'impresa certificata. Si può quindi presumere che un numero difficilmente quantificabile di violazioni della protezione dei dati venga già eliminato in questo modo.

Come l'anno precedente, al secondo riesame la Svizzera era rappresentata dalla SECO (direzione) e dall'IFPDT (ottica/vigilanza dal profilo del diritto sulla protezione dei dati). Per gli Stati Uniti hanno partecipato i rappresentanti del DoC.

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

La riunione si è svolta a conclusione del terzo riesame congiunto dello scudo UE-USA per la privacy, al quale la delegazione svizzera ha partecipato come osservatrice e dunque senza possibilità di prendere la parola. Al riesame congiunto UE-USA 2019 per gli Stati Uniti hanno partecipato rappresentanti delle seguenti autorità:

- Dipartimento del commercio (*Department of Commerce, DoC*);
- Dipartimento di Stato (*Department of State, DoS*);
- Commissione federale per il commercio (*Federal Trade Commission, FTC*);
- Dipartimento dei trasporti (*Departement of Transportation, DoT*);
- Ufficio del direttore dell'intelligence nazionale (*Office of the Director of National Intelligence, ODNI*);
- Dipartimento di giustizia (*Department of Justice, DoJ*);
- Comitato di tutela dei diritti alla privacy e alle libertà civili (*Privacy and Civil Liberities Oversight Board, PCLOB*), l'organo indipendente di monitoraggio della protezione della sfera privata e delle libertà civili,
- Mediatore (e collaboratore),
- Ispettore generale della comunità dei servizi segreti (*Inspector General of the Intelligence Community*)

Per l'UE hanno partecipato rappresentanti dei seguenti organi:

- Commissione europea,

- otto rappresentanti del Comitato europeo per la protezione dei dati (CEPD)

Come già l'anno scorso, date la similarità esistenti tra il regime svizzero e quello europeo in praticamente tutte le questioni contenutistiche, un gran numero di temi come per esempio l'accesso ai dati personali da parte delle autorità o importanti aspetti della parte commerciale inerenti al diritto della protezione dei dati (per es. settore di attività della FTC/ del DoT) sono stati trattati esclusivamente nell'ambito del riesame UE-USA (cfr. anche rapporto dell'IFPDT sul primo riesame congiunto dello scudo per la privacy, 2018[1]).

Per quanto riguarda l'Unione europea, la Commissione e l'CEPD (fino al 25 maggio 2018 il gruppo di lavoro articolo 29 [WP29]) hanno redatto propri rapporti sui riesami congiunti finora eseguiti (2017[2], 2018[3] e 2019[4]).

---

[1] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland/datenuebermittlung-in-die-usa.html

[2] WP29: 2017 https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf
Commissione europea: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52017DC0611

[3]CEPD:https://CEPD.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_it (disponibile soltanto in inglese)
Commissione europea: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_it (disponibile soltanto in inglese)

I precedenti scambi scritti con gli USA e la discussione avuta in occasione del terzo riesame congiunto UE-USA hanno permesso all'CEPD di trarre le sue principali conclusioni in materia di protezione dei dati. In generale tali conclusioni sono valide per analogia anche per lo scudo Svizzera-USA per la privacy. Le autorità statunitensi stanno quindi apportando adattamenti a entrambi i regimi tenendo conto della loro similarità.

Il ruolo dell'IFPDT corrisponde in gran parte a quello dell'CEPD (ex WP29).

Di conseguenza, il presente rapporto si sovrappone in larga misura a quello dell'CEPD.

Considerato il fatto che la Svizzera e l'UE riconoscono reciprocamente l'equivalenza dei loro sistemi giuridici in materia di protezione dei dati, la Svizzera dichiara adeguato il livello di protezione dei dati dello scudo Svizzera-USA per la privacy, nella misura in cui l'UE ritiene adeguato lo scudo UE-USA per la privacy.

Dopo che nel primo riesame del regime dello scudo Svizzera-USA per la privacy (2018) ci si era concentrati in particolare sull'istituzione e sulla gestione dei processi della parte commerciale del programma di scudo per la privacy e sulla presa di contatto personale con i rappresentanti statunitensi, quest'anno si è discusso intensamente anche dell'utilizzo del regime di scudo per la privacy da parte delle imprese con sede in Svizzera e di adattamenti e sviluppi specifici della parte commerciale.

Per dovere di completezza occorre menzionare il fatto che, nell'anno in esame, un arbitro residente in Svizzera si è fatto cancellare dall'elenco. Le autorità statunitensi hanno deciso di non procedere per il momento a una nuova nomina. Il meccanismo di arbitrato rimane comunque pienamente operativo per lo scudo Svizzera-USA per la privacy.[5]

Dal punto di vista della protezione dei dati, sono particolarmente rilevanti i seguenti punti:

II. Esame degli aspetti giuridici in materia di protezione dei dati

1. Aspetti commerciali

1.1. Informazioni e linee guida per le aziende statunitensi

Poiché il livello di protezione dei dati negli Stati Uniti non è considerato equivalente a quello elvetico, il trasferimento di dati dalla Svizzera agli USA è in linea di principio consentito soltanto alle condizioni di cui all'articolo 6 della legge federale sulla protezione dei dati (RS 235.1, DSG). Pertanto il regime dello scudo per la privacy è inteso a garantire un livello di protezione dei dati sufficiente a facilitare il trasferimento di dati negli USA alle aziende certificate nel regime definito nel testo dello scudo per la privacy. In considerazione di ciò e del fatto che l'interpretazione degli Stati Uniti del diritto sulla protezione dei dati è fondamentalmente diversa da quella della Svizzera (e dell'UE), è estremamente importante garantire un'interpretazione univoca del testo dello scudo per la privacy.

---

[4] CEPD: https://CEPD.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_it (disponibile soltanto in inglese)
Commissione europea: https://ec.europa.eu/commission/presscorner/detail/it/IP_19_6134

[5] Cfr. anche il sito Internet dell'IFPDT e la guida: https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/handel-und-wirtschaft/uebermittlung-ins-ausland/trasmissioni-di-dati-verso-gli-stati-uniti.html

In risposta a ciò, e su richiesta del WG29 prima e dell'CEPD poi (cfr. i rispettivi rapporti), dopo l'entrata in vigore del regime dello scudo per la privacy il DoC ha fornito guide per le imprese certificate sotto forma di FAQ (per es. «*Accountability for Onward Transfer Principle*»[6] e «*Processing Guidance*»[7]).

L'anno scorso il DoC ha pubblicato anche una scheda informativa sotto forma di FAQ sullo scudo per la privacy e il Regno Unito (Brexit)[8].

L'IFPDT si dice compiaciuto dell'approccio attivo assunto dal DoC per migliorare la comprensione da parte delle imprese e delle persone interessate del complesso testo riguardante lo scudo per la privacy.

Sulla base delle domande pervenutegli anche da parte di imprese con sede in Svizzera, l'IFPDT concorda in particolar modo con la proposta formulata dall'CEPD che il DoC, tra l'altro, illustri in modo più dettagliato la procedura per l'elaborazione dei dati relativi agli ordini o l'utilizzo di clausole contrattuali standard (*Standard Contractual Clauses; SCC*).

1.2. Informazioni chiare e di facile accesso per le persone interessate residenti in Svizzera

Come menzionato al numero I, la complessità del regime dello scudo per la privacy può rendere difficile alle persone interessate residenti in Svizzera e nell'UE far valere i propri diritti. Su richiesta del WP29 prima e dell'CEPD poi (cfr. i rispetti rapporti), fin dal primo anno di validità dello scudo UE-USA per la privacy e dello scudo Svizzera-USA per la privacy le autorità statunitensi hanno pubblicato sul proprio sito Internet informazioni più comprensibili sui diritti delle persone interessate, sui mezzi e sui rimedi giuridici disponibili. Sono illustrate anche le diverse possibilità di reclamo e in alcuni casi vengono forniti i corrispondenti link diretti. Dopo i primi riesami annuali del regime e in risposta alle proposte del WP29, il DoC ha aggiunto sul proprio sito Internet un documento di una pagina che fornisce una panoramica del programma, concentrandosi sui diritti degli individui e su come questi possono esercitarli[9].

Sono attese ulteriori guide.

Sul sito Internet dell'IFPDT sono pubblicate ulteriori informazioni sui diritti degli interessati svizzeri[10]. Come già detto, l'IFPDT può essere consultato per scritto o per telefono in caso di dubbi

1.3. Autocertificazione e rinnovo della certificazione (ricertificazione)

Per quanto riguarda la certificazione e la ricertificazione, nell'ambito del riesame svolto dal DoC sulla conformità delle imprese allo scudo per la privacy non vi sono stati cambiamenti rispetto al riesame dello scudo per la privacy dello scorso anno. Il DoC verifica i seguenti punti sia per la certificazione sia per la ricertificazione:

---

[6] https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs (disponibile soltanto in inglese)

[7] https://www.privacyshield.gov/article?id=Processing-FAQs (disponibile soltanto in inglese)

[8] https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs (disponibile soltanto in inglese)

[9] https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq

[10] https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/handel-und-wirtschaft/uebermittlung-ins-ausland/trasmissioni-di-dati-verso-gli-stati-uniti.html

- Registrazione a un meccanismo di ricorso indipendente (IRM)
- Pagamento dei contributi relativi all'allegato I *Arbitral Fund Contribution*
- Rispetto del «principio 8» (*Principle 8*) (Accesso ai dati personali)
- Completezza e coerenza dell'«informazione sulla certificazione» (*Certification Information*)
- Dichiarazione sulla protezione dei dati (la presenza dei 13 elementi richiesti dallo scudo per la privacy viene verificata anche nelle direttive sulla protezione dei dati delle imprese)

Ove necessario, il DoC continua a chiedere alle imprese di precisare le informazioni accessibili tramite link per facilitare agli interessati l'esercizio dei propri diritti. Inoltre, il DoC verifica gli annunci di incoerenza tra i dati contenuti nelle politiche sulla privacy delle imprese e quelli che figurano nell'elenco degli aderenti allo scudo per la privacy (per es. indicazioni riguardanti la certificazione per i dati delle risorse umane o dati al di fuori di questo settore). Grazie a queste verifiche, il DoC è stato in grado anche quest'anno di identificare il mancato rispetto dei requisiti in questo settore e di rifiutare l'adesione alle imprese non conformi allo scudo per la privacy. Il DoC continua a vietare alle imprese statunitensi di fare riferimento al programma di scudo per la privacy nelle loro politiche sulla privacy, fintanto che non avrà completato la verifica dell'autocertificazione e sarà stato pubblicato il nome dell'impresa nell'elenco degli aderenti allo scudo per la privacy, questo al fine di evitare incongruenze tra i dati contenuti nelle politiche sulla privacy e lo stato effettivo delle certificazioni iniziali.

L'IFPDT ritiene utili queste misure. Tuttavia, dal punto di vista sia dell'CEPD sia dell'IFPDT resta problematico il fatto che le verifiche effettuate dal DoC in base alle informazioni contenute nel riesame riguardino soprattutto criteri formali e non tocchino praticamente il rispetto del contenuto dei principi dello scudo per la privacy.

Un controllo materiale di questo tipo sarebbe tuttavia appropriato soprattutto perché la maggior parte delle imprese esegue la valutazione di conformità in modo indipen-dente (autocertificazione, *Compliance Assessment*) e non la affida a società esterne.

Come per il riesame dell'anno scorso dello scudo UE-USA per la privacy, anche quest'anno si è discusso del problema dato dal fatto che talvolta la validità della certificazione iniziale scade prima che sia concluso il processo di ricertificazione cosicché, per un certo periodo di tempo, talune imprese figurano nell'elenco degli aderenti senza una certificazione valida. Secondo le informazioni fornite durante il terzo riesame dello scudo UE-USA per la privacy, la durata del processo di ricertificazione può superare anche di 105 giorni la data di scadenza effettiva. Durante questo lasso di tempo le imprese rimangono sull'elenco degli aderenti come «attive».

L'IFPDT concorda con l'CEPD sul fatto che in questo lasso di tempo non vi sia alcuno svantaggio per le persone fintanto che l'impresa statunitense si impegna pubblicamente a rispettare in ogni momento i principi dello scudo per la privacy. Come l'CEPD, l'IFPDT è dell'opinione che bisognerebbe però trovare una soluzione in modo tale che la protezione delle persone interessate sia sempre garantita e non vi siano incertezze al riguardo. Nel frattempo, sia le persone sia le imprese interessate in Svizzera e nell'UE che trasferiscono dati personali a imprese statunitensi certificate devono essere rese attente sulla necessità di verificare di volta in volta la validità della certificazione.

Il terzo riesame dello scudo UE-USA per la privacy ha inoltre messo in risalto che sull'elenco degli aderenti allo scudo per la privacy figuravano diverse imprese «attive» benché la loro ricertificazione fosse scaduta nel 2018. In occasione del riesame di quest'anno l'CEPD ha chiesto al DoC di introdurre procedure per garantire che l'elenco degli aderenti «attivi» sia sempre aggiornato.

1.4. Rispetto dei principi: vigilanza e sorveglianza da parte del DoC

In occasione del primo riesame dello scudo UE-USA per la privacy (2017) il WP29 aveva criticato il fatto che per la vigilanza sugli aspetti commerciali dello scudo per la privacy si ricorresse soprattutto a impre-

se terze che mettevano a disposizione un meccanismo di ricorso indipendente (*Independent Recourse Mechanism*; IRM), e che il DoC non praticasse una vigilanza e un monitoraggio d'ufficio sufficienti.

Il successivo riesame dello scudo per la privacy pubblicato nel 2018 (il primo riguardante lo scudo Svizzera-USA per la privacy) ha evidenziato miglioramenti significativi per quanto riguarda la vigilanza da parte delle autorità statunitensi in entrambi i regimi (cfr. rapporto IFPDT, 2018 n. 1.4.).

Secondo le informazioni di quest'anno, lo scorso anno il DoC ha aumentato a 30 il numero mensile di imprese selezionate in modo casuale per i controlli a campione e ha inviato in totale 670 avvertimenti, per lo più riguardanti le cosiddette «false dichiarazioni» (*false claims*). Sebbene vadano accolti con favore i miglioramenti che il DoC ha apportato per garantire il rispetto formale dei principi dello scudo per la privacy, come indicato nell'ultimo rapporto, sia il Comitato europeo per la protezione dei dati (CEPD) sia l'IFPDT considerano problematico il fatto che i controlli continuino a essere incentrati più sulle formalità da espletare che non sul contenuto dei principi. Pertanto, nell'ambito del suo terzo riesame, l'CEPD continua a chiedere al DoC di estendere le sue attività di vigilanza così da includere elementi sostanziali come per esempio il principio della finalità. Anche in relazione al trasferimento successivo (*onward transfer*) il DoC non ha per esempio ancora chiesto copie delle disposizioni sulla privacy (*privacy provisions)* degli accordi tra le organizzazioni statunitensi e i loro mandatari (*agents*). Tuttavia, poiché i trasferimenti successivi possono essere fatti anche verso Stati terzi sprovvisti di un'adeguata protezione dei dati, dovrebbe essere sorvegliata anche la responsabilità. Il DoC continua a considerare che con la loro certificazione le imprese assumono obblighi giuridicamente vincolanti. Di conseguenza, anche gli interessati devono agire in prima persona. Il regime non prevede tuttavia controlli più sostanziali (cfr. anche n. 1.4. pag. 5 del rapporto 2018). Si potrebbe però ampliare il contenuto dei campioni.

Come l'CEPD, anche l'IFPDT ritiene opportuno che il DoC effettui controlli sostanziali per verificare che le imprese autocertificate applichino nella pratica i requisiti materiali dello scudo per la privacy. L'IFPDT seguirà gli ulteriori sviluppi e rimarrà in contatto con i rappresentanti dell'UE e degli USA.

1.5. Rispetto dei principi: vigilanza e sorveglianza da parte della FTC

L'IFPDT non ha potuto avere contatti diretti ufficiali con i rappresentanti della FTC neppure in occasione del secondo riesame congiunto. Questo perché i rappresentanti della FTC hanno partecipato esclusivamente al riesame UE-USA, al quale la Svizzera ha preso parte soltanto come osservatrice (cfr. n. I) senza possibilità di formulare domande. Tuttavia, le affermazioni fatte in quella sede valgono per analogia anche per il regime dello scudo Svizzera-USA per la privacy.

Dall'ultimo riesame dello scudo per la privacy la FTC ha registrato in totale sette nuovi casi. I casi di non conformità riguardano errori amministrativi e non violazioni materiali dei principi dello scudo per la privacy. L'CEPD raccomanda di effettuare ulteriori controlli sul trasferimento, in quanto le soluzioni create dalle imprese certificate non vengono controllate neppure dal DoC.

All'interno della divisione per la protezione dei dati e dell'identità della FTC, il *Bureau of Consumer Protection*, 40 avvocati si occupano quasi esclusivamente della protezione dei dati con, tra l'altro, il supporto tecnico di esperti. Per quanto riguarda la transazione raggiunta lo scorso anno con Facebook, nel riesame di quest'anno la FTC ha chiarito che l'ambito coperto da tale transazione non rientra nel campo d'applicazione dello scudo per la privacy.

L'CEPD constata con piacere che la FTC sta agendo sempre più spesso d'ufficio. Tuttavia, poiché quest'ultima continua a non fornire dettagli, rimane impossibile valutare i casi concreti e le sue attività. Ne consegue dunque l'impossibilità di valutare in che misura la FTC controlli effettivamente il rispetto dei principi.

1.6. Meccanismi di ricorso indipendenti (Independent Recourse Mechanisms, IRM)

Il numero di reclami ricevuti dai fornitori di IRM ha subito un leggero aumento rispetto all'ultimo riesame. I reclami sembrano tuttavia riguardare soprattutto aspetti di tecnica procedurale e non il sostanziale rispetto dei principi. Lo strumento dell'IRM non può quindi sostituire un maggiore controllo materiale da parte delle autorità statunitensi (cfr. n. 1.4. e 1.5.).

Come indicato nel rapporto sul riesame 2018, le società IRM sono tenute a descrivere nei rispettivi rapporti annuali in che modo evitano o intendono risolvere eventuali conflitti d'interesse (cfr. al riguardo n. 1.6. pag. 6 del rapporto 2018). A questo proposito il DoC ha spiegato di avere aggiornato le sue linee guida per il rapporto annuale sull'IRM al fine di individuare potenziali conflitti d'interesse. Ha inoltre incluso una descrizione di come poter evitare simili situazioni. Le linee guida non coprono tuttavia tutti gli aspetti contenuti nei rapporti. In particolare, l'CEPD ha rilevato che non è stato ancora introdotto un formato standard per i rapporti. Per garantire la totale confrontabilità, l'CEPD raccomanda pertanto al DoC d'introdurre un modello standardizzato per il rapporto annuale sull'IRM, che includa anche spiegazioni su come evitare possibili conflitti d'interesse.

1.7 Dati relativi alle risorse umane (RU)

Come già menzionato nel rapporto precedente (cfr. n. 1.7. rapporto 2018), l'UE e la Svizzera interpretano in modo diverso rispetto alle autorità statunitensi il concetto di dati delle risorse umane nel contesto dello scudo per la privacy. Nell'ultimo anno il DoC e le autorità europee hanno continuato a discutere sulle loro diverse interpretazioni di questo concetto, senza però giungere a un accordo. A causa di questa persistente discordanza tra le due definizioni, nell'ultimo riesame, come anche in questo, l'attenzione si è concentrata non tanto sul concetto in sé quanto sulle conseguenze che possono avere definizioni differenti. L'CEPD e l'IFPDT temono che ai dati raccolti al di fuori del processo di assunzione le autorità statunitensi o europee non applichino le misure di protezione supplementari stabilite nel regime per i dati personali dei dipendenti (p. es. trattamento dei dati a fini di marketing sulla base del consenso [opt-in] anziché diritto di opposizione [opt-out]). L'IFPDT condivide il parere dell'CEPD, secondo cui i dati personali devono sottostare a requisiti più severi indipendentemente dal fatto che siano trattati dal datore di lavoro o da un responsabile del trattamento (cfr. anche rapporto 2018, n. 1.7.). Le autorità europee e statunitensi porteranno avanti le discussioni al riguardo.

2. Accessi delle autorità a dati personali / sicurezza nazionale

Dall'ultimo riesame il quadro normativo statunitense non è cambiato in modo significativo. Rimangono pertanto invariate le principali riserve espresse dal WP29, e quindi dall'CEPD, e dall'IFPDT nei rapporti dello scorso anno in merito all'accesso da parte delle autorità a dati personali nell'ambito dello scudo per la privacy per motivi di sicurezza nazionale o ai fini del perseguimento penale. Le preoccupazioni riguardano in particolare la raccolta dei dati, la vigilanza, il ricorso e il meccanismo del mediatore. Da notare inoltre che attualmente la causa «Schrems II» (causa C-311/18) è pendente dinanzi alla Corte di giustizia dell'Unione europea (CGUE) e, poiché riguarda anche lo scudo UE-USA per la privacy, indirettamente è importante anche per lo scudo Svizzera-USA. La sentenza è prevista entro marzo e maggio 2020.

I rappresentanti statunitensi responsabili della sicurezza nazionale erano presenti soltanto al riesame UE-USA, al quale l'IFPDT ha partecipato in qualità di osservatore e pertanto non ha potuto esprimersi. Considerato che i regimi coincidono, l'IFPDT concorda con le osservazioni formulate dall'CEPD sull'accesso delle autorità, se non diversamente menzionato in modo esplicito qui di seguito. Si fa pertanto riferimento, in particolare, alla relazione dell'CEPD del 12 novembre 2019, (cfr. sopra, n. I), e anche ai rapporti del 22 gennaio 2019 e al rapporto del WP29 del 28 novembre 2017 (cfr. sopra n. I).

2.1. Raccolta di dati per motivi di sicurezza nazionale

2.1.1 Raccolta di dati secondo la sezione 702 del Foreign Intelligence Surveillance Act (FISA)

L'CEPD ribadisce la necessità di una valutazione indipendente della proporzionalità e della necessità in relazione alla definizione di obiettivi (*targets*) e al concetto di intelligence straniera (*foreign intelligence*) secondo la sezione 702 del FISA (anche nel contesto del programma UPSTREAM). Mantiene inoltre la propria richiesta di un'ulteriore valutazione indipendente dell'utilizzo di selezionatori (*selectors*) nei singoli casi (compito dei selezionatori «*tasking of selectors*», p. es. telefono, indirizzi e-mail ecc.). Il Comitato continua inoltre a chiedere ulteriori chiarimenti/spiegazioni circa il programma di sorveglianza UPSTREAM, in modo da escludere la possibilità che vengano raccolti (in blocco) in modo arbitrario dati personali di cittadini non statunitensi secondo la sezione 702 (cfr. anche rapporto 2018, n. 2.1.).

Riguardo alla sezione 702 del FISA, le discussioni del riesame di quest'anno hanno chiarito che la «persona» da identificare come «target» può riferirsi a più persone con lo stesso identificatore, a condizione che nessuna di esse sia cittadina statunitense e che tutte soddisfino i criteri applicabili per il raggiungimento dell'obiettivo.

L'CEPD si compiace del fatto che, in qualità di autorità di vigilanza indipendente, il *Privacy and Civil Liberities Oversight Board* (PCLOB), ora pienamente funzionante, abbia deciso di esaminare i dati chiesti dal FBI in base alla sezione 702, e che il PCLOB abbia indicato che avrebbe verificato in quale misura sono state prese in considerazione le raccomandazioni che aveva formulato nel suo rapporto sulla suddetta sezione. Tuttavia, l'CEPD si rammarica che il PCLOB non preveda di stilare e pubblicare un rapporto generale aggiornato sulla sezione 702 in base al rapporto presentato nel 2014. Un rapporto generale aggiornato contribuirebbe a fornire una valutazione delle nuove disposizioni di suddetta sezione (rinnovo dell'autorizzazione nel 2017) e delle procedure dei servizi segreti.

2.1.2. Raccolta di dati in base all'Executive Order 12333 (EO12333)

L'CEPD sostiene che l'adeguatezza del livello di protezione dei dati non dovrebbe limitarsi al monitoraggio entro i confini fisici/geografici di uno Stato terzo. Andrebbero piuttosto analizzate le basi legali che consentono a questo Stato terzo di effettuare un monitoraggio al di fuori del proprio territorio nazionale in relazione ai dati di cittadini UE (o svizzeri). Le limitazioni dell'accesso statale ai dati personali dovrebbero essere estese ai dati che sono «in viaggio» verso un Paese per il quale è riconosciuta l'adeguatezza.

In occasione dell'ultimo riesame le autorità statunitensi hanno sottolineato che l'EO 12333 non può essere utilizzato come base per la raccolta di dati all'interno del territorio statunitense e che la raccolta di dati nell'ambito di questo EO non rientra nel campo d'applicazione dello scudo per la privacy (cfr. anche il rapporto dello scorso anno dell'IFPDT, n. 2.1.).

Considerate l'incertezza e l'imprevedibilità persistenti riguardo all'applicazione dell'EO 12333, l'CEPD ha ribadito l'importanza che il PCLOB rediga rapporti chiarificatori su questo testo. Molto probabilmente però questi rapporti rimarranno segreti e non saranno messe a disposizione del pubblico o dei rappresentanti di Stati terzi ulteriori informazioni sul funzionamento concreto dell'EO12333 (e sulla sua necessità e proporzionalità).

2.1.3. Misure di protezione secondo la Presidential Policy Directive 28 (PPD-28)

L'CEPD ha accolto favorevolmente l'applicazione (di fondo) della PPD-28 confermata dalle autorità statunitensi (cfr. anche rapporto dell'IFPDT sul primo riesame, 2018), in particolare perché è l'unica che prevede garanzie e restrizioni per la raccolta e l'utilizzo di dati al di fuori degli USA (le restrizioni del FISA e altre leggi statunitensi più specifiche non sono applicabili a tal fine).

Al fine di proteggere meglio la privacy di tutti gli individui, inclusi i cittadini non statunitensi, la PPD-28 limita a sei i motivi di sicurezza nazionale in base ai quali può essere effettuata una raccolta di dati in blocco (spionaggio, terrorismo, cybersecurity, armi di distruzione di massa, pericoli per le forze armate, minacce criminali transfrontaliere).Nell'ambito del terzo riesame dello scudo UE-USA per la privacy non c'è stata alcuna nuova discussione sostanziale sull'interpretazione e sull'applicazione dei sei motivi di sicurezza che avrebbe permesso di valutare le garanzie fornite dalle autorità statunitensi.

Queste ultime sostengono che gli Executive Order e le Presidential Policy Directive sono «giuridicamente vincolanti». Tuttavia, occorre tenere presente che questi strumenti giuridici non creano diritti che possono essere fatti valere. Pertanto, le persone interessate in Svizzera o nell'UE non potrebbero ad esempio invocare direttamente la violazione della PPD-28 dinanzi a un tribunale statunitense (cfr. anche rapporto dell'IFPDT, 2018, n. 2.3.).

2.2. Vigilanza sul programma di sorveglianza delle autorità statunitensi

L'CEPD rammenta che è fondamentale una vigilanza completa su tutti i programmi di sorveglianza.

Già durante i due precedenti riesami annuali congiunti sono state presentate le attività di vigilanza di più organismi/unità. Secondo l'CEPD esiste una struttura di vigilanza completa composta da diverse unità, in parte indipendenti dalla comunità dei servizi segreti, tra cui i *Privacy and Civil Liberty officer*, l'ispettore generale (*Inspector General*), il PCLOB, la FISC ed il Congresso.

L'CEPD accoglie favorevolmente anche la nomina degli ultimi membri mancanti del PCLOB, che ora è pienamente operativo. Quest'ultimo ha presentato per la prima volta il suo programma di lavoro e l'CEPD si è espresso in modo positivo sulla trasparenza di questo organo di vigilanza. L'CEPD considera il PCLOB un importante organo indipendente all'interno della «struttura di vigilanza».

L'CEPD chiede però nuovamente la pubblicazione di rapporti nonché aggiornamenti dei rapporti precedenti (sezione 702 del FISA, PPD-28).

In generale va notato che è pressoché impossibile verificare opportunamente la vigilanza sui programmi di sorveglianza delle autorità statunitensi perché ai rappresentanti di Stati terzi viene concesso l'accesso soltanto ai documenti pubblici.

2.3. Vie legali per interessati svizzeri

Come menzionato nel rapporto dell'IFPDT dello scorso anno (n. 2.3.), per poter affermare che il livello di protezione dei dati di uno Stato terzo è adeguato è fondamentale che le persone interessate in Svizzera abbiano accesso a un organo di ricorso indipendente e imparziale.

Dato che, secondo le informazioni fornite dalle autorità statunitensi, il quadro giuridico non è cambiato rispetto all'ultimo riesame, occorre rinviare alle osservazioni formulate in quella sede (cfr. rapporto IFPDT 2018, n. 2.3.).

Un controllo giudiziario delle pratiche di sorveglianza (sezione 702 del FISA, EO12333 ecc.) è tuttora irrealistico a causa dell'attuale interpretazione molto restrittiva dei requisiti procedurali («*standing requirements*»). Il riesame UE-USA ha confermato che l'interpretazione del concetto di «standing» nelle questioni di sorveglianza è ancora in fase di sviluppo e vi sono ancora casi pendenti[11].

[11] Cfr. in particolare le cause ACLU v. Clapper e Wikipedia v. NSA

2.4 Il meccanismo del mediatore (ombudsperson)

Nel contesto del terzo riesame dello scudo UE-USA per la privacy, l'CEPD ha accolto con favore la nomina di Keith Krach a mediatore «permanente», il 18 gennaio 2019.

Dato che attualmente il meccanismo del mediatore costituisce praticamente l'unica possibilità diretta per verificare che le autorità statunitensi rispettino i principi legali della protezione dei dati secondo la PPD-28, l'EO 12333, la Sezione 702 FISA ecc., è essenziale che il mediatore sia indipendente e imparziale.

In qualità di sottosegretario di Stato per la crescita economica, l'energia e l'ambiente, Keith Krach è indipendente dai servizi segreti ma non dal Governo degli Stati Uniti.

Per quanto riguarda il trattamento dei reclami degli interessati, i mediatori di volta in volta in carica e il Governo statunitense hanno già spiegato in occasione degli ultimi riesami la garanzia del trattamento legale ed efficiente dei reclami. I collaboratori del mediatore hanno illustrato mediante casi astratti come vengono trattati i reclami (cfr. anche rapporto IFPDT 2018, n. 2.4.). Keith Krach ha confermato che, come i suoi predecessori, firma le lettere di chiusura dei casi soltanto se è convinto che siano stati trattati in modo regolare e che porta la controversia fino al livello più altro dell'autorità governativa statunitense se non è convinto del risultato che gli viene presentato.

Poiché le procedure relative all'accesso del mediatore alle informazioni rilevanti e all'interazione con la comunità dei servizi segreti comprese le autorità di vigilanza rimangono parzialmente segrete, risulta molto difficile valutare la procedura.

Anche se non ci sono indizi concreti per mettere in dubbio l'integrità del nuovo mediatore, l'CEPD chiede maggiori informazioni sui poteri che egli detiene nei confronti della comunità dei servizi segreti.

Sulla base delle informazioni disponibili non è ancora possibile concludere che le competenze del mediatore nei confronti dei servizi segreti siano sufficienti, poiché il suo «potere» in caso di violazione del diritto sembra essere limitato alla possibilità di confermare il mancato rispetto dei diritti fondamentali nei confronti del reclamante. Inoltre, le decisioni del mediatore non sono impugnabili dinanzi a un tribunale.

Questo si rivela problematico per quanto riguarda il diritto fondamentale a un procedimento dinanzi a un tribunale indipendente e imparziale.

III. Conclusione:

L'IFPDT esprime soddisfazione per gli sforzi compiuti dalle autorità statunitensi per migliorare il programma dello scudo per la privacy, in particolare per le misure di attuazione e di vigilanza adottate d'ufficio e la nomina degli ultimi membri mancanti del PCLOB e del mediatore permanente.

Rimangono tuttavia ancora punti da migliorare. Per quanto riguarda gli aspetti commerciali l'EDPB e l'IFPDT continuano a chiedere ad esempio lo svolgimento di controlli materiali da parte del DoC, il rispetto dei requisiti del trasferimento successivo o la soluzione alla problematica dei dati personali dei dipendenti (dati delle risorse umane).

Per quanto riguarda la raccolta di dati da parte delle autorità statunitensi, sarebbero utili tra l'altro rapporti ad esempio sulle garanzie della PPD-28.

Quanto al meccanismo del mediatore, dalle informazioni fornite in sede di riesame UE-USA non si può concludere che il mediatore abbia sufficienti poteri per accedere alle informazioni e porre rimedio alle violazioni della protezione dei dati. Attualmente non è quindi possibile affermare con certezza che il

meccanismo del mediatore soddisfi le esigenze di un organo di ricorso indipendente e imparziale neppure per lo scudo Svizzera-USA per la privacy.

a ricordato che bisognerà attendere la risoluzione delle cause pendenti dinanzi alla CGUE, in particolare la causa «Schrems II», che avrà un impatto indiretto anche sulla Svizzera.