Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2023-2024

Titolo tesi:

Il Data Privacy Framework EU-US: un’analisi sulle novità in tema di accesso e uso di dati personali trasferiti dall’Unione Europea da parte di autorità pubbliche negli Stati Uniti

Relatrice: Prof.ssa Annalisa Volpato

Studente**:** Mattia Linguanotto

ABSTRACT

Questa tesi intende esaminare gli sviluppi normativi e giurisprudenziali del flusso transatlantico di dati verso gli Stati Uniti, focalizzandosi sulle potenziali criticità legate all'accesso e all'utilizzo di dati da parte delle autorità pubbliche statunitensi nel quadro del Data Privacy Framework EU-US, il nuovo accordo che regola lo scambio di dati tra Unione Europea e Stati Uniti.

Gli accordi che consentono il flusso di dati verso paesi terzi costituiscono uno strumento fondamentale negli scambi internazionali, e la mancanza di un regime stabile ha effetti negativi sulle imprese europee e statunitensi.

Inizialmente viene delineato il quadro giuridico europeo che permette il trasferimento dei dati extra UE e i principi che lo sorreggono.

Successivamente, il presente elaborato si concentra sul flusso transatlantico di dati verso gli Stati Uniti, patria delle principali aziende che trattano le informazioni personali dei cittadini europei.

Si intende seguire da vicino la giurisprudenza della Corte di Giustizia dell'UE, dalla vicenda del Safe Harbour fino all'invalidazione del Privacy Shield, prestando attenzione alle criticità rilevate dalla Corte.

Seguirà poi un'analisi del Data Privacy Framework EU-US, il nuovo meccanismo messo in funzione dalla decisione di esecuzione della Commissione europea nel luglio 2023.

L'esame dell'accordo si concentra sulle novità proposte e sulle problematiche che potrebbero emergere con riguardo al trattamento effettuato da enti governativi per motivi di contrasto penale o di sicurezza nazionale, accompagnato da uno studio della legislazione statunitense in materia di sorveglianza, al fine di valutare se sia realmente garantito un livello sostanzialmente equivalente agli standard europei.

INDICE

1) Introduzione

Un volume consistente di dati personali dell'Unione Europea sono trasferiti e trattati oltreoceano. L'accordo che permette il flusso di dati verso gli Stati Uniti è uno strumento essenziale per il commercio internazionale, soprattutto se si considera l'aumento dei volumi degli scambi internazionali di dati a livello globale, come diretta conseguenza del fatto che "*i dati sono ora una materia prima centrale per l'economia globale*"[1].

I precedenti accordi tra Stati Uniti e UE si sono rilevati inadeguati nel tutelare i diritti degli interessati dell'Unione, specialmente a causa di un accesso e trattamento sproporzionato di dati personali da parte di autorità pubbliche statunitensi, violando i diritti fondamentali della privacy e della protezione dei dati personali, riconosciuti rispettivamente dall'art. 7 e 8 della Carta[2], nonché di un ricorso giurisdizionale effettivo per tali violazioni, in contrasto con l'art. 47 della Carta[3]. Alla luce del Data Privacy Framework, il nuovo regime per lo scambio di dati, la tesi intende fornire una panoramica delle criticità e delle novità dell'attuale decisione di esecuzione, in particolare sulle garanzie previste per gli individui in materia di trattamento per esigenze di sicurezza nazionale e contrasto penale, al fine di valutare se sia garantito negli Stati Uniti un livello di protezione sostanzialmente equivalente agli standard europei.

Qualora i dati vengano trasferiti verso un paese terzo, oltre ad una base giuridica per il trattamento dei dati di cui all'art. 6 e 9 del GDPR, è necessario adottare un layer addizionale di protezione in conformità con il Capo V del GDPR, che

---

[1] Christopher Kuner, 'Background and Introduction', *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013) 1 <https://global.oup.com/academic/product/transborder-data-flows-and-data-privacy-law-9780199674619?cc=it&lang=en&>. Tutte le traduzioni sono dell'autore.

[2] Art. 7 Carta: "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*"; Art. 8 Carta: "(1) *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.* (2) *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica*"

[3] Art. 47 Carta: "(1) *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* […]"

disciplina il trasferimento internazionale di dati attraverso un approccio multilivello.
Solitamente, gli accordi per il trasferimento si fondano su una decisione di adeguatezza ai sensi dell'art. 45 del GDPR, un atto esecutivo della Commissione europea con il quale constata che un paese terzo garantisce un livello di protezione adeguato, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali.
La presenza di tale decisione permette il flusso di dati senza richiedere ulteriori garanzie.
In mancanza di una decisione di adeguatezza, l'art. 46 stabilisce che il trasferimento può avvenire solo se vengono predisposte "*garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*".
In assenza di regimi validi, il flusso di dati UE-USA si è fondato su clausole contrattuali tipo ("Standard Contractual Clauses"), clausole ad hoc redatte dalla Commissione che vengono inserite nel contratto tra il titolare o responsabile del trattamento nell'UE e il destinatario dei dati in un paese terzo.
L'elaborato descrive i principali sviluppi giurisprudenziali e normativi del flusso transatlantico di dati, analizzando la legislazione statunitense in materia e riunendo le opinioni sul nuovo regime sviluppate a livello istituzionale e dottrinale. In questo modo si individuano le principali criticità dell'accordo in tema di accesso e uso dei dati personali da parte di enti pubblici, con lo scopo di fornire un'idea sul grado di stabilità che offre per le imprese europee e statunitensi che ne usufruiscono.
La tesi analizza (2) la giurisprudenza della Corte, dalla vicenda del Safe Harbour fino all'invalidazione del Privacy Shield, (3) spostandosi poi ad un esame del Data Privacy Framework, concentrandosi sulle questioni controverse sollevate dalla Corte, ovvero (3.1) le garanzie di necessarietà e proporzionalità previste per le misure attuate da autorità pubbliche a fini di contrasto penale e sicurezza nazionale e (3.2) l'effettività e indipendenza dei meccanismi di ricorso. (4) In conclusione, vengono delineate le prospettive future dell'accordo e del flusso internazionale di dati.

2) Il trasferimento di dati personali UE-USA

2.1) Il Safe Harbour e la sentenza Schrems I

Nel luglio 2000, la Commissione aveva adottato una decisione di esecuzione[4] in base all'articolo 25 della Direttiva 95/46. Tale decisione riconosceva che gli Stati Uniti assicuravano un livello di protezione adeguato, permettendo il trasferimento internazionale di dati dallo Spazio Economico Europeo ad aziende statunitensi certificate ai sensi dell'accordo.

Come i successivi regimi per il trasferimento internazionale di dati, quali il Privacy Shield e il Data Privacy Framework, il regime dell'Approdo Sicuro ("Safe Harbour") permetteva un trasferimento e successivo trattamento di dati personali alle aziende statunitensi certificate presso il *Department of Commerce* che aderiscono su base volontaria ai principi contenuti nell'allegato I dell'accordo.

Nel giugno 2013, Edward Snowden divulgò l'esistenza e il funzionamento del programma PRISM, un programma di sorveglianza della NSA che consentiva all'intelligence statunitense di accedere a dati relativi a metadati e contenuti di comunicazioni di individui statunitensi e non, compresi i cittadini e residenti nell'UE[5]. Queste dichiarazioni hanno portato la Commissione ad esprimere al Parlamento europeo e al Consiglio le sue preoccupazioni sulla sorveglianza di massa statunitense in due comunicazioni, nelle quali sottolineava l'importanza della relazione commerciale reciproca tra UE e USA, un interesse comune che deve essere perseguito garantendo un livello di protezione adeguato ai dati degli individui europei[6]. Inoltre, notava come le principali aziende statunitensi nel campo della raccolta, trattamento, uso e divulgazione dei dati erano

[4] Decisione di esecuzione (UE) 2000/520 della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti. 2000 (OJ L).
[5] John W Rollins and Edward C Liu, 'NSA Surveillance Leaks: Background and Issues for Congress' [2013] Congressional Research Service 1-21, 3.
[6] Commissione europea, "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA 2013" (Comunicazione) COM(2013) 846 final. 2013.

certificate nel quadro dell'Approdo sicuro e consentivano alle autorità americane, di accedere ai dati da loro detenuti[7].
Come stabilito nell'allegato I della decisione che implementava il regime dell'Approdo Sicuro, "*l'adesione a tali principi può essere limitata se necessario per esigenze di sicurezza nazionale* […]"[8]. A tale proposito, la Commissione aveva legittimi dubbi sulla corretta applicazione dei principi di proporzionalità e necessarietà nel caso di specie.

In questo panorama di evidente fragilità del regime del Safe Harbour e di preoccupazioni legate alla violazione dei diritti fondamentali della privacy e della protezione dei dati personali, nel luglio 2014, Maximilian Schrems, cittadino austriaco e utente di Facebook, presentò una denuncia al Commissario Irlandese per la Protezione Dati, autorità di controllo nazionale competente nell'esaminare reclami relativi a trattamenti effettuati all'interno dello Stato membro, contro Facebook Ireland chiedendo di interrompere il trasferimento dei suoi dati personali presso Facebook Inc., situata negli Stati Uniti.
Schrems sosteneva, alla luce delle recenti rivelazioni, che ai suoi dati personali non era garantito un livello di protezione adeguato.
L'autorità Irlandese rigettò la domanda per insufficienza di prove che potessero comprovare un nesso tra la violazione dei diritti dell'interessato e le misure di sorveglianza messe in atto dall'intelligence statunitense.
Schrems ha portato la causa dinanzi alla Corte d'Appello Irlandese contro il Commissario per la Protezione dei Dati, che ha accolto le argomentazioni di Schrems facendo in particolare leva sul principio di necessarietà e proporzionalità riconosciuti dalla Costituzione Irlandese, e presentando una

[7] Commissione europea, "sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite 2013" (Comunicazione) COM(2013) 847 final. 2013.
[8] Decisione di esecuzione (UE) 2000/520 allegato I.

domanda pregiudiziale alla Corte di Giustizia dell'UE vertente sull'interpretazione dell'art. 25 comma 6 della direttiva 95/46[9].[10]

In particolare, venne chiesto alla Corte se le autorità di protezione dei dati siano vincolate alla decisione della Commissione o se esse siano competenti per l'esercizio di poteri di indagine sulla validità delle disposizioni della decisione in seguito a sviluppi avvenuti posteriormente alla sua emanazione.

La Corte ha chiarito che una decisione di esecuzione non elimina o riduce i poteri di tali autorità, perciò gli interessati possono presentare un reclamo che verte sulla validità dell'atto della Commissione. Qualora l'autorità accerti che i motivi del reclamo siano fondati, *post* esercizio dei suoi poteri investigativi ai sensi dell'art. 28 della direttiva 95/46, deve promuovere un'azione giurisdizionale[11].

Successivamente, l'analisi della Corte si è spostata, sulla base delle richieste di Schrems, sulla validità della decisione 520/2000.

Come rilevato dalla Corte nell'analisi dell'art. 1 della decisione, il regime dell'Approdo Sicuro non prevedeva limitazioni o garanzie per quanto concerneva l'acquisizione e l'uso dei dati personali da parte di autorità pubbliche per fini di sicurezza nazionale, le quali avevano un accesso generalizzato ai dati detenuti dalle aziende private.

A ciò si aggiunge il fatto che i principi dell'accordo, come stabilito dall'allegato I, vincolavano le aziende private certificate ma non le autorità pubbliche statunitensi[12].

Inoltre, la decisione di esecuzione riconosceva esplicitamente un primato della legge statunitense, ergo, in caso di conflitto o incompatibilità dei principi di cui

[9]"*La Commissione può constatare […] che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona*"

[10] Causa C-362/14, *Data Protection Commissioner c Maximilian Schrems,* ECLI:EU:C:2015:650 para 26-36.

[11] ibid para 38-66.

[12] ibid para 82.

all’allegato I con la legge statunitense, “*le organizzazioni americane autocertificate che ricevono dati personali dall’Unione sono tenute a disapplicare senza limiti tali principi*”[13].

In aggiunta, la Corte ha individuato che l’ordinamento statunitense non prevedeva rimedi giurisdizionali o amministrativi effettivi agli interessati nell’Unione per tutelare i loro dati personali, in violazione dell’art. 47 della Carta[14].

Pertanto, questa possibilità di trattamento da parte delle autorità pubbliche in deroga ai principi, unitamente alla mancanza di un meccanismo di ricorso efficace a disposizione degli interessati nell’Unione, ha portato la Corte ad annullare la decisione di adeguatezza[15].

La Corte, al punto di valutare se gli Stati Uniti garantissero un livello di protezione adeguato, ha interpretato ed evoluto il concetto connesso al livello di protezione necessario da “adeguato” a “sostanzialmente equivalente”[16].

Si tratta di uno sviluppo che fornisce flessibilità al concetto, in quanto consente, nel riconoscimento di un livello di protezione adeguato di un paese terzo da parte della Commissione, di adattarsi a ordinamenti giuridici e sistemi politici differenti, all’interno dei quali vi possono essere interessi e bisogni diversi da quelli dell’Unione.

In concreto, la nuova metodologia di classificazione del livello di protezione garantito dal paese terzo richiede che “*gli strumenti dei quali tale paese terzo si avvale (…) per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all’interno dell’Unione*”[17].

[13] ibid para 86.
[14] ibid para 90.
[15] sulla base delle competenze attribuitegli dall’art. 267 TFUE
[16] ibid para 73.
[17] ibid 74.

Viene lasciata discrezionalità ai paesi terzi sulla scelta degli strumenti da adottare per garantire tale livello di protezione, fintantoché essi possano "*rivelarsi efficaci, nella prassi*" ad assicurare un livello di protezione adeguato[18]. Questo standard elaborato dalla Corte presuppone una "*protezione che deve essere comparabile a quella prevista nell'Unione dalla direttiva 95/46 letta alla luce della Carta*"[19].

Si tratta di uno sviluppo tendenzialmente positivo ma che potrebbe creare incertezze e complessità nello svolgimento della valutazione concreta.

Ad ogni modo, come ipotizzato da C. Kuner, "*la volontà della Corte sembra essere quella di evidenziare che il livello di protezione offerto dai paesi terzi deve essere elevato e avvicinarsi a quello previsto dall'ordinamento comunitario*"[20]. In tal caso, l'equivalenza di protezione nella sostanza potrebbe interpretarsi come una soglia minima necessaria di protezione per i diritti fondamentali degli interessati nell'UE.

Da tale sentenza emerge che l'adozione di decisioni di adeguatezza presuppone il rispetto di determinati criteri minimi per poter valutare concretamente come "sostanzialmente equivalente" il livello di protezione garantito nel paese terzo.

Il trattamento deve avere una base giuridica chiara, precisa e accessibile, gli obiettivi legittimi perseguiti devono essere conformi al principio di necessarietà e proporzionalità, deve essere istituito un organo di controllo indipendente e garantiti agli individui mezzi di ricorso effettivi, conformemente all'art. 47 della Carta[21].

---

[18] ibid.

[19] Laura Drechsler and Irene Kamara, 'Essential Equivalence as a Benchmark for International Data Transfers after Schrems II', *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 326 <https://www.elgaronline.com/edcollchap/edcoll/9781800371675/9781800371675.00022.xml>.

[20] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881-918, 902.

[21] EDPB Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza 2020 8–15.

L’applicazione di tali criteri alla sorveglianza attuata dalle autorità pubbliche presupporrebbe la presenza di una base giuridica precisa e di finalità ragionevoli esplicitate in modo chiaro e semplice, stabilendo la possibilità di limitazioni ai diritti degli individui e la loro portata. Un’applicazione concreta del principio di minimizzazione dei dati, affinché i dati raccolti siano limitati a quanto necessario per raggiungere una o più finalità specifiche perseguite dalla sorveglianza. Inoltre, dovrebbe essere garantito un meccanismo di controllo indipendente per la vigilanza dei programmi di sorveglianza. Infine, dovrebbe essere garantito agli individui l’accesso ad un meccanismo di ricorso efficace per tutelare i propri dati personali qualora presumano che il trattamento da parte delle autorità pubbliche non sia lecito[22].

2.2) Il Privacy Shield EU-US

L’invalidazione di un regime di tale importanza in ambito commerciale, economico e politico ha creato un clima di incertezza e stallo per le organizzazioni importatrici ed esportatrici di dati.

Le aziende statunitensi hanno continuato il trasferimento di dati dall’Unione sulla base legale delle clausole tipo di protezione dati, alternativa attuabile qualora le aziende non siano coinvolte nei programmi di sorveglianza statunitensi[23].

Repentinamente sono cominciati i negoziati USA-UE per trovare un sistema alternativo che soddisfi le questioni problematiche sollevate dalla Corte riguardo all’accordo. Nel frattempo i trasferimenti sarebbero continuati sulla base dell’art. 46 GDPR “*fino alla creazione di un “Approdo Sicuro più sicuro*””[24].

Nel febbraio 2016, gli Stati Uniti e l’UE hanno trovato un accordo per l’implementazione dello Scudo per la privacy (“Privacy Shield”), andando a colmare il vuoto lasciato dall’invalidazione del regime dell’Approdo sicuro.

[22] Jacques Bourgeois and others, ‘Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States’ 1-172, 3-4.
[23] Philipp E Fischer, ‘Getting Privacy to a New Safe Harbour: Comment on the CJEU Judgement of 6 October 2015, Schrems v. Data Protection Commissioner Case Comment’ (2015) 6 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 229-234, 230.
[24] ibid 231.

Nel luglio 2016, la Commissione ha emanato la decisione di esecuzione 1250/2016 con la quale determinava che gli USA garantivano un livello di protezione sostanzialmente equivalente a quello previso dal quadro normativo europeo[25].

Il 30 maggio 2016, l'EDPS ha espresso un'opinione[26] sul progetto del Privacy Shield, all'interno della quale notava le evoluzioni positive comparandolo al Safe Harbour, ma sottolineava l'insufficienza degli sviluppi. L'accordo poteva essere considerato una via di mezzo tra un accordo che soddisfaceva a pieno il livello di protezione richiesto e un regime simile al precedente: il Privacy Shield presentava un livello maggiore di protezione dei dati personali, derivante soprattutto dalle limitazioni e garanzie per i cittadini europei disposte dalla Direttiva Presidenziale 28 (PPD-28), ma non rispondeva pienamente ai requisiti evidenziati dalla Corte nella sentenza[27].

Nel Privacy Shield è possibile individuare all'allegato VI una sintesi delle informazioni fornite circa l'attività di intelligence statunitense, in particolare si concentra sulla PPD-28, sull'E.O. 12333, sulla legge relativa alla sorveglianza sull'intelligence straniera (FISA), su politiche di trasparenza intraprese dalla comunità di intelligence e sui mezzi di ricorso predisposti per la persona sottoposta a sorveglianza elettronica per finalità di sicurezza nazionale. Queste vengono integrate dalle dichiarazioni, contenute negli allegati della decisione, del *Department of Justice* e del *Director of National Intelligence*, che affermavano una limitazione e un controllo sul trattamento dei dati personali di interessati europei con riguardo alle attività delle autorità di intelligence. Nonostante ciò, si trattava di mere dichiarazioni prive di effetti vincolanti nei confronti di tali entità[28].

[25] 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. ELI: http://data.europa.eu/eli/dec_impl/2016/1250/oj (OJ L).
[26] EDPS Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision 2016.
[27] Fabien Terpan, 'EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?' (2019) 2018 3 European Papers 1045, 1050–1051.
[28] ibid 1051.

Inoltre, l'allegato III prevedeva un meccanismo di mediazione indipendente dalla comunità di intelligence ("*Privacy Shield Ombudsperson*") per trattare i reclami di cittadini e residenti dell'UE come soluzione alla questione sollevata dalla Corte nella sentenza *Schrems I* sulla mancanza di un meccanismo effettivo di reclamo per i cittadini europei, garantito dall'art. 47 della Carta[29].

2.3) Schrems II: l'invalidazione del Privacy Shield

A posteriori dell'invalidazione della decisione 2000/520, il giudice del rinvio ha annullato il rigetto della denuncia di Schrems da parte del Commissario, rinviandogli la denuncia precedentemente respinta[30]. Nel maggio 2016, sulla base delle conclusioni delle sue indagini, il Commissario ha considerato che il trasferimento di dati personali di Schrems avvenuto tramite clausole tipo di protezione dati sulla base della decisione CPT fosse ingiustificato, invitandolo a riformulare la denuncia[31].

Poiché la denuncia riformulata andava a porre in questione la validità della stessa decisione, il Commissario ha adito la High Court Irlandese[32].

Il giudice del rinvio ha rilevato ulteriori questioni sull'invalidità della decisione. In particolare, ha constatato che gli Stati Uniti non garantivano un livello di protezione sostanzialmente equivalente a quello dell'ordinamento europeo per via dell'accesso sproporzionato da parte delle autorità pubbliche ai dati dei cittadini europei, in violazione degli artt. 7 e 8 della Carta. Inoltre, ha individuando ostacoli nell'accesso ai mezzi di ricorso a disposizione degli individui, in violazione dell'articolo 47 della Carta[33].

Per tali motivi, la High Court ha sospeso il procedimento e presentato 11 questioni pregiudiziali alla Corte di Giustizia dell'UE riguardanti principalmente

[29] Decisione di esecuzione (UE) 2016/1250.
[30] Causa C-311/18, *Data Protection Commissioner c Facebook Ireland Limited e Maximillian Schrems* ECLI:EU:C:2020:559 para 54.
[31] ibid 55–56.
[32] ibid 57–58.
[33] ibid 64–65.

l'interpretazione e la validità della decisione CPT anche in relazione al Privacy Shield[34].[35]

A fini di coerenza con lo scopo del presente elaborato è necessario trattare la prima questione pregiudiziale affrontata in giudizio. La domanda verteva sull'applicazione del diritto UE, in particolare del GDPR, al trattamento di dati da parte di autorità pubbliche per finalità di sicurezza nazionale avvenuto successivamente ad un trasferimento per scopi commerciali dei dati personali presso uno stato terzo[36].

L'art. 4 co. 2 TUE stabilisce che l'UE "*rispetta le funzioni essenziali dello Stato, in particolare le funzioni di […] tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro*", escludendo qualsiasi competenza dell'Unione nell'ambito della sicurezza nazionale.

Tuttavia, le disposizioni di tale articolo si applicano ad attività di intelligence svolte in via diretta, non all'attuazione di attività di accesso ai dati precedentemente acquisiti dalle organizzazioni (in questo caso da aziende statunitensi certificate) ai sensi del diritto UE[37].

Difatti la Corte interpretava e chiariva tali incertezze sull'ambito di applicazione del GDPR[38] facendo rientrare al suo interno il trasferimento internazionale di dati a fini commerciali di un esportatore verso un importatore ubicato nel paese terzo qualora tali dati abbiano la possibilità di essere trattati "*a fini di pubblica sicurezza, di difesa e di sicurezza dello Stato da parte delle autorità del paese terzo*" [39].

---

[34] ibid 68.
[35] ibid 77,79. La Corte ha affermato che, "*sebbene le questioni pregiudiziali facciano riferimento alla direttiva 95/46, […] occorre rispondere [alle questioni pregiudiziali] alla luce delle disposizioni del GDPR*"
[36] ibid 68 1).
[37] Christopher Docksey and Kenneth Propp, 'Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective' (2023) 10 Oslo Law Review 1, 6.
[38] *Causa C-311/18* (n 29) para 89.
[39] ibid 86.

Ciò implica che gli operatori economici sono responsabili nell'assicurare un livello di protezione adeguato agli interessati nell'Unione, e allo stesso tempo che le attività di trattamento dei dati di autorità operanti nel campo della sicurezza nazionale rientrano nell'ambito di applicazione del GDPR [40]

In dottrina, C. Kuner specifica che "*l'ambito di applicazione territoriale della Carta equivale a quello del diritto UE*". Perciò, ogniqualvolta il GDPR trova applicazione in scenari che riguardano il trasferimento di dati presso un paese terzo, comprese le attività di intelligence, gli individui nell'UE godono della protezione offerta dalla Carta[41].

Con lo scopo di affrontare le altre diverse questioni che andavano a porsi sulla validità del Privacy Shield, la Corte ha ritenuto opportuno esaminare la decisione della Commissione con riguardo alla conformità dei requisiti enunciati dal GDPR, letto alla luce della Carta[42].

Rilevava, al pari del regime dell'Approdo sicuro, un primato delle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia sui principi elencati all'allegato II.I.5 della decisione, permettendo alle aziende certificate statunitensi di disapplicarli qualora fossero incompatibili con tali esigenze[43]. Ciò rendeva possibile un'ingerenza e utilizzo da parte di autorità pubbliche statunitensi di dati personali nell'attuazione di programmi di sorveglianza di massa[44].

Nella valutazione della Commissione che gli Stati Uniti garantivano un livello di protezione sostanzialmente equivalente a quella offerta dal diritto UE, la Commissione ha constatato, "*in base alle informazioni sull'ordinamento*

[40] Kristina Irion, 'Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law' (*European Law Blog*, 24 July 2020) <https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/>.
[41] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (n 19) 896.
[42] *Causa C-311/18* (n 29) para 161.
[43] ibid 164.
[44] ibid 165.

giuridico statunitense disponibili"[45], che tali ingerenze, effettuate qualora fossero disapplicati i principi dell'accordo, erano limitate allo stretto necessario per conseguire un obiettivo legittimo e che a tutela di tali ingerenze esisteva un meccanismo di ricorso efficace a disposizione degli individui[46].

La Corte, al contrario, ha sancito che l'articolo 702 FISA e l'E.O. 12333, in combinato disposto con la PPD-28, non garantivano un livello di protezione adeguato in quanto contrastanti con il requisito di proporzionalità[47].

In relazione ai diritti fondamentali, il principio di proporzionalità è riconosciuto dall'art. 52 co. 1 della Carta[48]. Esso stabilisce la possibilità di limitare i diritti e le libertà previsti dalla stessa nel rispetto del principio di legalità (necessaria una base legale) e di proporzionalità. Per proporzionalità si intende una necessarietà della restrizione, quindi la mancanza di alternative o di alternative meno incisive, unitamente al perseguimento di finalità di interesse generale perseguite dall'UE o per proteggere diritti e libertà altrui[49].

Nel caso di specie, si era verificata un'intrusione sproporzionata e non limitata allo stretto necessario al diritto fondamentale degli individui alla privacy e alla protezione dei dati personali rispettivamente riconosciuti all'art. 7 e 8 della Carta.

Altro requisito minimo per constatare come sostanzialmente equivalente il livello di protezione del Paese terzo è la presenza di "*mezzi di ricorso effettivi in sede amministrativa e giudiziaria*"[50].

---

[45] v. punto 67-135 della decisione

[46] *Causa C-311/18* (n 29) para 167.

[47] ibid 184.

[48] Art. 52(1) Carta "*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*"

[49] V. C-291/12 *Michael Schwarz c. Stadt Bochum* ECLI:EU:C:2013:670. Nel rinvio pregiudiziale la Corte applica il principio di proporzionalità a limitazioni poste sui diritti fondamentali riconosciuti all'art. 7 e 8 della Carta.

[50] *Causa C-311/18* (n 29) para 188.

A tal riguardo, la Corte ha notato come il *Privacy Shield Ombudsperson* non soddisfaceva con sufficienza tale garanzia: essendo "*designato dal Secretary of State*" [51] e sfornito della capacità di adottare decisioni vincolanti nei confronti dei servizi di intelligence ("*insufficienza di poteri effettivi*", evidenziata anche dal Parlamento europeo[52]) è stata messa in dubbio la sua indipendenza ed imparzialità, andando a violare i requisiti previsti dall'art. 47 della Carta[53].
Tale figura del mediatore può essere considerata un "*tentativo degli Stati Uniti di risolvere con astuzia l'obbligo di ricorso giudiziario*"[54], rispondendo in modo insufficiente alle questioni sollevate dalla Corte e prevedendo un metodo non realmente protettivo dei diritti fondamentali degli individui.
Per tali ragioni, la sentenza si è conclusa constatando la validità della decisione CPT relativa alle clausole contrattuali tipo per il trasferimento internazionale di dati, e determinando l'invalidità della decisione 1250/2016 riguardante il regime del Privacy Shield.

2.4) Prospettive per il nuovo accordo

Come puntualizzato in dottrina da C. Kuner, può essere interessante notare come tra le due sentenze siano emerse questioni simili, ovvero un'intrusione sproporzionata ai dati personali degli interessati nell'Unione e una mancanza di rimedi giurisdizionali o amministrativi effettivi a loro disposizione. Ciò fa pensare che la Commissione sia schiacciata, da una parte, dalla pressione politica da parte degli Stati Uniti derivante prevalentemente da interessi commerciali, e dall'altra dalla Corte che richiede una certa rigidità nel rispetto del diritto alla protezione dei dati personali. Questo metterebbe in dubbio l'imparzialità e la correttezza delle procedure che portano la Commissione ad adottare una

[51] ibid 195.
[52] Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy (2018/2645(RSP)) para 7.
[53] *Causa C-311/18* (n 29) para 196.
[54] Kenneth Propp and Peter Swire, 'After Schrems II: A Proposal to Meet the Individual Redress Challenge'. Lawfare <https://www.lawfaremedia.org/article/after-schrems-ii-proposal-meet-individual-redress-challenge>.

decisione ai sensi dell’art. 45 GDPR[55]. Per tali motivi, sarebbe opportuno una maggior trasparenza, dato che i negoziati per il Privacy Shield sono stati segreti e c’è stata pressione politica per estrapolare rapidamente una decisione[56].

In questa situazione, un terzo accordo con minimi cambiamenti rispetto ai precedenti non sarebbe credibile[57] e “*non è più possibile pretendere che un livello adeguato di protezione dati possa essere raggiunto a livello globale solo per mezzo di misure formali*”[58]. Infatti, i “*meccanismi procedurali possono soddisfare i requisiti formali del diritto alla protezione dei dati, ma non sono in grado di garantire una protezione contro la sorveglianza da parte dell’intelligence*”[59].

Nel frattempo, l’invalidazione della decisione 1250/2016 ha riportato il trasferimento dei dati UE-USA sulla base di clausole tipo per la protezione di dati regolate dalla decisione CPT di cui la Corte ha dichiarato la validità. Sebbene siano considerate uno strumento adeguato, la Corte le ha ritenute inadeguate in un contesto in cui le autorità pubbliche del paese terzo possano, in conformità con la loro legislazione in materia, accedere e utilizzare tali dati[60]. In tal caso, qualora l’esportatore non sia in grado di fornire misure supplementari volte ad assicurare un’adeguata protezione dei dati, il trasferimento non può avvenire.

---

[55] Christopher Kuner, ‘The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation’ (*European Law Blog*, 17 July 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>.
[56] Kuner, ‘Reality and Illusion in EU Data Transfer Regulation Post Schrems’ (n 19) 903.
[57] Kuner, ‘The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation’ (n 54).
[58] Kuner, ‘Reality and Illusion in EU Data Transfer Regulation Post Schrems’ (n 19) 918.
[59] ibid 885.
[60] *Causa C-311/18* (n 29) para 126.

3) Il nuovo Data Privacy Framework EU-US

3.1) Contenuti dell'accordo

Il 10 luglio 2023 la Commissione ha emesso una decisione di esecuzione che istituisce il regime del Data Privacy Framework (DPF), riconoscendo che gli Stati Uniti garantiscono un livello di protezione sostanzialmente equivalente a quello garantito nell'ordinamento europeo.

Questo nuovo meccanismo ha lo scopo di risolvere le questioni controverse sollevate dalla Corte che hanno portato all'invalidazione dei precedenti accordi, in modo da creare un quadro stabile per il flusso transatlantico di dati.

Come per gli accordi precedenti, è caratterizzato dal medesimo approccio "*volontario ma vincolante*"[61]. Le organizzazioni statunitensi possono aderire su base volontaria ai principi stabiliti dal *Department of Commerce* (DoC) all'allegato I, sottoponendosi ai poteri di vigilanza e di esecuzione della *Federal Trade Commission* (FTC) o del *Department of Transportation* (DoT). Le aziende, per continuare a ricevere i dati personali dall'UE, devono ricertificarsi annualmente[62].

I principi prevedono una specificazione delle finalità e un diritto di opporsi al trattamento da parte dell'interessato qualora gli venga richiesto il trattamento dei suoi dati per una diversa finalità (*Choice Principle*)[63]. Vengono descritti i principi di esattezza, minimizzazione, sicurezza dei dati[64] e trasparenza[65].

Gli interessati godono di un diritto di accesso che è strumentale all'esercizio di altri diritti, come la modifica o la rettifica di dati inesatti[66]. Sono poste limitazioni

[61] Docksey and Propp (n 36) 9.
[62] Decisione di esecuzione (UE) 2023/1795 della Commissione del 10 luglio 2023 a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali. ELI: http://data.europa.eu/eli/dec_impl/2023/1795/oj para 9.
[63] ibid 13-15
[64] ibid 20-24
[65] ibid 25-28
[66] ibid 29-36

al trasferimento successivo, che deve garantire un livello di protezione pari a quello garantito dai principi[67].

Infine viene previsto il principio di responsabilizzazione[68], che ha le potenzialità per costituire un istituto chiave per garantire maggior controllo e protezione ai dati personali da intrusioni di autorità pubbliche. Infatti, l'impegno delle organizzazioni certificate a dover dimostrare la conformità ai principi presuppone la predisposizione di misure tecnico-organizzative[69] che sono accessibili, in determinate circostanze, da autorità di controllo competenti, permettendo loro di monitorare il trattamento di dati da parte di enti di intelligence e constatarne l'eventuale illiceità.

Tali principi possono essere limitati per "*per soddisfare esigenze di interesse pubblico, di contrasto o di sicurezza nazionale, anche nel caso in cui le disposizioni legislative o regolamentari creino obblighi contrastanti*"[70]. Permane perciò un primato della legge statunitense sui principi, come previsto dal Privacy Shield. A tal riguardo la Corte aveva ritenuto che questa deroga, letta unitamente alle insufficienti garanzie fornite dalla legislazione statunitense, non forniva una protezione adeguata ai diritti degli interessati nell'Unione.

La stabilità dell'accordo sarà determinata perciò dalle riforme apportate al DPF per (3.2) garantire la proporzionalità delle attività di accesso e trattamento dei dati da parte delle autorità pubbliche, in particolare per finalità di sicurezza nazionale, e (3.3) l'istituzione di meccanismi di ricorso efficaci a protezione degli individui.

---

[67] ibid 37-43

[68] ibid 44-46.

[69] ibid 44.

[70] ibid allegato I.

3.2) Necessarietà e proporzionalità dell'accesso e uso da parte delle autorità pubbliche statunitensi

3.2.1) Accesso e uso da parte di autorità pubbliche per motivi di sicurezza nazionale

Nell'atto di esecuzione, la Commissione ha valutato che le riforme dell'ordinamento statunitense permettono di constatare che gli Stati Uniti offrono un livello di protezione sui dati sostanzialmente equivalente a quello garantito dal diritto UE[71].

Le autorità pubbliche possono raccogliere e trattare dati personali dalle organizzazioni certificate per finalità di sicurezza nazionale qualora ciò sia consentito dalle leggi in vigore[72]. Rilevano specialmente la FISA ("Foreign Intelligence Surveillance Act") e il decreto presidenziale ("Executive Order") 12333, presenti anche nei precedenti accordi e integrate dal nuovo decreto presidenziale 14086 che va ad abrogare parzialmente la PPD-28.

3.2.1.1) La Foreign Intelligence Surveillance Act e l'E.O. 12333

La FISA è stata emanata nel 1978 dal Congresso degli Stati Uniti come rimedio alle violazioni del diritto alla privacy di individui statunitensi da parte del governo nel perseguire esigenze di sicurezza nazionale[73].

Si tratta di uno strumento utile ad assicurare la sicurezza nazionale, in particolare per combattere il terrorismo o per acquisire informazioni su intelligence straniera, garantendo allo stesso tempo il rispetto delle libertà civili[74] degli individui statunitensi[75].

Oltre a perseguire interessi nazionali, il governo statunitense ritiene che le informazioni acquisite dall'art. 702 del FISA soddisfino interessi pubblici

[71] ibid 119.
[72] ibid 120–121.
[73] James G. McAdams, III, 'Foreign Intelligence Surveillance Act (FISA): An Overview' 11, 1.
[74] Per libertà civili intendiamo i diritti fondamentali riconosciuti agli individui che vengono protetti nei confronti di autorità pubbliche
[75] Nicholas J Whilt, 'The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties That Make Defense of Our Nation Worthwhile' (2006) 35 Southwestern University Law Review 361, 361–362.

dell'UE[76], e afferma che esse vengano condivise con gli Stati Membri per collaborare al contrasto di minacce estere[77].

Nella valutazione delle garanzie offerte da questa legge, la Commissione ha stabilito che la raccolta di dati personali, trasferiti ad un'organizzazione statunitense certificata, da parte dell'intelligence dei segnali (cioè "la raccolta di comunicazioni elettroniche e dati da sistemi informatici"[78]) è soggetta a limitazioni e garanzie disciplinate dall'art. 702 del FISA[79].

La legge stabilisce che, a seguito dell'emissione di un ordine della corte competente o, in situazioni di necessità e urgenza determinate dall'*Attorney General* e il *Director of National Intelligence*, "*l'Attorney General e il Director of National Intelligence possono autorizzare congiuntamente […] il targeting di persone ragionevolmente ritenute situate al di fuori degli Stati Uniti per acquisire informazioni di intelligence straniera*"[80].

La FISA consente quattro diverse tipologie di raccolta: (i) l'acquisizione di comunicazioni via cavo o via radio inviate o ricevute da una persona statunitense, (ii) l'acquisizione via cavo di informazioni situate all'interno degli Stati Uniti, (iii) l'acquisizione via radio di comunicazioni che avvengo all'interno degli Stati Uniti, indifferentemente dal fatto che la persona abbia o meno un'aspettativa ragionevole alla privacy[81] e (iv) l'acquisizione negli Stati Uniti, tramite un dispositivo per le intercettazioni, che avrebbe invece richiesto un decreto autorizzativo[82].

Tali attività di sorveglianza devono essere condotte nel rispetto delle procedure di targeting e di minimizzazione[83]. Le procedure di targeting sono misure

---

[76] US Government - White Paper, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II 2020 2.
[77] ibid 4.
[78] Decisione di esecuzione (UE) 2023/1795 para 142.
[79] ibid.
[80] Codice degli Stati Uniti, titolo 50, articolo 1881a lettera a).
[81] v. *Katz vs USA, 1967*; La legge stabilisce che per le persone situate extra USA non si applica il principio costituzionale del "*reasonable expectation of privacy*", elaborato dalla Corte Suprema degli Stati Uniti per delimitare la portata di applicazione del quarto emendamento
[82] Mark M Jaycox, 'No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333' (2021) 12 Harvard National Security Journal 58, 71–72.
[83] Codice degli Stati Uniti, titolo 50, articolo 1881a lettera c).

progettate per assicurare che l'acquisizione sia limitata a bersagli non ubicati negli Stati Uniti, mentre le procedure di minimizzazione riguardano la limitazione dell'acquisizione e conservazione di informazioni riguardanti cittadini statunitensi.

Non essendo espressamente previsto da atti normativi che gli effetti di tali procedure si estendano a cittadini europei, si può dedurre come tali garanzie siano predisposte solo per i cittadini statunitensi.

Inoltre la legge richiede la conformità con il quarto emendamento della Costituzione statunitense. Tuttavia, tale previsione protegge esclusivamente i cittadini statunitensi nei confronti di autorità pubbliche, non tutelando individui non residenti negli Stati Uniti[84]. Questo principio è stato applicato nel caso *United States v Verdugo-Urquidez*, nel quale viene esclusa l'applicazione del quarto emendamento per attività svolte da ufficiali statunitensi in un paese estero, a meno che la parte sorvegliata non presenti un "*collegamento con gli Stati Uniti*"[85].

L'intelligence è soggetta al controllo della FISC (Corte FISA)[86], un organo giurisdizionale che approva e supervisiona le attività di intelligence attuate ai sensi dell'art. 702 della FISA[87]. In particolare, è competente nel verificare la conformità della certificazione con i requisiti elencati[88], incluse le procedure di targeting e minimizzazione.

L'esame delle procedure di targeting non si limita alla mera disposizione scritta presentata nella certificazione, ma analizza l'implementazione nella pratica di

[84] Susan Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations' (2013) 11 IEEE Security & Privacy 54, 58.
[85] Stewart Young, 'Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases' (2003) 10 Michigan Telecommunications & Technology Law Review 139, 154.
[86] Decisione di esecuzione (UE) 2023/1795 para 142.
[87] US Government - White Paper, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II 6.
[88] Codice degli Stati Uniti, titolo 50, articolo 1881a lettera h).

tali procedure. In caso riscontri irregolarità, ha il potere di bloccare l'acquisizione o di emettere azioni correttive con effetti vincolanti[89].

Ogni anno l'*Attorney General* e il *Director of National Intelligence* presentano alla FISC le categorie di informazioni di intelligence estera acquisite[90]. Ciò soddisfa il principio di accountability e permette un controllo di conformità sulle attività svolte.

La sua capacità di evitare acquisizioni di dati sproporzionate può essere contestata considerando che, come stabilito dall'Avvocato Generale nella causa *Schrems II*, "*non autorizza singole misure di sorveglianza, ma piuttosto programmi di sorveglianza (...) basandosi sulle certificazioni annuali*"[91]. Infatti, questo si è concretizzato nell'approvazione in passato di programmi di sorveglianza di massa come PRISM[92].

Inoltre, essa non approva i singoli selettori, di conseguenza il controllo *ex ante* verte solo sulle categorie di informazioni acquisite e non verifica se i potenziali obiettivi (individui non statunitensi) siano dei bersagli appropriati[93].

Mentre la FISA permette l'accesso e uso di dati personali situati in territorio statunitense, l'E.O. 12333 consente lo svolgimento di attività di intelligence al di fuori dei confini USA, compresa l'attività di raccolta di dati in transito tra Europa e Stati Uniti[94], specialmente per acquisire informazioni di persone non statunitensi[95].

L'E.O. 12333 permette di svolgere attività di intelligence per raccogliere informazioni importanti per "*lo sviluppo e la conduzione di politiche di difesa ed*

---

[89] US Government - White Paper, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II 9.
[90] Decisione di esecuzione (UE) 2023/1795 para 142.
[91] Causa C-311/18, *Conclusioni dell'avvocato generale Henrik Saugmandsgaard Øe, Data Protection Commissioner c Facebook Ireland Limited, Maximillian Schrems* ECLI:EU:C:2019:1145 para 298.
[92] Michele Nino, 'La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo' [2020] Diritti umani e diritto internazionale 733, 749.
[93] *Causa C-311/18, Conclusioni dell'avvocato generale* (n 90) para 298.
[94] Decisione di esecuzione (UE) 2023/1795 para 122.
[95] Jaycox (n 81) 75.

economiche, e per la protezione di interessi pubblici degli Stati Uniti da minacce estere alla sicurezza”[96]; dando particolare attenzione al “*contrasto di minacce e attività di potenze estere o dei loro servizi di intelligence contro gli USA e i loro interessi […], minacce terroristiche […], minacce legate a sviluppo, possesso o uso di armi di distruzione di massa*”[97].

L’E.O. 12333, oltre a una raccolta mirata delle informazioni, permette una “raccolta in blocco” (*bulk data collection*)[98] di dati al di fuori degli Stati Uniti, per il raggiungimento di specifiche finalità[99]. Di conseguenza, non tutte le informazioni raccolte sono utili al raggiungimento degli obiettivi di intelligence[100]. L’utilizzo di selettori, come l’indirizzo IP di una persona, permette di concentrare l’attività di *data collection* solo sulle persone-obiettivo, mentre la c.d. *bulk collection* presuppone un’acquisizione di numerose informazioni che vengono filtrate e analizzate solo successivamente alla loro memorizzazione[101].

Il decreto presidenziale viene messo in discussione per le insufficienti limitazioni ai metodi di acquisizione previsti[102], compromettendo il principio di proporzionalità stabilito dalla Carta. Infatti, la capacità da parte dell’intelligence di trattare dati personali nell’attuazione di programmi di sorveglianza su larga scala non va a limitare il trattamento dei dati personali al minimo necessario per perseguire esigenze di sicurezza nazionale, andando a violare l’art. 7 e 8 della Carta.

Questa acquisizione di massa viene limitata dall’E.O. 14086, che favorisce una raccolta mirata[103] e cerca di conformarsi al requisito di proporzionalità richiamato dalla Corte.

[96] Executive Order 12333 - United States Intelligence Activities.
[97] ibid.
[98] Per raccolta in blocco si intende l’acquisizione o la disseminazione di grandi volumi di dati che avviene senza l’utilizzo di discriminanti (come identificatori o selettori).
[99] Decisione di esecuzione (UE) 2023/1795 para 141.
[100] ‘Department of Homeland Security, Office of Intelligence and Analysis - Intelligence Oversight Program and Guidelines’ glossary-1.
[101] Jaycox (n 81) 67–68.
[102] ibid 85.
[103] Decisione di esecuzione (UE) 2023/1795 para 141.

3.2.1.2) Dalla PPD-28 all'E.O. 14086: una soluzione?

Nell'ottobre 2022, il presidente degli Stati Uniti J. Biden ha firmato l'E.O. 14086[104] che va a sostituire quasi integralmente la PPD-28, integrato da un regolamento che istituisce il "*Data Protection Review Court*" (DPRC).

Il decreto presidenziale integra la FISA e l'E.O. 12333, potenziando le limitazioni e le garanzie offerte nello svolgimento di attività di intelligence dei segnali[105].

Essendo la FISA e l'E.O. 12333 invariati rispetto ai precedenti accordi, l'E.O. 14086 è l'unico strumento normativo che introduce cambiamenti nel campo della sicurezza nazionale. Pertanto, la stabilità dell'accordo dipende fondamentalmente dalla capacità del decreto presidenziale di conformare le attività di intelligence ai requisiti essenziali stabiliti dalla Corte[106].

La prima garanzia essenziale è la presenza di norme chiare, precise e accessibili sul trattamento che siano giuridicamente vincolanti. Qualsiasi limitazione ai diritti degli individui e la sua portata deve essere prevista dalla legge[107].

A riguardo, viene stipulato un elenco di dodici obiettivi legittimi per la raccolta e quattro obiettivi proibiti[108].

Come evidenziato dall'EDPB, gli obiettivi sono piuttosto generici, e la mancanza di chiarezza e precisione rischia di espandere ingiustificatamente la portata delle azioni di intelligence[109]. Generalmente si può definire come un elenco che contempla ogni motivo per il quale si potrebbe svolgere attività di intelligence[110].

---

[104] Executive Order 14086 - Enhancing Safeguards for United States Signals Intelligence Activities.
[105] L'E.O. 14086 non fornisce una definizione di "intelligence dei segnali". Si tratta di "*attività di intelligence su segnali elettronici e sistemi utilizzati da obiettivi stranieri, come sistemi di comunicazione, radar o bellici*" Fonte: https://www.nsa.gov/Signals-Intelligence/Overview/
[106] nella Sentenza Schrems I (C-311/18) ed elaborati successivamente dall'EDPB nel parere 2/2020
[107] EDPB Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza para 26,27,29.
[108] E.O. 14086 - art. 2 b) i).
[109] EDPB 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 2023 para 115.
[110] Andrej Savin, 'EU-US Data Privacy Framework – The New Framework for Transatlantic Data Transfers' (2023) 12 Journal of European Consumer and Market Law 159, 161.

Nel DPF è stabilito che tali obiettivi non possono essere utilizzati per giustificare le attività 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*". Ciò significa che la raccolta può avvenire esclusivamente per "*far progredire una priorità più specifica*"[111].

Tali priorità, elaborate dal *Director of National Intelligence*, sono preventivamente soggette ad una procedura di convalida basata su tre criteri di cui il *Civil Liberties Protection Officer* (CLPO)[112] è competente. Viene esaminato se perseguono uno o più obiettivi legittimi, se non siano previste per una raccolta di informazioni per uno degli obiettivi proibiti e se rispettino la vita privata e le libertà civili delle persone, inclusi individui non statunitensi. Dopo aver ottenuto la convalida, ogni priorità viene approvata dal Presidente[113].

Il Presidente degli Stati Uniti ha il potere di autorizzare nuovi obiettivi per urgenti esigenze di sicurezza nazionale. In tal caso, non ha l'obbligo di renderli pubblici qualora ciò possa costituire un rischio per la sicurezza nazionale[114], né ha un obbligo di informare l'UE[115].

Ad ogni modo, questa previsione assicura una certa flessibilità agli obiettivi, infatti lo sviluppo tecnologico potrebbe portare a rischi imprevedibili e immediati mettendo a repentaglio la sicurezza nazionale[116].

Nella sentenza *Schrems II*, il quadro legislativo statunitense per le attività di intelligence viene ritenuto non conforme al principio di proporzionalità definito all'art. 52 della Carta.

---

[111] Decisione di esecuzione (UE) 2023/1795 para 135.

[112] "*All'interno della comunità dell'intelligence, [il CLPO] ha il compito […] di garantire che la tutela delle libertà civili e della vita privata sia adeguatamente integrata nelle politiche e procedure dell'Ufficio del direttore dell'intelligence nazionale e degli enti di intelligence; di vigilare sul rispetto dei requisiti applicabili in materia di libertà civili e tutela della vita privata e di svolgere valutazioni dell'impatto sulla vita privata*" - Decisione di esecuzione (UE) 2023/1795 para 179

[113] E.O. 14086 - art. 2 b) iii).

[114] ibid art. 2 b) i) B).

[115] Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy (2018/2645(RSP)) para 3.

[116] Alex Joel, 'Necessity, Proportionality, and Executive Order 14086' [2023] Joint PIJIP/TLS Research Paper Series 1, 8.

Il decreto presidenziale introduce esplicitamente i concetti di necessarietà e proporzionalità, perseguendo un'equivalenza con l'ordinamento europeo.
Tra i principi prevede che le "*attività dell'intelligence dei segnali devono essere condotte nella misura e in modo proporzionale alle priorità convalidate di intelligence […] con l'obiettivo di compiere un giusto bilanciamento tra le priorità […] e l'impatto sulla privacy e sulle libertà civili delle persone […]"*[117].
La proporzionalità viene perseguita prendendo in considerazione ed adottando, nella raccolta di informazioni, le misure meno intrusive possibili nei diritti degli individui necessarie per perseguire la priorità convalidata. Queste misure non devono "*avere un impatto sproporzionato sulla privacy e le libertà civili"* tenendo conto di diversi fattori e circostanze, per esempio l'obiettivo perseguito o la tipologia di dati[118].
Il rispetto della proporzionalità viene messo in dubbio principalmente dai programmi di sorveglianza di massa.
La Corte, nella sentenza *Schrems II*, ha stabilito che la raccolta in blocco prevista dall'E.O. 12333, in combinato disposto con la PPD-28, non sia "*limitata allo stretto necessario*"[119]. Ciò significa, come rilevato dall'EDPB, che la Corte non dichiara illegittima la raccolta in blocco di informazioni, ma richiede che la sua portata sia limitata[120].
L'E.O. 14086 privilegia la raccolta mirata, consentendo comunque la "*bulk collection*" di dati ai sensi dell'E.O. 12333 esclusivamente come *extrema ratio*, ovvero qualora la raccolta non possa avvenire con metodi meno invasivi[121].
La Commissione ha riconosciuto che la raccolta in blocco di informazioni praticata dall'intelligence statunitense risponde al requisito di necessarietà e proporzionalità. Infatti, gli Stati Uniti si dimostrano propensi a preferire una raccolta mirata, attuando attività di raccolta in blocco solo qualora sia

[117] E.O. 14086 - art. 2 c) i) A).
[118] ibid art. 2 c) i) B).
[119] *Causa C-311/18* (n 29) para 185.
[120] EDPB Parere 5/2023 para 134.
[121] Decisione di esecuzione (UE) 2023/1795 para 141.

strettamente necessario, cioè quando l'acquisizione non possa ragionevolmente compiersi con altri mezzi, e svolgendola in maniera proporzionale agli obiettivi perseguiti[122].

Per queste attività di intelligence sono previsti sei obiettivi legittimi diversi da quelli sopramenzionati, considerati dall'EDPB come "*più dettagliati rispetto a quelli previsti dalla precedente PPD-28*". Nonostante ciò, "*la portata di tali possibilità di raccolta rimane potenzialmente ampia, ossia comprende grandi volumi di dati*"[123]. Inoltre, per questa tipologia di raccolta, non è istituita una procedura di convalida preventiva delle priorità, differentemente dalla raccolta mirata[124].

3.2.2) Accesso e uso da parte di autorità pubbliche per motivi di contrasto penale

Per esigenze di contrasto penale, scenario che rende possibile una limitazione dei principi dell'accordo, gli Stati Uniti sottolineano che si applicano le medesime procedure per tutte le organizzazioni statunitensi, certificate o meno[125].

In tal caso, è necessario verificare che le salvaguardie previste dalla legislazione statunitense offrano una protezione adeguata alle persone, indifferentemente dalla cittadinanza. Pertanto, la protezione riconosciuta ad un cittadino statunitense dovrebbe essere conforme ai principi enucleati nella Carta di Nizza.

Sono previste diverse procedure che permettono l'accesso alle informazioni detenute dalle aziende statunitensi.

In primo luogo, è possibile procedere al sequestro o alla perquisizione previo mandato del giudice, che viene emesso qualora sussista un "motivo plausibile"

[122] Docksey and Propp (n 36).
[123] EDPB Parere 5/2023 para 140.
[124] Savin (n 108) 161.
[125] Decisione di esecuzione (UE) 2023/1795 para 91.

che in determinato luogo siano presenti cose pertinenti al reato, incluse le informazioni contenute su un supporto elettronico[126].

Per reati gravi, cioè per reati che comportano una pena capitale o che siano infamanti, è possibile richiedere alla *grand jury*[127] (ramo del tribunale dotato di poteri investigativi[128]) una *subpoena* che concede l'accesso anche a informazioni conservate su supporto elettronico. La portata di accesso alle informazioni non deve essere eccessivamente ampia, e deve riguardare solo dati pertinenti alle indagini[129].

Inoltre, diverse basi giuridiche consentono di accedere ai dati relativi alle comunicazioni.

Il giudice può consentire l'intercettazione di dati, che non riguardano contenuti comunicativi[130], trasmessi via posta elettronica o telefono, a condizione che le informazioni siano pertinenti e previa indicazione del soggetto intercettato[131].

L'accesso a dati, anche di contenuto, in possesso di prestatori di servizi internet, telefonici o telematici può trovare fondamento nella legge sulle comunicazioni archiviate (Stored Communications Act)[132].

Infine, il giudice può predisporre l'intercettazione di qualsiasi comunicazione in tempo reale a condizione sussistano "*motivi plausibili per ritenere che l'intercettazione via cavo o elettronica fornirà la prova di un reato federale o del luogo in cui si trova un latitante*"[133].

L'EDPB riconosce che "*la richiesta di accesso per finalità di contrasto può essere considerata […] un obiettivo legittimo*"[134], e allo stesso tempo rileva che

---

[126] ibid 92.
[127] U.S. Constitution - Fifth Amendment "*No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury*"
[128] Decisione di esecuzione (UE) 2023/1795 allegato VI.
[129] ibid 93.
[130] ai sensi del "18 U.S. Code § 2510 - Definitions", il contenuto di una comunicazione elettronica include ogni informazione riguardante la sostanza, il significato o il proposito della comunicazione ("*substance, purport, or meaning of that communication*")
[131] Decisione di esecuzione (UE) 2023/1795 para 95.
[132] ibid 96.
[133] ibid 98.
[134] EDPB Parere 5/2023 para 83.

il sistema previsto dalla legislazione statunitense risponde ai requisiti di necessarietà e proporzionalità[135].

D'altro canto sottolinea che, sebbene la maggioranza delle procedure lo presuppone, non tutte richiedono un intervento *ex ante* del giudice, e il controllo giurisdizionale corrisponde ad una garanzia della necessarietà e proporzionalità delle attività svolte.

Tuttavia, è opportuno considerare che il Stored Communications Act (SCA)[136] prevede che i "fornitori di servizi di comunicazione elettronica"[137] possano consentire l'accesso a dati relativi a contenuti comunicativi (via cavo o elettronicamente) solo su decreto del giudice[138], e le organizzazioni che offrono tali servizi costituiscono i principali soggetti che conservano i dati di interessati dell'Unione, anche se non gli unici[139].

Nella causa *United States v. Microsoft*[140], era stata contestata l'extraterritorialità di un mandato del giudice fondato sulla SCA. Nel caso di specie, il *Department of Justice* degli Stati Uniti ha emesso un mandato di perquisizione nei confronti di Microsoft Ireland per accedere a dati che erano ubicati nell'Unione. La sede principale negli Stati Uniti aveva la capacità di accedere a tali dati, ma l'azienda statunitense si è rifiutata di farlo[141].

La controversia potrebbe sorgere in assenza di una decisione di adeguatezza. Infatti, in dottrina Peter Swire sostiene che l'istituzione di un accordo ex art. 45

---

[135] ibid 89.

[136] 18 U.S. Code Chapter 121 - Stored wire and electronic communications and transactional records access

[137] Ibid. § 2703 - Required disclosure of customer communications or records: "*provider of electronic communication service of the contents of a wire or electronic communication*"

[138] Jessica Shurson, 'Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law' (2020) 28 International Journal of Law and Information Technology 167, 168.

[139] Una ricerca filtrata nella lista del DPF, stabilisce che 1307 su 2753 aderenti appartengono alla categoria "information and communications technology". Dati acquisiti il: April 24, 2024 6:00 AM EST. Fonte: https://www.dataprivacyframework.gov/list

[140] United States v. Microsoft Corp., 584 U.S. (2018)

[141] La questione è stata risolta dal Clarifying Lawful Overseas Use of Data (CLOUD) Act, definendo che gli ordini giudiziari di acquisizione dei dati sono efficaci indipendentemente dal luogo di conservazione dei dati. Fonte: Theodore Christakis and Fabien Terpan, 'EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options' (2021) 11 International Data Privacy Law 81, 85.

fa sì che "*l'esistenza di un'indagine, dopo un trasferimento lecito, non fa diventare retroattivamente il trasferimento illecito*"[142].

Perciò, la presenza di una decisione di adeguatezza consente alle autorità pubbliche di accedere a dati relativi a contenuti comunicativi per finalità di contrasto penale qualora essi vengano trasferiti presso gli Stati Uniti ad aziende certificate qualificate come fornitori di servizi di comunicazione elettronica esclusivamente su mandato del giudice.

Inoltre, come stabilito dall'allegato VI, qualora non sussista l'obbligo di mandato, viene rafforzata la protezione dei cittadini europei dal quarto emendamento, che "*garantisce che il governo degli Stati Uniti non disponga di un potere illimitato o arbitrario*", sottoponendo l'attività di contrasto penale ad una verifica della "ragionevolezza"[143].

3.3) Effettività e indipendenza dei meccanismi di ricorso

Per quanto concerne i reclami per trattamenti di dati a fini di sicurezza nazionale, il nuovo accordo prevede un meccanismo completamente nuovo rispetto al *Privacy Shield Ombudsperson*.

Il regolamento che integra l'E.O. 14086 istituisce il *Data Protection Review Court* (DPRC), competente nella gestione di reclami su attività di intelligence dei segnali[144] indipendentemente dalla base giuridica del trasferimento (accessibile anche in caso di trasferimento tramite SCC)[145].

Individui provenienti da "Stati qualificati", cioè Paesi terzi designati dall'*Attorney General*, hanno il diritto di presentare reclamo presso un'Autorità per la Protezione dei Dati nazionale[146].

---

[142] Peter Swire, 'When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer' [2019] Cross-Border Data Forum <https://www.crossborderdataforum.org/when-does-gdpr-act-as-a-blocking-statute-the-relevance-of-a-lawful-basis-for-transfer/#_ftnref1>.
[143] Decisione di esecuzione (UE) 2023/1795 allegato VI.
[144] ibid para 176.
[145] EDPB Information Note on the Data Protection Framework redress mechanism for national security purposes 2024 2.
[146] Decisione di esecuzione (UE) 2023/1795 para 176–177.

La designazione di un Paese (o di un'organizzazione regionale di integrazione economica, quale l'UE) come "Stato qualificato" dipende dalle garanzie previste dalla legislazione in materia di intelligence dei segnali per i dati di individui statunitensi e dalla presenza di un accordo per il trasferimento di dati per scopi commerciali in quel paese terzo. La designazione deve perseguire interessi pubblici degli Stati Uniti[147].

Il reclamo è soggetto a requisiti minimi di ammissibilità. Non è necessario provare che i dati siano stati raccolti e trattati da autorità pubbliche statunitensi, ma gli interessati devono avere ragionevoli motivi che i dati siano stati trasferiti a organizzazioni statunitensi, fornire informazioni sui mezzi con i quali è stato effettuato il trasferimento, identificare, se conosciuto, l'ente che ha compiuto la presunta violazione e stabilire il provvedimento richiesto[148].

Inoltre, viene istituito un meccanismo di ricorso a due livelli:

(1) L'indagine preliminare sui reclami spetta al CLPO che fa parte dell'*Office of the Director of National Intelligence* (ODNI).

Esso svolge un esame "*applica[ndo] la legge in modo imparziale*"[149] e bilanciando interessi di sicurezza nazionale con il diritto alla privacy degli individui[150]. Per adempiere alle sue funzioni ha accesso alle informazioni di intelligence necessarie[151]. Esso verifica un'eventuale violazione del decreto presidenziale o del diritto statunitense pertinente, e se la riscontra, predispone una riparazione adeguata agli enti di intelligence[152].

Le decisioni del CLPO hanno effetto vincolante per tutti gli enti di intelligence, i quali devono conformarsi alle misure correttive stabilite dallo stesso[153].

---

[147] E.O. 14086 art. 3 f) i).
[148] Decisione di esecuzione (UE) 2023/1795 para 178.
[149] E.O. 14086 art. 3 c) i) B) iii).
[150] ibid art. 3 c) i) B) i).
[151] Decisione di esecuzione (UE) 2023/1795 para 180.
[152] ibid 181.
[153] E.O. 14086 art. 3 c) ii).

Il CLPO può essere revocato solo per giusta causa dal *Director of National Intelligence*[154] e non può subire interferenze da parte di enti di intelligence[155].
Concluso l'esame, il CLPO comunica al reclamante, tramite l'autorità nazionale, se ha predisposto una riparazione adeguata o se non è stata riscontrata alcuna violazione, unitamente alla possibilità di presentare ricorso al DPRC[156]. La contestazione della decisione deve avvenire tramite l'autorità nazionale competente entro 60 giorni[157].
(2) Il DPRC viene descritto come un tribunale indipendente, essendo "*composto da almeno sei giudici, nominati dall'Attorney General in consultazione con la PCLOB, il Secretary of Commerce e il Director of National Intelligence*". La designazione si fonda su criteri oggettivi di esperienza e competenza nel diritto alla protezione dei dati e al diritto della sicurezza nazionale, contestualmente al fatto che non possono presiedere altre cariche all'interno di pubbliche amministrazioni[158].
L'indipendenza del DPRC è garantita allo stesso modo del CLPO: sono vietate interferenze da parte dell'esecutivo, agisce in maniera imparziale e la revoca è possibile solo per giusta causa[159].
Il DPRC ha la facoltà di accedere ad informazioni classificate per formulare la sua decisione, che non è impugnabile ed ha effetti vincolanti[160]. Qualora accerti una violazione, può esercitare poteri correttivi vincolanti nei confronti degli enti di intelligence[161].

Questo sistema di ricorso è soggetto a controllo su base annuale da parte della PCLOB[162], che valuta la tempestività nel trattare i reclami, se è stato fornito un

---

[154] Decisione di esecuzione (UE) 2023/1795 para 179.
[155] ibid 180.
[156] ibid 183.
[157] ibid 184.
[158] ibid 185; E.O. 14086 art. 3 d) i) A).
[159] Decisione di esecuzione (UE) 2023/1795 para 187.
[160] ibid 191.
[161] E.O. 14086 art. 3 d) ii).
[162] "*Privacy and Civil Liberties Oversight Board*". Ente che fa parte dell'esecutivo competente nel bilanciare le attività di intelligence con i diritti alla privacy e le libertà civili degli individui

accesso alle informazioni necessarie e il rispetto delle garanzie contenute nell'E.O 14086. A tal riguardo, la PCLOB trasmette periodicamente le relazioni sul suo esame ad autorità coinvolte nelle attività di intelligence, e ne pubblica una versione senza informazioni riservate. Inoltre, certifica annualmente la conformità del meccanismo di ricorso con il decreto presidenziale[163].[164]

La giurisprudenza comunitaria presuppone che una protezione legale effettiva (riconosciuta dall'art. 19 TUE, dall'art. 47 della Carta e dall'art. 13 della CEDU) sia strettamente connessa con l'indipendenza dell'organo giudiziario[165].
L'indipendenza è determinata dalla composizione dei soggetti dell'organo, dalla loro nomina e dalle possibilità di rifiuto o revoca della nomina[166].
L'art. 47 della Carta prevede un diritto ad un "*ricorso effettivo dinanzi a un giudice*". Diversamente, l'art. 13 della CEDU stabilisce un diritto ad un "*ricorso effettivo davanti a un'istanza nazionale*". La giurisprudenza della Corte EDU ritiene sufficiente la presenza di un rimedio efficace[167] e per determinare l'effettività rilevano maggiormente i "*poteri e le garanzie procedurali*" attribuiti all'organo giudiziario, in particolare l'indipendenza e la capacità di adottare decisioni vincolanti, piuttosto che considerare meramente la natura dello stesso[168].

---

163 Decisione di esecuzione (UE) 2023/1795 para 194.
164 Oltre a questo sistema, esistono diverse procedure legali per agire in caso di illegittimità alla raccolta o al trattamento di dati personali da parte di enti governativi (decisione di esecuzione 1795/2023, para. 195-198), contestualmente a possedere un diritto di accesso (ai sensi della legge sulla libertà di informazione) alle registrazioni degli enti federali indipendentemente dal fatto che includano informazioni personali (para. 199). Agevolando l'accesso alle informazioni, diventa più semplice per l'individuo fornire le informazioni minime richieste affinché il reclamo sia dichiarato ammissibile.
165 Alejandro Sánchez Frías, 'A New Presumption for the Autonomous Concept of "Court or Tribunal" in Article 267 TFEU: ECJ 29 March 2022, Case C-132/20, *Getin Noble Bank*' (2023) 19 European Constitutional Law Review 320, 329.
166 ibid. Fonte originale: Corte di Giustizia dell'UE, Causa C-132/20, *Getin Noble Bank* para. 95
167 Docksey and Propp (n 36) 29.
168 Sergi Batlle and Arnaud van Waeyenberge, 'EU–US Data Privacy Framework: A First Legal Assessment' (2024) 15 European Journal of Risk Regulation 191, 190. Fonte originale: ECtHR, judgment of 6 September 1978, Klass and others v. Germany, n°5029/71. para 67.

Il principio di indipendenza richiesto dall’art. 47 della Carta presuppone che le decisioni del giudice non siano influenzate da decisioni o pressioni esterne[169]. Dalla recente decisione della Corte nella causa *BN, DM, EN v. Getin Noble Bank S.A.*[170] si può ricavare che l’indipendenza non dipende dalla mera nomina da parte dell’esecutivo, ma anche dall’influenza che l’esecutivo può esercitare, anche indirettamente, sui giudici[171].
La Corte ha sottolineato che il *Privacy Shield Ombudsperson* era designato dal *Secretary of State* ed era parte dell’esecutivo[172]. Allo stesso modo, nel nuovo meccanismo, il DPRC è nominato dall’*Attorney General* e fa parte dell’esecutivo. Tuttavia l’E.O. 14086 ha predisposto garanzie di indipendenza relative al DPRC che potranno considerarsi adeguate o meno esclusivamente in base a come verranno applicate nella pratica, e ciò determinerà la conformità o meno con il contenuto espresso dall’art. 47 della Carta[173].
Infatti, l’EDPB rileva che le garanzie, se non limitate dall’esecutivo ed adottate nella pratica, sono adeguate a garantire l’indipendenza del DPRC[174].

L’istituzione di un organo giurisdizionale precostituito per legge ed *ex lege* indipendente dall’esecutivo sarebbe stata la via più semplice per conformarsi all’ordinamento europeo.
Tuttavia, come delineato in dottrina da T. Christakis, K. Propp e P. Swire, sono da prendere in considerazione diversi fattori che complicano questa possibilità. In primo luogo è possibile evidenziare una difficoltà dal punto di vista politico, dovuta principalmente alla difficoltà nel riformare un ambito complesso come la sorveglianza.

---

169 Docksey and Propp (n 36) 28–29.
170 Causa C-132/20, *BN, DM, EN v. Getin Noble Bank S.A.*, Marzo 2022, EU:C:2022:235
171 Maria Giacalone, ‘Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework’ (2023) 2023 8 European Papers 149, 155–156.
172 *Causa C-311/18* (n 29) para 195.
173 Laura Carola Drechsler and others, ‘Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers from the European Union to the United States’ [2023] CiTiP Working Paper Series - KU Leuven 34 <https://lirias.kuleuven.be/4088124&lang=en>.
174 EDPB Parere 5/2023 para 228.

Inoltre, la dottrina costituzionale e la giurisprudenza della Corte Suprema americana dimostrano delle difformità con il diritto UE con riguardo al diritto di accesso alla giustizia[175]. In particolare, richiede a chi vuole agire in giudizio di "*dimostrare di aver subito un pregiudizio concreto, specifico ed effettivo o imminente*"[176]. Questo requisito di ammissibilità non è previsto per il meccanismo definito nell'accordo[177], permettendo ai cittadini europei di presentare reclamo senza dimostrare che i loro dati siano oggetto di trattamento[178]. Diversamente, l'istituzione di un organo giudiziario precostituito per legge renderebbe complicato aggirare questo requisito.

Questo dimostra come una simile riforma richiederebbe tempi lunghi e si scontrerebbe con difficoltà di varia natura. In ogni caso, la possibilità di assicurare un livello di protezione sostanzialmente equivalente permette agli Stati Uniti di istituire un meccanismo di ricorso diverso da quello dell'Unione ma che dovrà dimostrarsi ugualmente protettivo dei diritti degli individui europei.

Il DPF prevede un meccanismo di ricorso che protegge gli interessati nell'Unione in modo maggiore rispetto agli individui americani[179]. Infatti, sono evidenti gli sviluppi positivi rispetto al *Privacy Shield Ombudsperson*. Nonostante ciò, alcune delle problematiche esposte e il modo in cui le garanzie vengono implementate nella pratica potrebbero portare nuovamente il sistema di ricorso all'attenzione della Corte.

---

[175] Theodore Christakis, Kenneth Propp and Peter Swire, 'EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute Is Necessary to Produce an "Essentially Equivalent" Solution' (*European Law Blog*, 31 January 2022) <https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution/>.

[176] EDPB Parere 5/2023 para 214.

[177] Christakis, Propp and Swire (n 173).

[178] Decisione di esecuzione (UE) 2023/1795 para 178.

[179] Alex Joel, 'Protecting Privacy and Promoting Transparency in a Time of Change: My Perspective after 14 Years as Civil Liberties Protection Officer' 1, 10.

4) Conclusioni

La tesi ha analizzato le questioni controverse del nuovo meccanismo, cercando di determinare se il livello di protezione dei dati degli interessati nell'Unione garantito dal Data Privacy Framework sia sostanzialmente equivalente agli standard di protezione europei. Dall'analisi dell'accordo e della giurisprudenza della Corte emergono questioni critiche con riguardo all'accesso ed utilizzo di dati da parte di autorità pubbliche per finalità di sicurezza nazionale.

Nelle precedenti sentenze la Corte ha stabilito i requisiti essenziali che deve presentare il regime di trasferimento internazionale di dati, a cui la legislazione pertinente statunitense non sembra essersi totalmente conformata.

In primo luogo, per quanto riguarda il rispetto del requisito di necessarietà e proporzionalità, l'art. 702 FISA e l'E.O. 12333, che costituiscono i principali strumenti per lo svolgimento di attività di intelligence, non forniscono garanzie adeguate ai cittadini europei.

In particolare, la FISA limita la portata delle procedure di targeting e minimizzazione, e l'applicazione del quarto emendamento, ai soli cittadini statunitensi. A ciò si aggiunge una vigilanza della Corte FISA inadeguata, per via della mancanza di analisi sull'adeguatezza dei bersagli e da una verifica insufficiente delle misure approvate, denotata dall'approvazione in passato di programmi di sorveglianza di massa intrusivi nei diritti fondamentali dei cittadini statunitensi ed europei.

L'E.O. 12333 consente di praticare *bulk data collections*, che in mancanza delle dovute limitazioni costituiscono una violazione del requisito di proporzionalità.

La FISA e l'E.O. 12333 sono integrati dal recente E.O. 14086, con lo scopo di dare stabilità all'accordo.

Nonostante ciò, permangono delle criticità. La definizione degli obiettivi legittimi come fondamento delle attività di intelligence ha il potenziale per limitare la portata delle misure adottare, se non fosse che tali basi giuridiche per la raccolta sono notevolmente generiche. Per la raccolta di massa, che è consentita quando strettamente necessaria, sono definiti degli obiettivi legittimi differenti rispetto alle altre attività di raccolta che, nonostante la maggior precisione

rispetto al precedente accordo, costituiscono ancora una potenziale minaccia alla protezione dei dati dei cittadini europei.
A tal riguardo, l'EDPB sostiene che la raccolta in blocco di dati per attività di intelligence dovrebbe essere sottoposta ad un'autorizzazione giudiziaria *ex ante* da parte di un organismo indipendente dall'esecutivo[180]. Recentemente anche il Parlamento europeo ha sottolineato che, nonostante le garanzie previste alla raccolta di massa, "*essa non prevede un'autorizzazione preventiva indipendente per la raccolta generalizzata*", non permettendo al governo di giustificare ingerenze alla vita privata[181].
L'implementazione di un sistema di autorizzazioni giudiziarie preventive per tali attività di intelligence, come previsto in sede di contrasto penale, soddisferebbe il requisito di necessarietà e proporzionalità previsto dalla Carta, evitando violazioni degli artt. 7 e 8 della Carta e fornendo maggiore stabilità all'accordo.

In secondo luogo, la Corte aveva sottolineato la carenza di effettività e indipendenza dei precedenti meccanismi di ricorso, in violazione dell'art. 47 della Carta.
Come analizzato, la presenza di un organo non istituito *ex lege* è coerente con le tradizioni giuridiche degli Stati Uniti e la possibilità di perseguire su un piano sostanziale l'equivalenza all'Unione del livello di protezione dei dati lo rende legittimo ai sensi del diritto UE.
Le garanzie di indipendenza sono più solide rispetto al *Privacy Shield Ombudsperson*, ma potrebbero essere contestate data l'appartenenza all'esecutivo. Secondo la giurisprudenza della Corte, l'indipendenza non dipende dalla mera natura dell'organo, ma anche dall'influenza che diversi soggetti possono esercitarvi. Per tale motivo, la conformità del meccanismo di ricorso con i principi della Carta dipenderà dall'esperienza pratica.

180 EDPB Parere 5/2023 para 142–144.
181 Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy (2018/2645(RSP)) para 3.

Determinata l'instabilità dell'accordo, dovuta a problematiche rilevate dall'EDPB e in dottrina, è possibile che il nuovo accordo venga messo nuovamente al vaglio della Corte. Qualora l'accordo fosse dichiarato nuovamente invalido, è necessario stabilire delle misure adeguate a dare continuità al flusso di dati, salvaguardando i diritti degli individui.

Come affermato in dottrina da T. Christakis, indubbiamente "*la soluzione più semplice è quella di non trasferire i dati qualora ci sia un rischio di accesso da parte di entità governative*"[182]. Tuttavia, questo approccio non prende in considerazione il valore, anche per i cittadini UE, dei flussi di dati e non effettua un bilanciamento appropriato con il perseguimento di obiettivi di sicurezza nazionale. A riguardo, l'EDPB stabilisce che l'accesso ai dati da parte di autorità pubbliche è sempre possibile qualora uno "Stato interessato si "*trovi dinanzi a una minaccia grave alla sicurezza nazionale, che si dimostri reale e attuale o prevedibile*"[183].

Una possibile prospettiva futura è la mitigazione del rischio con il "*data localization*", inteso come la conservazione e il trattamento dei dati all'interno dell'Unione con lo scopo di evitare accessi illegittimi da parte di governi esteri[184]. Questa prospettiva sarebbe in linea con l'intenzione, recentemente manifestata dalle istituzioni europee, di raggiungere la c.d. "*European Digital Sovereignty*", intesa, nel panorama dei dati, come una capacità per l'Europa di "*riprendere il controllo dei suoi dati*" in un ambiente gestito prevalentemente da società estere[185]. Attualmente, la presenza della decisione di adeguatezza limita la sovranità sui dati perseguita dall'Europa, ma si potrebbe trattare di una potenziale soluzione temporanea in caso di invalidazione del nuovo accordo.

---

182 Theodore Christakis, 'The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach.' [2024] CIPL/CBDF Paper Series 11 <https://papers.ssrn.com/abstract=4732294>.
183 EDPB Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza para 34.
184 Christakis (n 180) 12.
185 Madiega Tambiama, 'Digital Sovereignty for Europe' [2020] EPRS | European Parliamentary Research Service 1, 3.

BIBLIOGRAFIA

a) Fonti normative

1. Atti vincolanti

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), 119 OJ L § (2016). http://data.europa.eu/eli/reg/2016/679/oj/ita.

Decisione di esecuzione (UE) 2000/520 della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti., 215 OJ L § (2000).
ELI: http://data.europa.eu/eli/dec/2000/520/oj/ita.

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., 207 OJ L § (2016).
ELI: http://data.europa.eu/eli/dec_impl/2016/1250/oj.

Decisione di esecuzione (UE) 2023/1795 della Commissione del 10 luglio 2023 a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali.
ELI: http://data.europa.eu/eli/dec_impl/2023/1795/oj

Executive Order 12333 - United States Intelligence Activities (2008).
https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf.

Executive Order 14086 - Enhancing Safeguards for United States Signals Intelligence Activities (2022).
https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence.

2. Atti non vincolanti

Commissione europea, "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA 2013" (Comunicazione) COM(2013) 846 final. (2013).
https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:52013DC0846.

Commissione europea, "sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite 2013" (Comunicazione) COM(2013) 847 final. (2013).
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52013DC0847.

EDPB Information Note on the Data Protection Framework redress mechanism for national security purposes (2024). https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.

EDPB 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 (2023). https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en.

EDPB Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza (2020). https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_it.

EDPB Rules of Procedure on the Data Protection Framework redress mechanism for national security purposes (2024). https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.

EDPS - Opinione sul «Data protection reform package» (2012). https://www.edps.europa.eu/data-protection/our-work/publications/opinions/data-protection-reform-package_en.

EDPS Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016). https://www.edps.europa.eu/data-protection/our-work/publications/opinions/eu-us-privacy-shield_en.

Risoluzione del Parlamento europeo - Adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati - 2023/2501(RSP) (2023). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_IT.html.

Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy - 2018/2645(RSP) (2018). https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52018IP0315.

US Government - White Paper, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II (2020). https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

b) Giurisprudenza

Causa C-311/18, Conclusioni dell'avvocato generale Henrik Saugmandsgaard Øe, *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems* ECLI:EU:C:2019:1145

Causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems* ECLI:EU:C:2020:559

Causa C-362/14, *Data Protection Commissioner c. Maximilian Schrems* ECLI:EU:C:2015:650

Causa C-291/12, *Michael Schwarz c. Stadt Bochum* ECLI:EU:C:2013:670

c) Fonti dottrinali

1. Libri

Adam, Roberto, e Antonio Tizzano. Lineamenti di diritto dell'Unione europea. Quinta edizione. Torino: Giappichelli, 2022.

Naef Tobias. *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*. Vol. 28. European Yearbook of International Economic Law. Cham: Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-19893-9.

2. Articoli / Capitoli di libro

Drechsler Laura, e Irene Kamara. «Essential Equivalence as a Benchmark for International Data Transfers after Schrems II». In *Research Handbook on EU Data Protection Law*, 314-352. Edward Elgar Publishing, 2022. https://www.elgaronline.com/edcollchap/edcoll/9781800371675/9781800371675.00022.xml.

Kuner Christopher. «Background and Introduction». In *Transborder Data Flows and Data Privacy Law*, 1-23. Oxford, New York: Oxford University Press, 2013. https://global.oup.com/academic/product/transborder-data-flows-and-data-privacy-law-9780199674619?cc=it&lang=en&.

Directorate General for Internal Policies of the Union (European Parliament), e Caspar Bowden. *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*. Publications Office of the European Union, 2013. https://data.europa.eu/doi/10.2861/34622.

Batlle Sergi, e Arnaud van Waeyenberge. «EU–US Data Privacy Framework: A First Legal Assessment». *European Journal of Risk Regulation* 15, fasc. 1 (marzo 2024): 191–200. https://doi.org/10.1017/err.2023.67.

Bourgeois Jacques, Cameron Kerry, William Long, Maarten Meulenbelt e Alan Charles Raul. «Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States», 2016, 1–20.

Brännström Leila. «Global Inequality and the EU International Law Position on Cross-Border Data Flows». *Nordic Journal of International Law* 92, fasc. 1 (21 aprile 2023): 119-137. https://doi.org/10.1163/15718107-bja10059.

Brännström Leila, Markus Gunneflo, Gregor Noll, e Amin Parsa. «Legal Imagination and the US Project of Globalising the Free Flow of Data». *AI & SOCIETY*, 9 agosto 2023. https://doi.org/10.1007/s00146-023-01732-y.

Callewaert Johan. «Do We Still Need Article 6(2) TEU? Considerations on the Absence of EU Accession to the ECHR and Its Consequences». *Common Market Law Review* 55, fasc. 6 (1 dicembre 2018). https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\COLA\COLA2018142.pdf.

Chander Anupam. «Is Data Localization a Solution for Schrems II?» *Journal of International Economic Law* 23, fasc. 3 (10 novembre 2020): 771-784. https://doi.org/10.1093/jiel/jgaa024.

Christakis Theodore e Fabien Terpan. «EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options». *International Data Privacy Law* 11, fasc. 2 (6 agosto 2021): 81-106. https://doi.org/10.1093/idpl/ipaa022.

Cole Mark D. e Christina Etteldorf. «Recent Developments and Overview of the Country and Practitioners Reports ». European Data Protection Law Review (EDPL) 8, fasc. 4 (2022): 507-510.

Cole Mark D. e Annelies Vandendriessche. «From Digital Rights Ireland and Schrems in Luxembourg to Zakharow and Szabo/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance Case Notes». *European Data Protection Law Review (EDPL)* 2, fasc. 1 (2016): 121-129.

Costello Róisín Áine. «Schrems II: Everything Is Illuminated?» *European Papers* 2020 5, fasc. 2 (15 ottobre 2020): 1045-1059. https://doi.org/10.15166/2499-8249/396.

«Department of Homeland Security, Office of Intelligence and Analysis - Intelligence Oversight Program and Guidelines», 19 gennaio 2017.

Di Salvo Philip e Gianluigi Negro. «Framing Edward Snowden: A Comparative Analysis of Four Newspapers in China, United Kingdom and United States». *Journalism* 17, fasc. 7 (1 ottobre 2016): 805–822. https://doi.org/10.1177/1464884915595472.

Docksey Christopher. «Schrems II and Individual Redress - Where There's a Will, There's a Way | Lawfare», 12 ottobre 2020. https://www.lawfaremedia.org/article/schrems-ii-and-individual-redress-where-theres-will-theres-way.

Docksey Christopher, e Kenneth Propp. «Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective». *Oslo Law Review* 10, fasc. 1 (14 novembre 2023): 1-34. https://doi.org/10.18261/olr.10.1.2.

Drechsler Laura Carola, Abdullah Elbi, Els Kindt, Janos Meszaros, e Koen Vranckaert. «Third time is the charm? The draft Data Privacy Framework for international personal data transfers from the European Union to the United States». *CiTiP Working Paper Series - KU Leuven*, maggio 2023. https://lirias.kuleuven.be/4088124&lang=en.

Fischer Philipp E. «Getting Privacy to a New Safe Harbour: Comment on the CJEU Judgement of 6 October 2015, Schrems v. Data Protection Commissioner Case Comment». *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 6, fasc. 3 (2015): 229–233.

Ghibellini Nicolo. «Some Aspects of the EU's New Framework for Personal Data Privacy Protection Survey - Cyberspace Law». *Business Lawyer* 73, fasc. 1 (2018 2017): 207–14.

Giacalone Maria. «Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework». *European Papers* 2023 8, fasc. 1 (14 giugno 2023): 149-157. https://doi.org/10.15166/2499-8249/644.

Haq, Ayesha. «Mending the Broken Data Privacy Framework». *Ohio Lawyer* 36, fasc. 4 (2022): 14-17.

Henderson Rebecca. «The EU-US Data Privacy Framework: Doomed Like Its Predecessors?» *Business Law Review* 44, fasc. 5 (1 ottobre 2023): 188-189. https://doi.org/10.54648/bula2023024

Ivers Emily A. «Using State-Based Adequacy Now, National Adequacy over Time to Anticipate and Defeat Schrems III Notes». *Boston College Law Review* 62, fasc. 7 (2021): 2573–2618.

James G. McAdams III. «Foreign Intelligence Surveillance Act (FISA): An Overview», s.d., 1-11. https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf

Jaycox Mark M. «No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333». *Harvard National Security Journal* 12, fasc. 1 (2021): 58-115.

Joel Alex. «Necessity, Proportionality, and Executive Order 14086». *Joint PIJIP/TLS Research Paper Series*, 1 maggio 2023, 1–31. https://digitalcommons.wcl.american.edu/research/99

Joel Alex. «Protecting Privacy and Promoting Transparency in a Time of Change: My Perspective after 14 Years as Civil Liberties Protection Officer», 13 febbraio 2023, 1–13.

Kuner Christopher. «Protecting EU Data Outside EU Borders under the GDPR». *Common Market Law Review* 60, fasc. 1 (1 febbraio 2023): 77–106. https://doi.org/10.54648/cola2023004.

Kuner Christopher. «Reality and Illusion in EU Data Transfer Regulation Post Schrems». *German Law Journal* 18, fasc. 4 (luglio 2017): 881–918. https://doi.org/10.1017/S2071832200022197.

Kuner Christopher. «Schrems II Re-Examined». *Verfassungsblog: On Matters Constitutional*, 25 agosto 2020. https://doi.org/10.17176/20200825-183419-0.

Landau, Susan. «Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations». *IEEE Security & Privacy* 11, fasc. 4 (luglio 2013): 54–63. https://doi.org/10.1109/MSP.2013.90.

Margulies Peter. «Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy Cybersurveillance in the Post-Snowden Age». *Washington and Lee Law Review* 72, fasc. 3 (2015): 1283-1306.

Margulies Peter, e Ira Rubinstein. «EU Privacy Law and U.S. Surveillance: Solving the Problem of Transatlantic Data Transfers», 3 ottobre 2021. https://www.lawfaremedia.org/article/eu-privacy-law-and-us-surveillance-solving-problem-transatlantic-data-transfers.
Marionneaux Mark Andrew. «International Scope of Fourth Amendment Protections: United States v. Verdugo-Urquidez Note». *Louisiana Law Review* 52, fasc. 2 (1992 1991): 455-478.

Mulligan Andrea. «Constitutional Aspects of International Data Transfer and Mass Surveillance Short Articles and Comments». *Irish Jurist* 55 (2016): 199–208.

Nino Michele. «La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo». *Diritti umani e diritto internazionale*, fasc. 3 (2020): 733-759. https://doi.org/10.12829/99542.

Propp Kenneth, e Peter Swire. «After Schrems II: A Proposal to meet the Individual Redress Challenge», 13 agosto 2020. https://www.lawfaremedia.org/article/after-schrems-ii-proposal-meet-individual-redress-challenge.

Rembert Robert L. «TikTok, WeChat, and National Security: Toward a U.S. Data Privacy Framework Comments». *Oklahoma Law Review* 74, fasc. 3 (2022): 463–502.

Rollins John W. e Edward C. Liu. «NSA Surveillance Leaks: Background and Issues for Congress». *Congressional Research Service*, 4 settembre 2013, 1–21.

Sánchez Frías Alejandro. «A New Presumption for the Autonomous Concept of 'Court or Tribunal' in Article 267 TFEU: ECJ 29 March 2022, Case C-132/20, *Getin Noble Bank*». *European Constitutional Law Review* 19, fasc. 2 (giugno 2023): 320-345. https://doi.org/10.1017/S157401962300007X.

Savin Andrej. «EU-US Data Privacy Framework – The New Framework for Transatlantic Data Transfers». *Journal of European Consumer and Market Law* 12, fasc. 4 (1 agosto 2023): 159-164.

Shurson Jessica. «Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law». *International Journal of Law and Information Technology* 28, fasc. 2 (1 marzo 2020): 167-184. https://doi.org/10.1093/ijlit/eaaa011.

Siemion Rita. «Protecting Privacy in the Digital Age: Beyond Reforming Bulk Telephone Records Collections». *Human Rights* 41, fasc. 4 (2015): 17-20.

Sloan Alistair. «Schrems II: Commission 0». *Business Law Review* 41, fasc. Issue 6 (1 dicembre 2020): 257-259. https://doi.org/10.54648/BULA2020127.

«Statement of April F. Doss, Partner Artner Saul Ewing LLP, before the United States House of Representatives Hudiciary Committee Concerning Section 702 of the Foreign Intelligence Surveillance Act», 1 marzo 2017.

Stehlík Václav e Lusine Vardanyan. «Schrems II: Will It Really Increase the Level of Privacy Protection against Mass Surveillance?» *Bratislava Law Review* 4, fasc. 2 (31 dicembre 2020): 111-128. https://doi.org/10.46282/blr.2020.4.2.215.

Swire Peter. «When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer». Cross-Border Data Forum, 4 novembre 2019. https://www.crossborderdataforum.org/when-does-gdpr-act-as-a-blocking-statute-the-relevance-of-a-lawful-basis-for-transfer/#_ftnref1.

Tambiama Madiega. «Digital Sovereignty for Europe». EPRS | European Parliamentary Research Service, luglio 2020, 1–12.

Terpan Fabien. «EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?» *European Papers* 2018 3, fasc. 3 (8 febbraio 2019): 1045-1059. https://doi.org/10.15166/2499-8249/261.

«The United States and the European Union Begin Implementation of the European Union-U.S. Data Privacy Framework». *American Journal of International Law* 117, fasc. 2 (aprile 2023): 346–352. https://doi.org/10.1017/ajil.2023.17.

Toy Alan, e Gehan Gunasekara. «Is There a Better Option than the Data Transfer Model to Protect Data Privacy?» *University of New South Wales Law Journal* 42, fasc. 2 (2019): 719-746.

Vries, Sybe A. de. «EU and ECHR: Conflict of Harmony?» *Utrecht Law Review* 9, fasc. 1 (2013): 78–79.

Whilt Nicholas J. «The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties That Make Defense of Our Nation Worthwhile». *Southwestern University Law Review* 35, fasc. 3 (2006): 361-404.

Young Stewart. «Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases». *Michigan Telecommunications & Technology Law Review* 10, fasc. 1 (1 ottobre 2003): 139-174.

Zinser Alexander. «European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers». *Tulane Journal of Technology and Intellectual Property* 6 (2004): 171-179.

Cohen Alexandra. «Can a Federal District Court Review the Decisions of the New Data Protection Review Court?», 20 ottobre 2022. https://privacyacrossborders.org/2022/10/20/can-a-federal-district-court-review-the-decisions-of-the-new-data-protection-review-court/.

Joel Alex. «Without Confirming or Denying», 22 febbraio 2023. https://privacyacrossborders.org/2023/02/22/without-confirming-or-denying/.

Mantel Lauren. «The Civil Liberties Protection Officers: The Gateway to Redress», 23 aprile 2024. https://privacyacrossborders.org/2024/04/23/the-civil-liberties-protection-officers-the-gateway-to-redress/.

Pervaiz Shanzay. «Overview of Implementation Procedures for EO 14086», 15 dicembre 2022. https://privacyacrossborders.org/2022/12/15/overview-of-implementation-procedures-for-eo-14086/.

Pervaiz Shanzay. «What's Next for the New Executive Order and the DPRC?», 14 ottobre 2022. https://privacyacrossborders.org/2022/10/14/whats-next-for-the-new-executive-order-and-the-dprc/.

d) Blog / News / Preprints

Christakis Theodore Kenneth Propp, e Peter Swire. «EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute Is Necessary to Produce an "Essentially Equivalent" Solution». *European Law Blog* (blog), 31 gennaio 2022. https://europeanlawblog.eu/2022/01/31/eu-us-adequacy-negotiations-and-the-redress-challenge-whether-a-new-u-s-statute-is-necessary-to-produce-an-essentially-equivalent-solution/.

DIGITALEUROPE. «Schrems II Impact Survey Report», 26 novembre 2020. https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/.

Irion Kristina. «Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law». *European Law Blog* (blog), 24 luglio 2020.

https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/.

Joel Alex e Francesca Oliveira. «Redress: What Is the Problem?» *European Law Blog* (blog), 28 settembre 2021. https://europeanlawblog.eu/2021/09/28/redress-what-is-the-problem/.

Kuner Christopher. «Exploring the Awkward Secret of Data Transfer Regulation: The EDPB Guidelines on Article 3 and Chapter V GDPR». *European Law Blog* (blog), 13 dicembre 2021. https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr/.

Kuner Christopher. «The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation». *European Law Blog* (blog), 17 luglio 2020. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

Sajfert Juraj. «Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy». *European Law Blog* (blog), 26 ottobre 2020. https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/.

Christakis Theodore. «After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe». *European Law Blog* (blog), 21 luglio 2020. https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/.

Christakis Theodore. «"Schrems III"? First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 1)». *European Law Blog* (blog), 13 novembre 2020. https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/.

Christakis Theodore. «"Schrems III"? First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 2)». *European Law Blog* (blog), 16 novembre 2020. https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/.

Christakis Theodore. «"Schrems III"? First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 3)». *European Law Blog* (blog), 17 novembre 2020. https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/.

Christakis Theodore, Kenneth Propp e Peter Swire. «EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers». *European Law Blog* (blog), 16 febbraio 2022. https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers/.

Propp Kenneth. «In the Shadow of the European Court of Justice: The Luxembourg Conference on Transatlantic Data Transfers». *European Law Blog* (blog), 17 novembre 2023. https://europeanlawblog.eu/2023/11/17/in-the-shadow-of-the-european-court-of-justice-the-luxembourg-conference-on-transatlantic-data-transfers/.

Ruschemeier Hannah. «Nothing New in the West? The Executive Order on US Surveillance Activities and the GDPR». *European Law Blog* (blog), 14 novembre 2022. https://europeanlawblog.eu/2022/11/14/nothing-new-in-the-west-the-executive-order-on-us-surveillance-activities-and-the-gdpr/.

Swire Peter, Theodore Christakis, e Kenneth Propp. «The redress mechanism in the Privacy Shield successor: On the independence and effective powers of the DPRC», 11 ottobre 2022. https://iapp.org/news/a/the-redress-mechanism-in-the-privacy-shield-successor-on-the-independence-and-effective-powers-of-the-dprc/.

Greenwald, Glenn. «NSA Collecting Phone Records of Millions of Verizon Customers Daily». *The Guardian*, 6 giugno 2013, sez. US news. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn, e Spencer Ackerman. «NSA Collected US Email Records in Bulk for More than Two Years under Obama». *The Guardian*, 27 giugno 2013, sez. US news. https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

Greenwald, Glenn, e Ewen MacAskill. «NSA Prism Program Taps in to User Data of Apple, Google and Others». *The Guardian*, 7 giugno 2013, sez. US news. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

O'Keefe, Ed. «Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program». *Washington Post*, 26 novembre 2021. https://www.washingtonpost.com/news/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/.

Barczentewicz Mikolaj. «Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States». SSRN Scholarly Paper. Rochester, NY, 25 settembre 2023. https://papers.ssrn.com/abstract=4585431.

Christakis Theodore. «"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy». SSRN Scholarly Paper. Rochester, NY, 7 dicembre 2020. https://doi.org/10.2139/ssrn.3748098.

Christakis Theodore. «The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach.» *CIPL/CBDF Paper Series*, 20 febbraio 2024. https://papers.ssrn.com/abstract=4732294.

Christakis Theodore. «Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?» SSRN Scholarly Paper. Rochester, NY, 27 maggio 2019. https://papers.ssrn.com/abstract=3397047.

Christakis Theodore e Katia Bouslimani. «National Security, Surveillance and Human Rights». SSRN Scholarly Paper. Rochester, NY, 1 dicembre 2019. https://papers.ssrn.com/abstract=3599994.

Korff Douwe. «The Inadequacy of the October 2022 New US Presidential Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities». SSRN Scholarly Paper. Rochester, NY, 30 novembre 2022. https://doi.org/10.2139/ssrn.4495169.

Lock Tobias. «EU Accession to the ECHR: Implications for the Judicial Review in Strasbourg». SSRN Scholarly Paper. Rochester, NY, 7 dicembre 2010. https://papers.ssrn.com/abstract=1736602.

Rauhofer Judith e Caspar Bowden. «Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud». SSRN Scholarly Paper. Rochester, NY, 21 giugno 2013. https://doi.org/10.2139/ssrn.2283175.