RIVISTA DI DIRITTI COMPARATI

Il *Data Privacy Framework* e il trasferimento dei dati personali tra Stati Uniti e Unione Europea. Appunti di una comparazione *

Vittoria Margherita Sofia Trifiletti

SOMMARIO: 1. Introduzione. – 2. Il trasferimento dei dati personali al di fuori dell'Unione Europea ai sensi dell'art. 45 GDPR. – 3. Le vicende del trasferimento dei dati personali tra UE e US. – 4. La decisione *Schrems II*. – 5. Il *Data Privacy Framework*: un vero cambio di paradigma? – 6. Il problema del canone di proporzionalità. – 7. Un effettivo meccanismo di tutela giurisdizionale? – 8. Tutto cambia affinché tutto resti uguale? – 9. Conclusioni.

1. *Introduzione*

Negli ultimi anni il problema relativo al trasferimento dei dati personali dall'Unione Europea agli Stati Uniti è stato avvertito con particolare urgenza. Infatti, due celebri pronunce della Corte di Giustizia – la C - 362/14[1] e la C - 311/18[2], meglio note come *Schrems I* e *II* –, avevano bocciato le modalità di trasferimento dei dati personali esistenti tra Unione Europea e Stati Uniti, ritenendo che le garanzie offerte dalla legislazione statunitense in materia non fossero equiparabili agli standard di protezione offerti e richiesti dal diritto dell'Unione Europea. Così, a seguito di queste due pronunce, la disciplina del trasferimento dei dati personali tra una sponda e l'altra dell'Oceano era, quindi, diventata particolarmente problematica.

La questione parrebbe essere oggi finalmente risolta grazie al *Data Privacy Framework* (DPF)[3] – oggetto della presente riflessione – ovvero un nuovo accordo intervenuto tra gli Stati Uniti e l'Unione Europea, a seguito del quale la Commissione europea, con una decisione di adeguatezza[4], ha ritenuto le nuove garanzie prestate dagli Stati Uniti equiparabili a quelle previste dall'Unione Europea.

In questo scenario il presente contributo intende allora analizzare le novità introdotte dalla legislazione statunitense sul punto, nonché la conseguente decisione

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a *double-blind peer review*.

[1] Corte giust., 6 ottobre 2015, C- 362/14, *Schrems I*.

[2] Corte giust., 16 luglio 2020, C- 311/18, *Schrems II*.

[3] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, 25 marzo 2022, disponibile sul sito https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.

[4] Decisione di implementazione della Commissione Europea del 10/7/2023.

di adeguatezza della Commissione Europea per comprendere, così, se il quadro normativo attuale possa essere davvero l'atto definitivo di questa annosa querelle o se, al contrario, rischi anch'esso di cadere, al pari delle precedenti discipline, sotto la scure della Corte di Giustizia.

È allora bene ricordare che l'Unione Europea ha disciplinato in modo compiuto la tutela dei dati personali, in particolare attraverso il Regolamento 679/2016, *General Data Protection Regulation* (GDPR). L'importanza di tale atto normativo è il riflesso del fatto che ogni giorno, in un mondo sempre più globalizzato[5], i dati dei cittadini europei si trovano ad essere oggetto di utilizzo e di trasferimento[6]. In questo contesto un particolare problema è, allora, quello del trasferimento dei dati al di fuori dell'Unione, giacché in questa ipotesi occorrerà valutare se i paesi terzi dispongano o meno, ed in quale misura, di garanzie idonee alla protezione dei dati dei cittadini europei.

Il punto è, invero, di particolare rilevanza, tant'è che il GDPR dedica espressamente il capo V proprio al trasferimento dei dati personali al di fuori dell'Unione Europea, ammettendo diverse modalità di trasferimento che, però, non presentano tutte lo stesso grado di agevolezza.

2. Il trasferimento dei dati personali al di fuori dell'Unione Europea ai sensi dell'art. 45 GDPR

La modalità più agevole di trasferimento dei dati al di fuori dell'Unione Europea è certamente quella prevista dall'articolo 45 GDPR che si fonda su una decisione di adeguatezza resa dalla Commissione Europea. Si tratta, dunque, di un atto politico-amministrativo con il quale, proprio la Commissione, garantisce che il livello di protezione dei dati personali esistente nello stato terzo in questione sia adeguato rispetto agli standard previsti dal diritto dell'Unione. Si noti che non si richiede un livello di protezione identico a quello previsto dall'Unione Europea, bensì un livello sostanzialmente equivalente. A tal fine, nel formulare la sua decisione, la Commissione dovrà quindi – in forza del comma 2 dell'articolo 45 – tenere in considerazione la sussistenza di alcuni elementi quali: le modalità con cui i dati personali nel sistema giuridico extraunionale in questione sono effettivamente tutelati, la presenza o meno di un'autorità di controllo indipendente, deputata a sorvegliare il rispetto della tutela dei dati personali, nonché gli impegni assunti in sede

[5] D. Di Micco, *Regolare la globalizzazione. Contributo giuridico – comparante all'analisi del fenomeno globale*, Milano, 2018.

[6] Si pensi, a titolo di esempio, al trasferimento dei dati personali posto in essere da strumenti come Google Analytics. Sul punto cfr. *ex multis* W.G. Voss, *Transatlantic Data Transfer Compliance*, in *Boston University Journal of Science & Technology Law*, 2022, p. 199 ss.; F. Zorzi Giustiniani, *Il Panopticon digitale. I cookies tra diritto e pratica nell'Unione Europea*, in *Freedom, Security & Justice: European Legal Studies*, 2022, p. 247 ss.

internazionale dal paese in questione in relazione alla protezione dei dati personali[7]. Questo anche in considerazione del considerando numero 104, dove si prevede, invero, che la Commissione fondi la sua valutazione su criteri chiari e obiettivi e che il livello di protezione offerto dallo stato terzo debba essere, appunto, «sostanzialmente equivalente a quello assicurato all'interno dell'Unione»[8].

A conferma di quanto la questione sia delicata è bene osservare come tale valutazione sia soggetta, invero, a rivalutazioni periodiche. Pertanto, laddove in sede di riesame le tutele offerte da uno stato terzo non risultassero più adeguate rispetto agli standard europei, l'atto di esecuzione verrebbe allora sospeso, dando luogo così a nuove consultazioni tra l'Unione e lo stato in questione, ma fermo restando che la valutazione definitiva spetterà comunque sempre unilateralmente alla Commissione Europea (previo parere dell'*European Data Protection Board*, EDPB).

Si noti come questa modalità politico-amministrativa sia stata largamente utilizzata per regolare il trasferimento dei dati personali dall'Unione verso i paesi terzi, basti pensare ad esempio a quanto avviene con l'Argentina, Israele, il Canada[9], e il Giappone[10] e più recentemente con la Repubblica di Corea[11]. Questo perché, a fronte del rigoroso vaglio che abbiamo poc'anzi descritto segue però una procedura piuttosto agile: operando infatti ai sensi dell'articolo 45 GDPR non verranno più richieste le autorizzazioni specifiche ai fini del trasferimento dei dati personali nel paese extraunionale, dal momento che, proprio in ragione della decisione di adeguatezza emessa dalla Commissione, lo stato terzo in questione verrà sostanzialmente equiparato ad uno stato membro dell'Unione Europea. Ed è allora proprio questo effetto, conseguenza della pronuncia della Commissione, ciò che semplifica il trasferimento dei dati e che rende, quindi, l'ipotesi di cui all'articolo 45 GDPR preferibile alle altre[12].

---

[7] In particolare, l'articolo in esame fa riferimento a diversi elementi da prendere in considerazione nel valutare l'adeguatezza del livello di protezione del paese terzo quali, ad esempio, lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la legislazione generale e settoriale e gli impegni internazionali assunti dal paese terzo.

[8] Regolamento UE 679/2016, Considerando n. 104. Peraltro, la Corte di Giustizia nel caso *Schrems I* aveva già precisato questo requisito (Corte giust., 6 ottobre 2015, C- 362/14, *Schrems I*, par. 73 ss.).

[9] Relazione del 15 gennaio 2024 della Commissione al Parlamento Europeo ed al Consiglio sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE.

[10] Relazione del 3 aprile 2023 della Commissione al Parlamento Europeo ed al Consiglio sul primo riesame della decisione di adeguatezza relativa al Giappone.

[11] Decisione di Esecuzione (UE) 2022/254 della Commissione Europea del 17 dicembre 2021.

[12] Si rileva come in realtà questo modus operandi non sia nuovo, ma trovi il suo fondamento già con la direttiva 95/46/CE. In particolare, tale direttiva sanciva all'art. 25, par. 6 in materia di trasferimento di dati personali verso paesi terzi che la Commissione Europea potesse constatare l'adeguatezza del livello di protezione dei dati personali previsto da un paese terzo. Pertanto, alla luce di questa disposizione la Commissione Europea aveva ritenuto che le garanzie offerte dal diritto statunitense in materia di protezione dei dati personali fossero adeguate con la decisione del 26 luglio

Questo ragionamento è confermato anche dalla vicenda che riguarda il trasferimento dei dati personali tra l'Unione Europea e gli Stati Uniti, giacché già nel 2016[13] con il cosiddetto Privacy Shield[14] si procedette in questo modo.

In quell'occasione la Commissione Europea aveva ritenuto che le tutele offerte dal diritto statunitense fossero adeguate agli standard imposti dal GDPR e, pertanto, il trasferimento dei dati tra l'Unione Europea e gli Stati Uniti avveniva ai sensi dell'articolo 45 GDPR.

Di segno opposto è stata però nel 2020 la pronuncia della Corte di Giustizia nel noto caso *Schrems II*[15], che, ritenendo che il diritto statunitense non offrisse tutele

---

2000, meglio nota come Safe Harbour Framework. Tale valutazione fu poi smentita nel 2015 dalla Corte di giustizia all'esito del caso *Schrems I*, dal momento che le garanzie offerte dal diritto statunitense in materia di protezione dei dati personali furono ritenute in contrasto con gli art. 7, 8 e 47 della Carta di Nizza. Invero in questa decisione la Corte ha precisato come il livello di protezione adeguato offerto dal paese terzo debba essere inteso «nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta» (Corte giust., 6 ottobre 2015, C- 362/14, *Schrems I*, par. 73).

[13] Sul punto cfr. C. Kuner, *Protecting Eu Data outside Eu borders under the GDPR*, in *Common Market Law Review*, 2023, p. 84 ss.; F. Bignami – G. Resta, *Transatlatic Privacy Regulation: conflict and cooperation*, in *Law and Contemporary Problems*, 2015, p. 238 ss.; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, London, 2021, p. 128 ss.; O. Pollicino – M. Bassini – G. De Gregorio, *Internet Law and Protection of Fundamental Rights*, Milano, 2022, p. 185 ss.; M. Mastracci, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbour al Privacy Shield*, in *La Comunità Internazionale*, 2016, p. 558 ss.; B. Carotti, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa*, in *Giornale Diritto Amministrativo*, 2016, p. 333 ss.; G. Scarchillo, *Dal Safe Harbor al Privacy Shield il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems*, in *Rivista del commercio internazionale*, 2016, p. 910 ss., X. Tracol, *"Invalidator" strikes back: The harbour has never been safe*, in *Computer Law & Security Review*, 2016, p. 345 ss.; S.J. Schulhofer, *An International right to privacy? Be careful what you wish for*, in *International Journal of Constitutional Law*, 2016, p. 238 ss.; D. Cole – F. Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, in *International Journal of Constitutional Law,* 2016, p. 220 ss.; A. Vedaschi, *Privacy and Data Protection versus National Security in Transnational Flights: the EU – Canada PNR Agreement*, in *International Data Privacy Law*, 2018, p. 129 ss.; C. Kuner, *Reality and illusion in EU data transfer regulation post-Schrems*, in *German Law Journal*, 2017, p. 881 ss.

[14] Decisione di Esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016.

[15] Sul punto cfr. ex multis C. Peraro, *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione Europea verso paesi terzi*, in *Ordine Internazionale e Diritti Umani,* 2021, p. 666 ss.; E. Terolli, *Privacy e Protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *Il Diritto dell'Informazione e dell'Informatica*, 2021, p. 49 ss.; O. Pollicino, *Diabolical Persistence. Thoughts on the Schrems II Decision*, in *MediaLaws*, 2020, p. 314 ss.; R. Bifulco, *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno*, in *Diritto Pubblico Europeo – Rassegna Online*, 2020, p. 5 ss.; M. 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*, in *Diritti Umani e Diritto Internazionale*, 2020, p. 733 ss.; F. Rossi Dal Pozzo, *L'Accordo Privacy Shield non è un vero scudo per la privacy: scenari passati e futuri in merito al trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Rivista di Diritto Internazionale*, 2020, p. 1112 ss.; X. Tracol, "*Schrems II": the return of*

paragonabili a quelle dell'Unione, ha invalidato la decisione di adeguatezza della Commissione Europea dando luogo così ad una situazione di incertezza circa le possibilità effettive di trasferimento dei dati tra gli Stati Uniti e l'Unione Europea. Di conseguenza, proprio a valle della pronuncia della Corte, si è quindi avvertita la necessità di avviare nuovi negoziati tra gli Stati Uniti e l'Unione Europea dai quali nascerà, infine, il *Data Privacy Framework*, oggetto della presente trattazione.

3. Le vicende del trasferimento dei dati personali tra UE e US

Nel corso degli anni gli Stati Uniti e l'Unione Europea hanno quindi sempre tentato di regolare il trasferimento dei dati personali attraverso una decisione di adeguatezza della Commissione europea.

Già prima dell'entrata in vigore del GDPR, infatti, i rapporti tra gli Stati Uniti e l'Unione Europea erano fondati sul cosiddetto *Safe Harbor Framework*[16], un accordo che mirava anch'esso a garantire un'adeguata protezione nel trattamento dei dati, ma che è però venuto meno nel 2015 a seguito della pronuncia della CGUE nel caso *Schrems I*[17] con cui la Corte ha ritenuto che il livello di garanzie relative al trattamento dei dati personali negli Stati Uniti non fosse equiparabile a quello richiesto dall'Unione Europea.

Ciò che ne seguì fu una situazione di profonda incertezza, che spinse i due soggetti a definire una nuova disciplina. Infatti, già nel 2016 venne concluso tra gli Stati Uniti e l'Unione Europea un nuovo accordo: il cosiddetto *Privacy Shield*, che però ebbe anch'esso vita breve. Già nel 2020 la Corte di Giustizia, con la pronuncia *Schrems II*, lo dichiarò in contrasto con la Carta dei diritti fondamentali dell'Unione, ravvisando che il trattamento dei dati personali negli Stati Uniti non fosse assistito da garanzie adeguate rispetto agli standard europei.

A seguito di questa seconda pronuncia di inadeguatezza il tema del trasferimento dei dati personali tra gli Stati Uniti e l'Unione Europea era tornato,

---

the Privacy Shield, in *Computer Law & Security Review*, 2020, p. 1054 ss.; T. Christakis – F. Terpan, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International Data Privacy Law*, 2021, p. 81 ss.; G. Formici, *Schrems colpisce ancora? Il trasferimento dei dati personali dall'Unione Europea a Stati terzi, le Conclusioni dell'avvocato generale nel caso Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems e una storia che rischia di ripetersi*, in *MediaLaws*, 2020, p. 310 ss.; M. Giraudo, *On legal bubbles: some thoughts on legal shockwaves at the coreo of the digital economy*, in *Journal of Institutional Economics*, 2022, p. 592 ss; E. Celeste – F. Fabbrini, *Competing Jurisdictions: Data Privacy Across the Borders*, in T. Lynn et al. (curr.), *Data Privacy and Trust in Cloud Computing*, Cham, 2021.

[16] Decisione della Commissione Europea del 26 luglio 2000.

[17] Sul punto cfr. *ex multis* G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il Diritto dell'Informazione e dell'Informatica*, 2015, p. 697 ss.; O. Pollicino – M. Bassini, *La Carta dei diritti fondamentali dell'Unione Europea nel* reasoning *dei giudici di Lussemburgo*, in *Il Diritto dell'Informazione e dell'Informatica*, 2015, p. 741 ss.

allora, ad essere particolarmente incerto[18]. Gli Stati Uniti dovevano, quindi, intervenire sulla loro legislazione risolvendo le diverse problematiche che indirettamente erano state rilevate dalla Corte di Giustizia nel caso *Schrems II*. In questa prospettiva, nell'ottobre 2022 l'amministrazione Biden ha, dunque, disposto l'Executive Order 14086[19].

Così, nel luglio 2023, proprio in ragione della procedura di cui all'articolo 45 GDPR che abbiamo descritto, la Commissione Europea ha approvato il Data Privacy Framework, assumendo, quindi, che l'Executive Order 14086 garantirebbe un livello di protezione dei dati personali equivalente rispetto ai canoni previsti dall'Unione Europea[20].

A valle di ciò è allora opportuno domandarsi se le recenti modifiche legislative apportate dall'amministrazione Biden al quadro legislativo statunitense in materia di garanzia dei dati personali soddisfino davvero, e definitivamente, gli standard previsti dal diritto dell'Unione Europea per come interpretati dalla Corte di Giustizia. È quindi opportuno ripercorrere le argomentazioni utilizzate dalla Corte di Giustizia nel caso *Schrems II* per comprendere, così, la natura delle problematiche evidenziate dalla Corte e capire, allora, se le soluzioni recentemente adottate potranno davvero dirsi risolutive.

4. La decisione Schrems II

Come abbiamo visto, nel luglio 2020 la Corte di Giustizia aveva ritenuto che il Privacy Shield fosse incompatibile con le garanzie previste dall'Unione Europea in

[18] Sul punto cfr. M. Giraudo – E. Fosch-Villaronga – G. Malgieri, *Competing Legal Futures*, in corso di pubblicazione in *German Law Journal*, consultabile al link: https://ssrn.com/abstract=4499785.

[19] Federal Register Vol. 87, No. 198, 14 ottobre 2022. Sul punto cfr. C. Docksey – K. Propp, *Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective*, in *Oslo Law Review*, 2023, p. 1 ss.

[20] La Commissione Europea ha ritenuto soddisfacenti le garanzie implementate dagli Stati Uniti pur a fronte di una valutazione negativa emessa dal Parlamento Europeo il 5 maggio 2023, accessibile al link https://www.europarl.europa.eu/doceo/document/B-9-2023-0234_IT.html). Preoccupazioni in merito al Data Privacy Framework sono state espresse anche nel Parere 5/2023 del 28 febbraio 2023 dell'European Data Protection Board, accessibile al link: https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf. Anche in dottrina si sono manifestati dubbi riguardo alle garanzie offerte dal Data Privacy Framework. Sul punto cfr. A. Savin, *The New Framework for Transatlantic Data Transfers*, in *Copenhagen Business School Law Research Paper*, 2023, p. 1 ss.; S. Gerke – D. Rezaeikhonakdar, *Privacy Shield 2.0. A New Trans – Atlantic Data Privacy Framework Between the European Union and the United States*, in *Cardozo Law Review*, 2023, p. 351 ss. Perplessità sulle garanzie relative alla protezione dei dati personali derivanti dal nuovo Data Privacy Framework sono state altresì evidenziate dal Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (cfr. *Jahresberichte der Landesbeauftragten für Datenschutz und Informationsfreiheit*, 9 febbraio 2024, p. 80 ss.).

materia di trattamento dei dati personali e segnatamente con gli articoli 7, 8, 47 e 52 della Carta di Nizza.

In particolare, l'articolo 7 della Carta di Nizza sancisce il rispetto della vita privata e familiare, nonché del domicilio e delle comunicazioni di ogni persona. Ancora più esplicitamente il successivo articolo 8 prevede per ciascuno il diritto alla protezione dei dati di carattere personale che lo riguardano. Si noti, come chiarisce la Corte di Giustizia, che questi non sono diritti assoluti, e come tali incomprimibili, ma sono diritti che rivestono una funzione sociale e come tali possono essere limitati, ma unicamente secondo le modalità previste dall'articolo 52 della Carta di Nizza[21], secondo cui «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».

La valutazione che compie quindi la Corte si incentra su due punti. In primis si occupa di verificare se le limitazioni alla tutela dei dati personali siano o meno conformi al principio di proporzionalità. In secondo luogo, la Corte vaglia poi la compatibilità dei meccanismi di accesso alla giustizia per la tutela dei dati personali offerti dal paese terzo rispetto agli standard previsti dall'Unione.

Il primo nodo del caso *Schrems II* è, dunque, quello relativo alla possibilità di comprimere, ed eventualmente entro quali limiti, un diritto che è ritenuto fondamentale nell'ordinamento dell'Unione quale è appunto quello alla privacy. In particolare, la Corte si è soffermata su due normative statunitensi – la sezione 702 del *Foreign Intelligence Surveillance Act* (FISA) e l'*Executive Order 12333* – che comprimono la tutela dei dati personali in ragione di esigenze di sicurezza nazionale e di intelligence, domandandosi se tale compressione avvenga o meno nel rispetto del principio di proporzionalità di cui agli articoli 7 e 8 della Carta. La risposta della Corte è stata di segno negativo ravvisando in tali compressioni una violazione del canone di proporzionalità che è principio del diritto europeo.

È infatti possibile osservare che la sezione 702 FISA non prevede delle limitazioni ai programmi di sorveglianza per scopi di intelligence, né prevede garanzie per i cittadini stranieri che fossero assoggettati a tali programmi. Proprio alla luce di tali carenze, la Corte ha pertanto ritenuto che tale normativa statunitense non soddisfacesse il principio di proporzionalità di cui alla Carta di Nizza, poiché «una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura e impongano requisiti minimi»[22]. In aggiunta a ciò, e con riguardo al secondo punto, occorre poi osservare che il mero fatto che la sezione 702 FISA si poggi sui requisiti

[21] Sul punto, Corte giust., 16 luglio 2020, C – 311/18, *Schrems II*, par. 172: «tuttavia, i diritti sanciti agli articoli 7 e 8 della Carta non appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale».

[22] *Ibidem*, par. 180.

indicati dalla *Presidential Policy Directive 28* (PPD – 28) non conferisce ai soggetti titolari dei diritti, che qui vengono compressi, gli strumenti necessari ad agire in sede giurisdizionale, nei confronti delle autorità statunitensi, per la tutela degli stessi.

Problema analogo è rilevato dalla Corte anche in relazione all'Executive Order 12333 che tace circa le possibilità di ricorso in sede giurisdizionale per i soggetti titolari dei diritti che vengono compressi. La Corte rileva, inoltre, come anche la raccolta "in blocco" dei dati personali, prevista da tale normativa, non sia conforme ai canoni europei dal momento che la stessa non è circoscritta in modo sufficientemente chiaro e preciso[23].

In particolare, poi, la Corte chiarisce come non possa essere inteso quale vero e proprio ricorso giurisdizionale l'istituzione della figura dell'*Ombudsperson*. Questa figura, infatti, da intendersi alla stregua di un mediatore, non costituisce affatto un organo davvero indipendente e capace di produrre decisioni vincolanti[24]. Designato dal Segretario di Stato, il mediatore è parte integrante del Dipartimento di Stato degli Stati Uniti e non trova, pertanto, alcuna vera garanzia circa la sua inamovibilità ed indipendenza dal potere politico. A ciò si aggiunga, infine, che l'ordinamento statunitense non prevedeva nemmeno la vincolatività delle decisioni emesse da questo organo.

Pertanto, alla luce di questi dati, la Corte di Giustizia ha ritenuto che la decisione di adeguatezza con cui la Commissione europea affermava l'equiparabilità alle garanzie del diritto dell'Unione Europea in materia di protezione dei dati personali della normativa statunitense, non fosse corretta. Infatti, la compressione del diritto alla privacy realizzata dalle normative statunitensi prese in esame non risultava affatto bilanciata da alcun meccanismo di proporzionalità e mancava, inoltre, di un'adeguata tutela giudiziaria.

5. Il Data Privacy Framework: un vero cambio di paradigma?

Abbiamo così assistito ad una sostanziale contrapposizione tra la Commissione Europea da una parte, ed in particolare tra le sue decisioni di adeguatezza, e la prospettiva adottata dalla Corte di Giustizia dall'altra. Se per la prima gli standard di adeguatezza forniti dagli Stati Uniti sarebbero sempre risultati adeguati, di segno opposto è stata, invece, ogni valutazione operata da parte della seconda.

A questo punto, è quindi opportuno chiedersi se l'*Executive Order 14086* soddisfi finalmente gli standard e le garanzie richieste dalla Corte di Giustizia.

A tal proposito è bene osservare che le novità in esso contenute hanno sì in larga parte sostituito la normativa precedente (ed in particolare la PPD – 28 ad eccezione della Sezione 3, di una appendice complementare e della Sezione 6 che

[23] *Ibidem*, parr. 181 – 184.
[24] *Ibidem*, parr. 192 – 199.

restano invariate[25]), ma continuano a doversi coordinare con le altre normative che non sono state modificate. Pertanto permane la dicotomia sancita dalla sezione 702 FISA tra cittadini statunitensi e stranieri, così come anche l'*Executive Order* 12333 continua ad essere vigente. Ad entrambe queste normative, però, si applicano i principi introdotti dall'Executive Order 14086 e soprattutto si introduce un sistema di *redress*, cioè di ricorso, su due livelli operante anche in relazione alle altre due normative. Questo è, dunque, l'attuale assetto delle fonti del diritto statunitense sul punto.

L'*Executive Order 14086* cerca, quindi, di risolvere le problematiche evidenziate dalla Corte di Giustizia nel caso *Schrems II* senza stravolgere l'intero assetto normativo, bensì operando un intervento mirato. Resta allora da vedere se ciò sia sufficiente.

6. Il problema del canone di proporzionalità

Con l'Executive Order 14086 assistiamo indubbiamente a un tentativo molto più compiuto da parte dell'amministrazione degli Stati Uniti di circoscrivere l'ambito di intervento dell'intelligence statunitense di quanto non fosse avvenuto in passato. Emerge qui, a ben vedere, la tensione esistente tra due diritti di pari rango, ovvero tra il diritto alla privacy da un lato e le esigenze di sicurezza nazionale dall'altro, e la difficoltà di operare per il loro bilanciamento.

Sul primo piatto della bilancia troviamo il diritto alla privacy. Se nell'ordinamento dell'Unione Europea esso è espressamente riconosciuto nella Carta di Nizza[26], risulta, invece, molto più complesso[27] rinvenire il suo specifico riconoscimento nell'ordinamento statunitense[28]. Questo sistema giuridico è infatti

[25] Decisione di implementazione della Commissione Europea del 10/7/2023, 124 ss.

[26] Art. 8 Carta di Nizza.

[27] Per una analisi comparata sul regime giuridico della privacy nell'ordinamento statunitense ed in quello unionale cfr. R. De Bruin, *A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence*, in *Hastings Science and Technology Law Journal*, 2022, p. 130 ss.

[28] Nel dibattito statunitense si rileva come la tematica relativa al diritto alla privacy emerga con particolare evidenza a partire dal celebre articolo di Louis D. Brandeis e Samuel D. Warren pubblicato sull'Harvard Law Review nel 1890 (S.D. Warren – L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, p. 193 ss.). Invero si tratta di un saggio che ha segnato profondamente la discussione su questo diritto nel panorama statunitense come rilevato *ex multis* da Fred R. Shapiro e da Harry Kalven Jr. (sul punto cfr. F.R. Shapiro, *The Most – Cited Law Review Articles*, in *California Law Review*, 1985, p. 1545 ss.; H. Kalven Jr., *Privacy in Tort Law – Were Warren and Brandeis Wrong?*, in *Law and Contemporary Problems*, 1966, p. 327 ss.) che lo definiscono rispettivamente un «unquestioned classic» e il «most influential law review article of all». Invero secondo James Q. Whitman si dovrebbe far risalire la genesi del diritto di privacy alla pronuncia della Corte Suprema *Boyd v. United States* (116 U.S. 616 (1886)), secondo l'Autore più vicina alla nozione di privacy intesa come «sanctity of the home», più propria del diritto statunitense e come tale, dunque, più legata al concetto di *dignity*, piuttosto che alla nozione più continentale di questo diritto, come tale legata al concetto di *liberty*, a cui paiono più legati

molto più sfuggente di quello europeo già solo nel fornire, ad esempio, una qualsivoglia definizione unitaria di questo concetto, dal momento che le esigenze della sua tutela si sono affermate attraverso due distinti percorsi, identificabili rispettivamente come *privacy decisional* e *privacy informational*[29]. Col primo termine ci si riferisce essenzialmente alla libertà dell'individuo nel porre in essere autonomamente – e dunque senza l'interferenza statale – le proprie scelte di vita privata; un concetto, quindi, che non ritroviamo nella nozione di privacy di matrice europea e che nella giurisprudenza statunitense è stato legato a diversi aspetti della vita degli individui, quali, ad esempio, il diritto all'aborto[30]. Con il secondo[31], invece, si fa riferimento alla protezione dell'individuo nel trattamento dei suoi dati personali, un concetto, quindi, ben più vicino a quello di provenienza dell'Unione Europea.

Diversamente, nella tradizione del diritto europeo, l'approccio alla privacy si caratterizza per una visione generalmente più unitaria, volta cioè a realizzare una protezione quanto più possibile ampia, opponibile cioè a ogni possibile fonte e forma di inferenza e lesione di tale diritto.

Tuttavia, nonostante questo quadro di visibile diversità di approccio in cui l'ordinamento statunitense non sembra trovare una forma omogenea di tutela, è però altresì doveroso osservare che in diverse occasioni la Corte Suprema[32] ha espressamente ravvisato nella Costituzione statunitense[33] il fondamento ultimo di

---

nel loro celebre articolo Warren e Brandeis (sul punto cfr. J.Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, in *Yale Law Journal*, 2004, p. 1213 ss.).

[29] Sul punto cfr. *ex multis* T. Azarchs, *Informational Privacy: Lessons from Across the Atlantic*, in *Journal of Constitutional Law*, 2014, p. 805 ss.; M.D. Fan, *Constitutionalizing Informational Privacy by Assumption*, in *University of Pennsylvania Journal of Constitutional Law*, 2012, p. 953 ss.; A. Etzioni, *A Communitarian Perspective on Privacy*, in *Connecticut Law Review*, 2000, p. 897 ss.; J. Rubenfeld, *The Right to Privacy*, in *Harvard Law Review*, 1989, p. 737 ss. Si rileva, inoltre, come tale dicotomia emerga altresì nella pronuncia della Corte Suprema *Whalen v. Roe* nella quale si precisa come la nozione di privacy tuteli due interessi: da un lato «the individual interest in avoiding disclosure of personal matter» e dall'altro «the interest in indipendence in making certain kinds of important decisions» (429 U.S. 599 (1977), 599 – 600).

[30] *Roe v. Wade*, 410 U.S. 113 (1973). Sul punto cfr. ex multis J.H. Ely, *The Wages of Crying Wolf: A Comment on Roe v. Wade*, in *Yale Law Journal*, 1973, p. 920 ss.; D. Barnard et al., *The Evolution of the Right to Privacy after Roe v. Wade*, in *American Journal of Law & Medicine*, 1987, 13, p. 365 ss.

[31] Tale nozione emerge a partire dal caso *Whalen v. Roe*, 429 U.S. 599 (1977).

[32] Giova ricordare che il fondamento costituzionale della cosiddetta informational privacy non è incontroverso. Sul punto, infatti, il Giudice Antonin Scalia nella sua opinione concorrente, a cui ha aderito anche il Giudice Thomas, nella decisione *NASA v. Nelson* afferma espressamente che «a federal constitutional right to "informational privacy" does not exist» (*NASA v. Nelson*, 562 U.S. 134 (2011), Scalia concurring, p. 1).

[33] Nella celebre pronuncia *Roe v. Wade*, il Giudice Blackmun, autore dell'opinione di maggioranza, stabilisce che, pur non essendo il diritto alla privacy esplicitamente menzionato nella Costituzione, la Corte Suprema ne ha identificato le basi a seconda delle occasioni nel I Emendamento, nel IV e nel V, nelle «penumbras of the Bill of Rights», nel IX e nel XIV Emendamento (410 U.S. 113 (1973), p. 152 ss.).

questo diritto, elevandolo così nelle sue ragioni di tutela. In particolare, nel caso *Griswold v. Connecticut*[34] la Corte ha individuato tale fondamento nelle cosiddette «*penumbras*» del *Bill of Rights*[35]. Accanto a ciò è poi bene ricordare, sia pur qui incidentalmente, che esiste anche un complesso e variegato catalogo di tutele previste nello strumentario tradizionale del *common law*, e in particolare nella *tort law*. In particolare, già William Prosser identificò quattro *tort* che garantivano una protezione al diritto alla privacy: *intrusion upon seclusion or solitude or into the plaintiff's private affairs*, *public disclosure of embarassing private facts*, *appropriation of name or likeness* e *false light in the public eye*[36]. Inoltre anche gli *statutes*, statali e federali, concorrono alla costruzione di un ampio apparato di tutele sia pur diffuso e frazionato per settori[37]. Emerge così con chiarezza come il diritto alla privacy di matrice statunitense non risulti essere uniforme ed omogeneo quanto quello dell'Unione Europea.

Sull'altro piatto della bilancia, poi, contrapposto al diritto alla privacy, vi è un interesse vitale per ogni nazione, ovvero quello alla sicurezza nazionale. Negli Stati Uniti questa esigenza è stata avvertita con particolare urgenza soprattutto a seguito dell'attentato dell'11 settembre 2001, all'esito del quale si è intensificata l'attività di

---

Sulla protezione del diritto alla privacy negli Stati Uniti cfr. ex multis D.J. Garrow, *Privacy and the American Constitution*, in *Social Research*, 2001, p. 55 ss.; A. Di Martino, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Napoli, 2017; N. Lugaresi, *Internet, Privacy e Pubblici Poteri negli Stati Uniti*, Milano, 2000, p. 39 ss.; U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008; D.J. Solove, *A Taxonomy of Privacy*, in *University of Pennsylvania Law Review*, , p. 477 ss.; J. Greene, *The So – Called Right to Privacy*, in *U. C. Davis Law Review*, 2010, p. 715 ss.; S.E. Igo, *The Known Citizen. A History of Privacy in Modern America*, Cambridge, 2018.

[34] 381 U.S. 479 (1965).

[35] La Corte Suprema ha dunque ritenuto che il diritto di privacy emerga dalla lettura di alcune parti della Costituzione ed in particolar modo sia riconducibile al I, III, IV, V, IX Emendamento, benché non sia esplicitamente menzionato dal testo costituzionale.

[36] Sul punto cfr. W.L. Prosser, *Law of Torts*, Eagan, 1971; Id., *Privacy*, in *California Law Review*, 1960, p. 383 ss.; T. Gerety, *Redefining Privacy*, in *Harvard Civil Rights – Civil Liberties Law Review*, 1977, p. 247 ss. Inoltre viene fornita tutela a questo diritto anche anche grazie ad altri *tort* quali: *breach of confidence*, *defamation*, *infliction of emotional distress*, *trespass* (P. Guarda – G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, 2023, p. 220 ss.).

[37] Invero a livello federale le leggi sono poche e settoriali, basti pensare, ad esempio, al Privacy Act del 1974 (5 U.S.C. § 552) in materia di raccolta e utilizzo dei dati personali da parte delle agenzie federali, ma anche al Health Insurance Portability and Accountability Act (100 Stat. 2548, 1996) noto anche con l'acronimo HIPAA, in materia di dati sanitari, al Gramm – Leach – Bliley Act o GLBA del 1998 (15 U.S.C. 6801) in materia di diritto bancario e al Children's Online Privacy Protection Act o COPPA (15 U.S.C. 6501 - 6505) in materia di tutela del diritto alla privacy online dei minori di anni 13. Anche a livello statale le leggi in materia di diritto alla privacy sono poche e settoriali, tra quelle più complete si segnala il California Consumer Privacy Act o CCPA emanato nel 2018 che opera solo a favore dei consumatori.

Sul punto cfr. J. Beverage, *The Privacy Act of 1974: An Overview*, in *Duke Law Journal*, 1976, *Seventh Annual Administrative Law Issue*, p. 301 ss.; Commitee on Government Operations United States Senate, Commitee on Government Operations House of Representatives, *Legislative History of the Privacy Act of 1974 S. 3418* (Public Law 93 – 579), Washington, 1976.

intelligence nel Paese. Sul punto è bene osservare come la sezione 702 FISA[38] sia stata profondamente riformata nel 2008, col *FISA Amendments Act*, introducendo così una disparità di trattamento tra cittadini americani o stranieri e a seconda che gli uni e gli altri si trovino o meno sul territorio statunitense[39].

Questo aspetto è di fondamentale importanza perché ci consente di capire che il conflitto tra il diritto alla privacy e la sicurezza nazionale viene risolto dall'ordinamento statunitense in modo diverso a seconda della nazionalità del soggetto coinvolto. Se si tratta di un cittadino statunitense, infatti, la sezione 702 FISA che comprime fortemente il diritto alla privacy, fino sostanzialmente ad annichilirlo, non solo non può essere applicata, ma, laddove lo fosse, sarebbe in contrasto con il IV Emendamento[40] e, perciò, incostituzionale. Laddove, invece, si tratti di un cittadino straniero, che si trovi ragionevolmente all'estero, ed è proprio questo l'ambito di applicazione della sezione 702 FISA, non sorge una questione di incostituzionalità proprio perché il IV Emendamento non è applicabile agli stranieri ubicati all'estero[41]. Questo principio, invero, è emerso nella giurisprudenza statunitense a partire dal caso *United States v. Verdugo – Urquidez*[42] che ha sancito la non applicabilità agli stranieri delle garanzie dettate dal IV Emendamento

A valle di questa distinzione nella disciplina, operata in base alla nazionalità degli individui e a dove essi si trovino, l'Executive Order 14086 nella seconda sezione si occupa di definire e circoscrivere il legittimo intervento dell'intelligence. Si tratta, a ben vedere, di un elenco di ipotesi che pare, però, piuttosto variegato ed ampio[43],

---

[38] Si rileva, inoltre, che la sez. 702 FISA è un provvedimento temporaneo che sarebbe dovuto scadere nel 2018. La sua validità è stata prorogata nel 2018 fino al dicembre 2023 con il FISA Amendments Reauthorization Act. Il 22 dicembre 2023 il National Defense Authorization Act for Fiscal Year 2024 ha esteso la sua validità fino al 19 aprile 2024.

[39] Sulla genesi del FISA cfr. Privacy And Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 28 settembre 2023, p. 20 ss.; D.S. Sills, *Strengthen Section 702: A Critical Intelligence Tool Vital to the Protection of Our Country*, in *National Security Law Brief*, 2017, p. 1 ss.

[40] Sul rapporto tra IV Emendamento e il diritto di privacy cfr. P.M. Schwartz – J.R. Reidenberg, *Data Privacy Law – A Study of United States Data Protection*, Charlottesville, 1996, p. 60 ss.; D.J. Solove – P.M. Schwartz, *Information Privacy Law*, New York, 2018, p. 253 ss.

[41] In relazione al rapporto tra il IV Emendamento e la sezione 702 FISA cfr. *United States v. Muhtorov*, No. 18-1366 (10th Cir. 2021); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019); *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016), ma anche R.G. Miller, *FISA Section 702: Does Querying Incidentally Collected Information Constitute a Search Under the Fourth Amendment?*, in Notre Dame Law Review Reflection, 2020, 95, 3, p. 139 ss.; P.G. Machtiger, *Updating the Fourth Amendment Analysis of U.S. Person Communication Incidentally Collected Under FISA Section 702*, in *Harvard Law School National Security Journal*, 2021, p. 1 ss. Sull'applicabilità delle garanzie previste dal IV Emendamento anche agli stranieri cfr. A. Walen, *Fourth Amendment Rights for Nonresident Aliens*, in R.A. Miller (ed.), *Privacy and Power. A Transatlantic Dialogue in the Shadow of the NSA – Affair*, Cambridge, 2017, p. 282 ss.

[42] 494 U.S. 259 (1990).

[43] Infatti, l'Executive Order 14086 nella Sec. (2) (iii) (b) (i) individua diversi obiettivi qualificati come legittimi, tra cui, ad esempio, la protezione contro il terrorismo, quella contro le attività di spionaggio poste in essere dai governi stranieri e quella contro le minacce alla cybersecurity.

ragion per cui risulta difficile affermare che esso sia in sé bastevole per ritenere sufficientemente circoscritte le attività di intelligence. Si pensi, ad esempio, al fatto che, oltre alle ipotesi classiche di sicurezza nazionale, risultano ricomprese anche numerose altre previsioni, quali ad esempio quelle relative al cambiamento climatico, sicché tale catalogo sembra tutt'altro che circoscritto[44].

In questo quadro, per risolvere il conflitto tra i diritti ora menzionato, l'*Executive Order 14086* fa rimando alle nozioni di ragionevolezza e di proporzionalità. Infatti, si stabilisce espressamente che, nel pesare i due piatti della bilancia, dove sono contrapposti da un lato il diritto alla privacy e dall'altro gli interessi di sicurezza nazionale, questi ultimi prevarranno anche laddove questi metodi di indagine non siano gli unici percorribili[45]. In ogni caso, si potrà procedere in questo modo unicamente nelle ipotesi in cui ciò sia giudicato conforme al canone di proporzionalità, all'esito di un giudizio di bilanciamento di detti diritti[46].

Pertanto, posto che il catalogo di ipotesi in cui il diritto alla privacy cede il passo alle esigenze di sicurezza nazionale è molto ampio (e forse troppo perché si possa ritenere che si stia procedendo effettivamente in base ad un catalogo di ipotesi tassative) è bene domandarsi se, nel quadro dei rapporti con l'Unione Europea in materia di protezione dei dati, tale modus operandi possa ritenersi altresì adeguato anche per soddisfare le indicazioni dalla Corte di Giustizia nella sentenza *Schrems II*.

La verifica di tale ipotesi non può prescindere da una riflessione su come il criterio di proporzionalità venga inteso sulle due sponde dell'Atlantico. A ben vedere, infatti, la nozione di bilanciamento propria dell'ordinamento statunitense, pur essendo forse più ampia nelle sue declinazioni[47], non sembra però rispondere perfettamente alle logiche di valutazione che innervano il concetto di proporzionalità europeo[48]. Del resto, anche la genesi di queste due modalità decisionali – *balancing* e proporzionalità – sono state storicamente molto differenti[49].

---

[44] M.C. Daly, *The New EU/US Privacy Framework – is it enough?*, in *Privacy & Data Protection*, 2023, p. 8 ss.

[45] EO 14086, Sec. 2 (a) (ii) (A): «signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority».

[46] EO 14086, Sec. 2(a) (ii) (B): «signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside».

[47] Sul punto cfr. V.M.S. Trifiletti, *Tra categorizzazione e bilanciamento: la giurisprudenza della Corte Suprema statunitense in una dicotomia dai labili confini*, in *Isaidat Law Review*, 2022, p. 91 ss.

[48] Sul punto cfr. A. Stone Sweet – J. Mathews, *Proportionality Balancing and Global Constitutionalism*, in *Columbia Journal of Transnational Law*, 2008, p. 74 ss.

[49] Sul punto cfr. M. Cohen – Eliya – I. Porat, *American Balancing and German Proportionality: The Historical Origins*, in *International Journal of Constitutional Law*, 2010, p. 263 ss.

Dal momento che, quindi, il concetto di proporzionalità non ha esatto omologo nel contesto giuridico di arrivo, e cioè in quello statunitense, è ben possibile che l'applicazione di questa nozione non sarà affine a quella di provenienza dell'Unione Europea e che, quindi, ci si baserà su una valutazione ancorata, invece, sui parametri del bilanciamento statunitense. Del resto, lo stesso Executive Order 14086 fa riferimento non solo al concetto di proporzionalità, ma altresì a quello di bilanciamento, quasi a suggerire che nel diritto statunitense questi concetti – in realtà non completamente sovrapponibili – siano speculari[50]. La scarsa chiarezza sul punto potrebbe così creare ancora maggiori problemi di coordinamento tra la normativa statunitense e quella dell'Unione Europea.

A tutto ciò si aggiunga un'ulteriore considerazione: è vero che, finalmente, l'ordine esecutivo fa espresso riferimento al canone della proporzionalità, ma la sua concreta operatività pare già essere limitata *ex ante*. Infatti, si prevede che l'attività di intelligence sia ammessa solamente quando sia necessario procedere con questo strumento, ma non si richiede affatto che esso sia l'unico mezzo in astratto disponibile[51].

7. Un effettivo meccanismo di tutela giurisdizionale?

Nel quadro attuale, per come riformato, i cittadini dell'Unione Europea che ritenessero di aver subito una violazione dei propri dati personali devono rivolgersi al Garante della Privacy nel proprio Stato membro di appartenenza e sarà poi quest'ultimo a trasmettere tali reclami al Garante Europeo, *European Data Protection Board*, che li trasmetterà a sua volta alle competenti autorità statunitensi.

A questo punto, sull'altra sponda dell'Oceano, in ragione dell'Executive Order 14086 entra in azione un sistema di controllo giudiziario per tali violazioni disegnato in due tempi, che prende il nome di *redress*. Un primo vaglio è affidato al *Civil Liberties Protection Officer of the Office of the Director of National Intelligence* (CLPO), istituito dalla sezione 103D del *National Security Act* del 1947[52]. Si tratta di un soggetto nominato dal *Director of National Intelligence* e che riferisce direttamente allo stesso delle eventuali violazioni riscontrate[53]. Per assicurargli il requisito dell'indipendenza si prevede, però, che il predetto direttore non debba interferire in questa attività di *redress* e che possa

[50] Sulla differenza tra bilanciamento e proporzionalità cfr. V.A. Da Silva, *Balancing may be everywhere, but the proportionality test is not*, in *Global Constitutionalism*, 2023, p. 1 ss.

[51] EO 14086, Sec. 2, (a) (ii) (A) «signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority».

[52] 50 U.S.C. 3029.

[53] 50 U.S.C. 3029, Sec. 103D: «within the Office of the Director of National Intelligence, there is a Civil Liberties Protection Officer who shall be appointed by the Director of National Intelligence. (2) The Civil Liberties Protection Officer shall report directly to the Director of National Intelligence».

rimuovere il CLPO solamente in casi di suo grave inadempimento, o di incapacità sopravvenuta[54].

Il secondo livello di tutela è invece affidato ad una corte: la *Data Protection Review Court* (DPRC)[55], regolamentata da un provvedimento del Dipartimento di Giustizia[56]. Essa è composta da sei giudici nominati dall'Attorney General previo parere del Secretary of Commerce, dell'Office of the *Director of National Intelligence* e del *Privacy and Civil Liberties Oversight Board*, scelti tra persone che non siano membri del Governo degli Stati Uniti. Questa corte è affiancata nel suo lavoro da due *Special Advocates*, soggetti abilitati al patrocinio legale ed esperti nel settore della privacy. In modo speculare a quanto previsto per il *Civil Liberties Protection Officer* si prevede a garanzia dell'indipendenza di costoro che essi non siano sottoposti alla direzione ed al controllo dell'*Attorney General* e che possano essere destituiti dal loro incarico solo in presenza di ipotesi eccezionali quali, ad esempio, la sopravvenuta incapacità, eventuali gravi inadempimenti nell'espletamento del loro incarico o la commissione di atti illeciti[57].

Si tratta quindi di una corte che, per quanto non rientri nell'Articolo 3 della Costituzione statunitense, dovrebbe comunque essere connotata dal carattere dell'indipendenza. A differenza di quanto avveniva con il precedente *Ombudsperson*, istituito dal *Privacy Shield*, è bene notare che i soggetti che svolgono questo *redress* possono essere rimossi solamente in casi di effettiva negligenza o di incapacità a svolgere il mandato loro affidatogli. Sicché questo dato sembrerebbe poter allora costituire un nuovo e vero elemento di indipendenza.

Quanto al procedimento, e sul piano probatorio, è poi bene osservare come l'*Executive Order 14086*[58] non richieda alla parte ricorrente l'effettiva e dettagliata dimostrazione dell'asserita violazione da parte delle autorità di sicurezza nazionale, ma è altresì sufficiente che tale pretesa sia circostanziata[59]. Di tutta evidenza, infatti, assoggettare il ricorrente ad un simile onere probatorio sarebbe eccessivo e vedrebbe di fatto ampiamente vanificato ogni intento di tutela.

---

[54] EO 14086 §3(c)(iv).

[55] I primi componenti di questa corte sono stati nominati 14 novembre 2023 nelle persone di: James E. Baker, Rajesh De, James X. Dempsey, Mary B. DeRosa, Thomas B. Griffith, Eric H. Holder Jr., David F. Levi, e Virginia A. Seitz.

[56] 28 CFR § 201.

[57] 28 CFR §201.9(g).

[58] EO 14086, Sec. 4 (k).

[59] L'Ordine Esecutivo in esame precisa, infatti che devono essere opportunamente allegate dal ricorrente una serie di elementi affinché il reclamo sia ammissibile tra i quali, ad esempio, le ragioni in base alle quali costui ritiene sussistente una violazione (senza però la necessità di allegare e dimostrare una vera e propria prova del fatto che questi dati sono stati impiegati dall'intelligence statunitense nell'espletamento delle sue attività), nonché le modalità con cui si ritiene che i dati personali siano stati trasmessi agli Stati Uniti e le autorità governative degli Stati Uniti che si ritengono coinvolte nella pretesa violazione (EO 14086, Sec. 5(k) (ii)).

È allora qui bene notare come un simile meccanismo non possa andare esente da alcuni rilievi. Se è vero, infatti, che è sufficiente una pretesa circostanziata per aversi un reclamo ammissibile non è però altrettanto chiaro che cosa si debba intendere per "circostanziata". Sarà, ad esempio, sufficiente affermare genericamente che i dati violati erano contenuti nella propria casella di posta elettronica, o sarà, piuttosto, necessario indicare nel dettaglio anche le ragioni per cui si sarebbe avuta una tale violazione?

Di fatto in questo scenario sia il *Civil Liberties Protection Officer* sia la *Data Protection Review Court* potrebbero trovare ampi spazi di discrezionalità.

Inoltre, quanto al fatto che tali organi di tutela non sarebbero propriamente riconducibili al potere giudiziario federale di cui all'articolo 3 della Costituzione statunitense, è da notare come tale circostanza parrebbe essere un falso problema. Se è vero, infatti, che la Corte di Giustizia europea richieda alte garanzie di terzietà ed imparzialità per la figura che sarà preposta all'esercizio della giurisdizione in materia di dati personali, nulla dice, però, nel dettaglio sul fatto che ad assolvere tale ruolo debba essere per forza un'istituzione giudiziaria di cui all'articolo 3 della Costituzione USA né avrebbe ragione di farlo. Sarà, infatti, sufficiente che tali organi soddisfino concretamente gli standard e le previsioni riconosciute in materia di terzietà ed imparzialità dell'organo giudicante.

Si noti, inoltre, come tale impostazione porti con sé anche un ulteriore vantaggio. Invero qualora si riconducessero le funzioni di tali organi di garanzia all'alveo dell'articolo 3 della Costituzione USA ne conseguirebbe, in capo al ricorrente, l'onere di provare l'aver subito un danno concreto, attuale e dimostrabile[60], come puntualizzato dalla celebre decisione della Corte Suprema *Clapper v. Amnesty International USA*[61]. Diversamente, invece, se ponessimo la questione delle garanzie di terzietà e indipendenza dell'organo di giudizio senza ricondurle per forza alla predetta ipotesi costituzionale, potremmo comunque immaginare di vederle soddisfatte dalla secolare cultura istituzionale del sistema giuridico statunitense, senza però aggravare il ricorrente di un onere probatorio che facilmente potrebbe tradursi in un più difficile accesso alla giustizia.

Sul punto è poi bene notare che, sempre con riguardo al tema dell'accesso alla giustizia ed in particolare per ciò che concerne le persone fisiche, lo schema disegnato dal *redress* lo facilita sensibilmente dal momento che tale procedimento si apre direttamente dinnanzi ai garanti dei singoli stati membri dell'Unione, sicché per il cittadino questo è certamente un vantaggio.

Tuttavia, nonostante quanto di positivo abbiamo sin qui evidenziato, va però segnalato che nel momento in cui gli organi di garanzia europei trasmetteranno le istanze ai summenzionati organi di garanzia statunitensi, questi procederanno per il

[60] *Ibidem*, Opinion of the Court, p. 10 «to establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challanged action; and redressable by a favorable ruling».

[61] 568 U.S. 398 (2013).

tramite di una risposta standard, ma vincolante, che afferma semplicemente che «non è stata ravvisata una qualche violazione al trattamento dei dati personali o che comunque se è stata ravvisata vi è stato posto rimedio»[62]. È dunque questo il punto più fragile di tutto l'iter: i ricorrenti non otterranno una specifica risposta nel merito della loro istanza e dunque non sapranno se effettivamente sono stati controllati o meno dai servizi segreti, ma riceveranno, invece, una generica comunicazione standardizzata e sempre uguale[63]. Sembra, dunque, questo il punto in cui le speranze di tutela e trasparenza si infrangono di fronte alle esigenze di tutela della sicurezza nazionale[64].

8. Tutto cambia affinché tutto resti uguale?

Sarebbe sbagliato affermare che la nuova normativa statunitense non abbia alcun carattere di novità rispetto alla precedente regolamentazione. Se infatti il *Privacy Shield* sembrava una mera replica del *Safe Harbor Framework*, oggi la normativa che stiamo esaminando presenta senz'altro molteplici tratti di innovazione, a riprova dell'evidente volontà dell'amministrazione statunitense di andare incontro alle richieste della Corte di Giustizia europea. Forse anche perché, nel periodo successivo alla pronuncia *Schrems II* che aveva cassato la decisione di adeguatezza ai sensi dell'articolo 45 GDPR, il trasferimento dei dati personali tra Stati Uniti e Unione Europea ricadeva necessariamente nel più complesso e meno agile operare degli articoli 46 e seguenti GDPR. In quel frangente, infatti, molto spesso si procedeva in base alle *Standard Contractual Clauses* (SCCs)[65] cioè a clausole che possono essere

[62] EO 14086 §3(c)(i)(E)(1): «review either did not identify any covered violations or the CLPO issued a determination requiring appropriate remediation»; EO 14086 §3(d)(i)(H) «the review either did not identify any covered violations or the [DPRC] issued a determination requiring appropriate remediation».

[63] Department of Justice – Office of the Attorney General – 28 CFR Part 201: «individual complainants will not be informed whether they were subject to signals intelligence activities, but instead will receive a standardized notice that states that the DPRC's review has been completed and either did not identify any covered violations or the DPRC issued a determination requiring any appropriate remediation».

[64] Si rileva poi come in realtà questa motivazione possa essere fornita in un momento successivo laddove le esigenze di sicurezza nazionale lo consentano (EO 14086 § 3(d)(v): «within 5 years of the EO and at least every 5 years thereafter, Commerce will contact the relevant element(s) of the Intelligence Community regarding whether information pertaining to the review of a complaint by the CLPO or DPRC has been declassified, and if so, notify the complainant through the public authority that such information may be available under applicable law»).

[65] Con la Decisione di esecuzione della Commissione Europea 2021/914 del 4 giugno 2021 sono state adottate delle nuove SCCs. Inoltre, in *Schrems II* la Corte di Giustizia aveva precisato come le Standard Contractual Clauses impongano comunque sempre a chi se ne avvale di garantire che nello stato terzo via sia un livello di protezione dei dati personali essenzialmente equivalente allo standard vigente nell'Unione Europea (cfr. Corte giust., 16 luglio 2020, C- 559/20, *Schrems II*, par. 124 ss.)

volontariamente inserite nei contratti e che garantiscono la conformità del trattamento dei dati personali al GDPR[66]. Queste clausole dovevano però essere obbligatoriamente precedute dal DPIA (*Data Protection Impact Assessment*), un documento indicante esattamente quali erano i possibili rischi connessi al trattamento dei dati personali e che doveva contenere anche la cosiddetta TIA (*Transfer Impact Assessment*)[67]. Quest'ultima consiste in una valutazione d'impatto relativa all'adeguatezza della protezione dei dati personali nel paese terzo presso il quale i dati medesimi verranno esportati. Insomma, in questi casi il trasferimento dei dati personali risultava, invero, tutt'altro che agevole[68].

Si comprende allora forse così, alla luce di questo accidentato percorso di cui agli articoli 46 e seguenti GDPR gli sforzi dell'amministrazione statunitense per cercare di tornare ad operare in seno all'articolo 45 GDPR.

È dunque nella prospettiva della recente storia che abbiamo sin qui ripercorso, ovvero quella delle difficoltà di mutuo riconoscimento dei livelli di garanzia offerti sulle due sponde dell'Atlantico, che occorre allora domandarsi se oggi il Data Privacy Framework sia finalmente in grado di garantire livelli di protezione dei dati personali equiparabili tra Stati Uniti e Unione Europea, alla luce della Carta di Nizza e delle indicazioni offerte dalla Corte di Giustizia[69].

In particolare, parrebbe essere ancora problematico l'ampio margine di intervento che viene comunque garantito all'intelligence statunitense dal momento che neppure l'*Executive Order 14086* sembra costituire un effettivo tentativo di limitazione degli ampi margini tradizionalmente lasciati all'intelligence. Parrebbe, infatti, che si sia scelto di procedere indicando un novero di ipotesi in cui l'intervento dell'intelligence sarebbe ammesso, ma a ben vedere tale scelta sembra essere tutt'altro che limitante, conservando in realtà tratti piuttosto ampi e discrezionali a favore dell'intelligence. Inoltre, come abbiamo già detto, anche con riguardo alla questione del criterio di proporzionalità va qui ricordato che nella tradizione giuridica statunitense il concetto si è sviluppato in modo diverso da quanto non sia avvenuto nel paradigma europeo.

---

[66] Invero non si tratta delle uniche modalità alternative alla decisione di adeguatezza della Commissione Europea. Infatti, l'art. 46 GDPR prevede non soltanto le SCCs, ma anche le cosiddette BCRs (Binding Corporate Rules), i codici di condotta ed un apposito meccanismo di certificazione. Inoltre, l'art. 49 GDPR individua delle ipotesi eccezionali in cui il trasferimento dei dati personali verso Stati terzi è possibile pur in assenza delle modalità previste dagli artt. 45 e 46 GDPR.

[67] M. Corrales Compagnucci – M. Aboy – T. Minssen, *Cross – BorderTransfers of Personal Data After Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, in *Nordic Journal of European Law*, 2021, p. 42 ss.

[68] Sull'impatto della pronuncia *Schrems II* cfr. J.X. Dhont, *Schrems II. The EU Adequacy Regime in Existential Crisis*, in *Maastricht Journal of European and Comparative Law*, 2019, p. 597 ss.; N. Singh, *Schrems II: Impact on International Exchange of Personal Data*, in *Indian Journal of Law and Legal Research*, 2023, p. 1 ss.; D. Calia, *Schrems II: The EU's Influence on U.S. Data Protection and Privacy Laws*, in *Washington University Global Studies Law Review*, 2022, p. 247 ss.

[69] Sul punto cfr. C-311/18, 180 ss.

Ritornando poi sulla questione delle garanzie di terzietà ed imparzialità offerte dagli organi statunitensi, per quanto riguarda la possibilità che questi soddisfino o meno i requisiti di cui all'articolo 47 della Carta di Nizza[70], è bene ricordare come la Corte di Giustizia abbia più volte posto l'accento proprio sulla questione dell'indipendenza, rimarcando come tale principio si ponga quale fondamento irrinunciabile del diritto europeo. Si pensi, ad esempio, alla pronuncia del 2019, Commissione Europea contro Repubblica di Polonia[71] nella quale la Corte ha precisato che tale requisito si compone di due caratteri, dove il primo consta nell'esigenza di fornire delle idonee garanzie al potere giudiziario, quali l'inamovibilità dei giudici, e dove il secondo, invece, fa riferimento all'imparzialità dei giudicanti[72].

Ovviamente l'affermazione di tali principi non può che trovare applicazione anche con riguardo alle vicende che stiamo analizzando, dove entrambi i requisiti sembrerebbero trovare affermazione. Per quanto riguarda infatti sia il *Civil Liberties Protection Officer* sia la *Data Protection Review* Court possiamo certamente ritenere che siano a tutti gli effetti indipendenti, dal momento che come dicevamo non possono essere rimossi, se non per giusta causa (incapacità sopravvenuta o grave negligenza nell'espletamento del proprio mandato). Inoltre, il fatto che il loro incarico abbia una durata considerevole, seppur non sia a tempo indeterminato, sembrerebbe concorrere alle garanzie della loro indipendenza.

Più delicato è invece il fatto che questi organi non si pronuncino nello specifico del caso e con una vera motivazione, ma si limitino, semmai, ad una risposta standard. Il dubbio riguarda dunque proprio questo tipo di pronuncia che in molto differisce dai caratteri che siamo soliti riconoscere alle pronunce di un organo giudicante. Sembrerebbe, quindi, che una tale scelta costituisca ancora una volta una sorta di paravento per l'operare dell'intelligence, dal momento che attraverso una non risposta si assolve un obbligo procedurale, ma di fatto si prescinde dal merito.

9. Conclusioni

Dopo che due diversi tentativi di regolamentazione del trasferimento dei dati personali tra le due sponde dell'Atlantico sono venuti meno, in seguito ai rilievi della Corte di Giustizia Europea, il Data Privacy Framework è oggi chiamato a sostituire e correggere tali tentativi di normazione. Le note pronunce *Schrems I* e *II* avevano, infatti, rivelato con chiarezza la ripetuta antinomia tra i formanti del diritto europeo[73],

[70] A. Rosanò, *La nozione di tribunale costituito per legge nella giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di Giustizia dell'Unione Europea: considerazioni alla luce di alcune recenti sentenze*, in *Rivista Eurojus*, 2021, p. 48 ss.

[71] Corte giust., 5 novembre 2019, C - 192/18, *Commissione Europea contro Repubblica di Polonia*.

[72] *Ibidem*, par. 108 ss.

[73] R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law, Install. I-II*, in *American Journal of Comparative Law*, 1991, p. 1 ss.

dal momento che ciò che la Corte ha poi cassato era stato in precedenza, e per ben due volte, creato e avallato proprio dalla Commissione. In altre parole, quegli standard di protezione dei dati personali che alla Corte sono risultati inadeguati erano, invece, sembrati sufficienti alla Commissione, con tutto ciò che questo comporta per una riflessione in termini di politica del diritto e coerenza di un sistema.

È allora in questo contesto che si inserisce il *Data Privacy Framework*, chiamato a sostituire e migliorare la regolamentazione del trasferimento dei dati personali verso gli Stati Uniti proprio alla luce dei rilievi della Corte. Non vi è infatti alcun dubbio che, nel disporre questo ulteriore tentativo di regolamentazione, gli Stati Uniti abbiano fatto qualche sforzo in più, rispetto al passato, per adeguare la loro legislazione interna agli impulsi e alle indicazioni della Corte di Giustizia Europea; tuttavia, come qui osservato, restano invero diversi i punti ancora aperti e forse tuttora distanti dai rilievi della Corte[74].

Sembra così potersi affermare che, ad oggi, il margine di discrezionalità di intervento concesso all'intelligence statunitense sia ancora piuttosto ampio e pertanto lontano dal soddisfare gli standard dell'Unione. Quanto poi al modus operandi del nuovo meccanismo di *redress*, introdotto nell'ordinamento statunitense attraverso l'*Executive Order 14086* proprio al fine di avere un implemento di garanzie nel trattamento dei dati personali, dobbiamo rilevare come tale meccanismo non sembri però davvero capace di garantire un giudice, il cui operato sia rendicontabile, davvero terzo ed imparziale per come tali concetti sono tradizionalmente interpretati dall'*acquis* del diritto comunitario.

A tutto ciò si aggiunga, infine, che l'atteggiamento assunto dalla Corte di Giustizia potrebbe però anche sembrare ambiguo sulle due sponde dell'Atlantico. Se è infatti vero, come abbiamo sin qui visto, che la Corte vaglia nel merito l'adeguatezza o meno delle garanzie offerte dai paesi extraunionali rispetto agli standard del diritto europeo, è però altrettanto vero che lo stesso rigoroso controllo non avviene nei confronti degli Stati membri dell'Unione, dal momento che la sicurezza nazionale è materia rimessa ai singoli stati.

Di certo, la maggiore attenzione riservata al trasferimento dei dati al di fuori dell'Unione è il doveroso tentativo di proteggere i cittadini europei in quello che è un diritto fondamentale, che si assume invece come pienamente garantito all'interno dell'Unione grazie al GDPR.

---

[74] Invero l'avvocato ed attivista Max Schrems ha già affermato di voler agire in giudizio per far dichiarare invalido il Data Privacy Framework, sul punto cfr. M. Barczentewics, *Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States*, in *International Center for Law & Economics*, Issue Brief, 2023, p. 4 ss. Inoltre il parlamentare francese Philippe Latombe ha adito la Corte di Giustizia per far dichiarare invalido il Data Privacy Framework. Sul punto la Corte con l'ordinanza del 12 ottobre 2023 (T – 553/23 R) ha rigettato il suo ricorso proposto ex artt. 278 e 279 TFUE poiché non è stato ritenuto provato il requisito dell'urgenza. La Corte, dunque, non si è così dovuta pronunciare sul merito della domanda.

Non si può però non notare, in conclusione, come questo doppio regime rischi di far apparire, al di fuori dei suoi confini, l'Unione europea, come una sorta di Giano bifronte: rigorosa e zelante paladina dei diritti all'esterno, ma non altrettanto equipaggiata nei confronti dei suoi stessi Stati membri. È dunque alla luce di tutto ciò che resta ad oggi legittimo domandarsi se il Data Privacy Framework sia davvero una risposta definitiva o se, al pari dei suoi precedenti, sarà anch'esso rimesso in discussione dalla Corte.

***

Abstract: The transfer of personal data between the United States and the European Union is now regulated by the Data Privacy Framework, a new agreement between the two sides, which facilitates data transfers across the Atlantic. In light of this, the European Commission, in its adequacy decision, considered the US data protection regime as substantially equivalent to the EU regime in terms of protection of the rights of data subjects. The aim of this contribution is, from a comparative perspective, to analyse the content of this decision in an attempt to predict whether it will actually be decisive or whether it will fall, like its predecessors, under the axe of the Court of Justice of the European Union.

Keywords: Data Privacy Framework - comparative law – right to privacy - transfer of personal data – balancing

***

Vittoria Margherita Sofia Trifiletti – Dottoranda in Diritto comparato presso l'Università degli Studi di Torino(vittoriamargheritasofia.trifiletti@unito.it)