INSIGHT

VERSO *SCHREMS III*? ANALISI DEL NUOVO *EU-US DATA PRIVACY FRAMEWORK*

MARIA GIACALONE*

ABSTRACT: The *Insight* aims to analyse whether the Executive Order 14086 of 7 October 2022, signed by the President of the United States following the achievement of the so-called EU-US Data Privacy Framework, has addressed the requirements emerging from the Court of Justice's ruling in the case *Schrems II* (case C-311/18). It further aims to assess whether, as claimed by the European Commission, the US effectively ensures a level of data protection "essentially equivalent" to that guaranteed in the EU by Regulation 2016/679 (GDPR).

KEYWORDS: data protection – Data Privacy Framework – *Schrems II* – art. 52 CDFUE – art. 47 CDFUE – GDPR.

I. INTRODUZIONE

Il 25 marzo 2022, dopo quasi due anni di contrattazione, il Presidente degli Stati Uniti e la Presidente della Commissione europea hanno annunciato il raggiungimento del c.d. *EU-US Data Privacy Framework*, un accordo volto ad apporre delle modifiche sostanziali alla legislazione statunitense al fine di renderla compatibile con i requisiti stabiliti dalla Corte di Giustizia nella sentenza del 2020 *Schrems II*[1] e, così facendo, favorire i flussi di dati tra l'Unione e gli Stati Uniti.

A seguito dell'accordo, il presidente Biden ha firmato il nuovo *Executive order* 14086 (*Enhancing Safeguards for United States Signals Intelligence Activities*)[2] il quale mira a rafforzare la tutela della privacy e delle libertà civili applicabili alle attività di intelligence degli Stati Uniti. La Commissione europea, sostenendo che le innovazioni della legislazione statunitense costituiscono una protezione "sostanzialmente equivalente" a quella accordata dall'UE, il 13 dicembre 2022 ha presentato la *Draft Adequacy Decision for the EU-US*

*Dottoranda, Sapienza Università di Roma, maria.giacalone@uniroma1.it.

[1] Causa C-311/18 *Data Protection Commissioner c Facebook Ireland Limited e Maximillian Schrems* ECLI:EU:C:2020:559 (di seguito *Schrems II*)

[2] The White House, *Fact sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework,* in www.whitehouse.gov.

ISSN 2499-8249
doi: 10.15166/2499-8249/644

Data Privacy Framework[3] con cui ha dato avvio alla procedura[4] di adozione della definitiva decisione di adeguatezza.[5]

Il contributo intende analizzare come l'*Executive order 14086* è intervenuto sulle violazioni lamentate dalla Corte di giustizia nella sentenza *Schrems II* e verificare se, come sostiene la Commissione europea, gli Stati Uniti garantiscono effettivamente un livello di tutela di protezione dei dati "sostanzialmente equivalente"[6] a quello garantito nell'UE dal Regolamento 2016/679 (GDPR) letto alla luce della Carta dei diritti fondamentali dell'Unione europea. È opportuno sottolineare che l'analisi viene svolta su documenti preliminari che, tuttavia, costituiscono la base del futuro accordo e della relativa normativa in materia.

La struttura del *Draft* ricalca essenzialmente quella delle due precedenti decisioni di adeguatezza. Come nel caso del *Safe Harbour*[7] e del *Privacy Shield*,[8] anche la nuova deci-

[3] Commissione europea, *Draft Adequacy Decision for the EU-US Data Privacy Framework* www.commission.europa.eu. Per un maggiore approfondimento, la Commissione ha prodotto un breve Q&A che offre maggiori dettagli sul suo progetto di decisione: Commissione europea, *Questions & Answers: EU-US Data Privacy Framework, Draft Adequacy Decision* www.ec.europa.eu.

[4] La Commissione ha presentato la bozza di decisione al Comitato europeo per la protezione dei dati (EDPB). Successivamente, la Commissione chiederà l'approvazione di un comitato composto da rappresentanti degli Stati membri dell'UE, il Parlamento europeo ha il diritto di controllo sulle decisioni di adeguatezza. Una volta completata la procedura, la Commissione potrà procedere all'adozione della decisione finale di adeguatezza.

[5] Una decisione di adeguatezza è uno strumento giuridico emesso dalla Commissione europea che stabilisce che un Paese extra UE fornisce un livello di protezione dei dati personali sostanzialmente equivalente al livello di protezione garantito all'interno dell'Unione europea. Ai sensi dell'art. 45 del GDPR, tale decisione è uno dei meccanismi che consentono il trasferimento di dati personali dall'UE a un Paese terzo senza la necessità di ulteriori garanzie. La decisione conferma che il Paese terzo garantisce un livello adeguato di protezione dei dati personali trasferiti e, pertanto, i trasferimenti di dati verso tale Paese non richiedono alcuna autorizzazione aggiuntiva o accordo specifico. La decisione di adeguatezza viene adottata dalla Commissione europea a seguito di una valutazione del quadro giuridico del Paese terzo, dell'accesso e dell'utilizzo dei dati personali e delle garanzie di protezione dei dati, tra gli altri fattori. Una volta emessa, la decisione di adeguatezza rimane in vigore finché non viene invalidata o annullata dalla Corte di giustizia.

[6] Il requisito dell'adeguatezza è stato introdotto nella direttiva 95/46 come meccanismo per permettere il trasferimento di dati personali verso Paesi extra UE che forniscono un livello adeguato di protezione. Il criterio è stato ripreso nel regolamento 2016/679. Tuttavia, a seguito soprattutto delle rivelazioni di Edward Snowden circa la sorveglianza di massa attuata dagli Stati Uniti, la Corte di giustizia nella sentenza *Schrems I* ha interpretato il requisito di adeguatezza in modo maggiormente rigoroso sostenendo che "la nozione di 'livello di protezione adeguato' deve essere intesa nel senso che essa richiede che il Paese terzo assicura, effettivamente, in forza del suo diritto interno o dei suoi impegni internazionali, un livello di tutela dei diritti e delle libertà fondamentali 'sostanzialmente equivalente' a quello garantito all'interno dell'UE in forza della direttiva 95/46, letta alla luce della Carta di Nizza": Causa C-362/14 *Maximillian Schrems c Data Protection Commissioner* ECLI:EU:C:2015:650 (di seguito *Schrems I*) par. 73. L'interpretazione restrittiva è stata confermata in *Schrems II* cit.

[7] Decisione della Commissione 2000/520/CE 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.

[8] 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.

sione di adeguatezza presenta un sistema di certificazione: i titolari e responsabili del trattamento potranno autocertificare la loro adesione a una serie di principi[9] al fine di poter ricevere e trattare i dati provenienti dall'UE.[10] Tali principi presentano una struttura molto analoga a quelli del *Privacy Shield*, tuttavia, le modifiche intervenute mirano ad avvicinarli a quelli enunciati dal GDPR.

Il punto del *Draft* che merita maggiore attenzione è quello dedicato all'accesso e utilizzo dei dati personali da parte delle autorità pubbliche statunitensi per scopi di sicurezza nazionale.[11] Questo profilo, infatti, ha costituito la questione centrale sulla quale poggia l'intera vicenda Schrems.[12]

Difatti, nella sentenza del 2020 la Corte di Giustizia ha invalidato la decisione di adeguatezza della Commissione 2016/1250 (c.d. *Privacy Shield*)[13] per l'incompatibilità con l'art. 45 (1) GDPR,[14] letto alla luce degli art. 7, 8 e 47 della Carta di Nizza.[15]

La decisione della Corte si articola in due profili:

- il mancato rispetto del principio di proporzionalità *ex* art. 52 della Carta di Nizza in quanto i programmi di intelligence statunitensi permettevano una sorveglianza governativa ingiustificatamente ampia. La Corte di giustizia ha quindi accertato che l'ingerenza nei diritti fondamentali di cui agli art. 7 e 8 della Carta non fosse necessaria e proporzionata rispetto alle esigenze di sicurezza nazionale;

- la violazione dell'art. 47 della Carta poiché, in relazione a tale sorveglianza statunitense, gli interessati europei non disponevano del diritto a un ricorso effettivo dinnanzi a un giudice indipendente e imparziale.

È bene esaminare per prime le questioni attinenti al principio di proporzionalità per passare, successivamente, a quelle che concernono i diritti al ricorso effettivo.

[9] Per poter ottenere la certificazione un'organizzazione deve essere soggetta ai poteri di indagine e di applicazione della *Federal Trade Commission* (FTC) o del Dipartimento dei Trasporti degli Stati Uniti. I principi troveranno applicazione immediatamente dopo la certificazione. Come viene spiegato nei punti 47-51, le società dovranno certificare la loro aderenza ai principi annualmente.

[10] Si veda a questo proposito *Schrems II* cit. par. 81, in cui la Corte di giustizia ha confermato che un sistema di autocertificazione può garantire un livello di protezione adeguato.

[11] *Draft Adequacy Decision for the EU-US Data Privacy Framework,* par. 3.2.

[12] Occorre ricordare come la sentenza *Schrems I* ha avuto origine dalle preoccupazioni sollevate dal sig. Schrems in seguito alle dichiarazioni effettuate nel 2013 da Edward Snowden circa la sorveglianza di massa attuata dagli Stati Uniti attraverso i programmi di intelligence della NSA: cfr. *Schrems I* cit. par. 28.

[13] Decisione di esecuzione (UE) 2016/1250 cit.

[14] L'art. 45 GDPR, rubricato "Trasferimento sulla base di una decisione di adeguatezza", al par. 1 stabilisce "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche".

[15] *Schrems II* cit. par. 199.

II. Art. 52 della Carta dei diritti fondamentali dell'Unione europea

Con riferimento al principio di proporzionalità, l'*Executive order 14086* ribadisce il principio, già presente nel *Privacy Shield*, del primato delle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia, in forza del quale le società statunitensi che ricevono dati dall'Unione europea sono tenute a disapplicare l'accordo allorché questo interferisca con tali esigenze.[16] Tuttavia, a differenza del precedente accordo, l'*Executive order* prevede una serie di obiettivi legittimi che giustificano le attività di intelligence e un elenco di casi in cui invece suddette attività sono proibite.[17] Vi sono, dunque, delle migliorie rispetto al *Privacy Shield*.

Ciononostante, la Corte di giustizia ha più volte indicato che, in ossequio all'art. 52 della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea devono essere previste dalla legge e devono rispettare il contenuto essenziale di detti diritti e libertà; inoltre, tali limitazioni possono essere apportate solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dell'UE o all'esigenza di proteggere i diritti e le libertà altrui.[18]

Tra i criteri enunciati dall'art. 52 della Carta, il nuovo *Executive order* presenta maggiori criticità con riferimento alla previsione per legge della limitazione al diritto fondamentale e il rispetto del contenuto essenziale dei diritti e delle libertà enunciate dalla Carta.

Quanto al primo criterio, dalla giurisprudenza della Corte[19] emerge come la base giuridica dell'ingerenza nel diritto fondamentale deve essere chiara, precisa e prevedibile. Nel testo dell'*Executive Order*, gli obiettivi legittimi che giustificano le attività di *intelligence* hanno una formulazione generica che ne permette un'interpretazione altrettanto ampia,[20] dunque, è lecito dubitare della chiarezza e precisione della limitazione; in aggiunta

[16] Parte I Punto 5 dell'Allegato III alla decisione 2016/1250 cit., rubricato "Principi del regime dello scudo Unione europea-Stati Uniti per la privacy".

[17] Presidente degli Stati Uniti, *Executive Order* 14086 del 7 ottobre 2022 *Enhancing Safeguards for United States Signals Intelligence Activities*, Federal Register, vol. 87, n. 198, 2022, Sec. 2 (i), 62283.

[18] Art. 52 (1) Carta dei diritti fondamentali dell'Unione europea; in tal senso v. *Schrems II* cit., par. 174; parere 1/15 (Accordo PNR UE-Canada), EU:C:2017:592, par. 139; cause riunite C-203/15 e C-698/15 *Tele2 Sverige AB c Post- och telestyrelsen e Secretary of State for the Home Department contro Tom Watson e altri* ECLI:EU:C:2016:572, conclusioni dell'AG Saugmandsgaard Øe, par. 137-154; causa C-70/10 *Scarlet Extended SA c Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* ECLI:EU:C:2011:255, par. 88-114; causa C-62/14 *Peter Gauweiler e altri c Deutscher Bundestag* ECLI:EU:C:2015:400, par. 67; causa C-331/88 *The Queen c The Minister of Agriculture, Fisheries and Food e The Secretary of State for Health, ex parte: Fedesa e altri* ECLI:EU:C:1990:391, par. 13.

[19] Cause riunite C-293/12 e C-594/12 *Digital Rights Ireland Ltd c Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri* ECLI:EU:C:2014:238 para. 58 (di seguito *Digital Rights Ireland*); cause riunite C-203/15 e C-698/15 *Tele2 Sverige AB c Post- och telestyrelsen e Secretary of State for the Home Department c Tom Watson e altri* ECLI:EU:C:2016:970 par. 111-112 (di seguito *Tele2*); *Schrems II* cit. par. 180-181.

[20] A titolo esemplificativo: "understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat

non può dirsi soddisfatto neppure il requisito della prevedibilità dell'applicazione della misura poiché nell'*Executive order 14086* è indicato come tali obiettivi possano essere modificati e integrati dal Presidente in caso di minaccia alla sicurezza nazionale.[21]

Un altro nodo problematico è dato dal fatto che nell'*Executive Order* è chiaramente indicato che lo stesso non sarebbe intervenuto sulla normativa vigente, o meglio, sarebbe intervenuto unicamente sulla *Presidential Policy Directive 28*,[22] lasciando invariata sia la sez. 702 *Foreign Intelligence Surveillance Act* (FISA)[23] sia *l'Executive Order 12333*,[24] disposizioni già valutate negativamente dalla Corte di giustizia. In effetti, sia nella sentenza *Schrems II* che nella sentenza *Schrems I*, la Corte ha concluso che tale normativa non "corrisponde ai requisiti minimi connessi, nel diritto dell'Unione, al principio di proporzionalità"[25] poiché dette disposizioni, che consentono ingerenze nei diritti fondamentali, non definiscono la portata della limitazione all'esercizio del diritto fondamentale *ex* art. 7 e 8 della Carta e non prevedono norme chiare e precise che regolino la portata e l'applicazione della misura.

Con riferimento al rispetto del contenuto essenziale dei diritti, sebbene non vi sia una giurisprudenza cospicua per quanto riguarda le condizioni in cui l'essenza di un diritto viene intaccata,[26] si può sostenere che ciò si verificherebbe se la limitazione si spingesse a tal punto da svuotare il diritto dai suoi elementi fondamentali e impedirne, dunque,

to the national security of the United States or of its allies or partners; protecting against foreign military capabilities and activities; protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person" (*Executive Order 14086* cit. 62284).

[21] *Ibid*. 62284.

[22] La *Presidential Policy Directive 28* (Presidente degli Stati Uniti, *Presidential Policy Direcrive 28* (PPD-28) del 17 gennaio 2014, *Signals Intelligence Activities*) è una direttiva del Presidente degli Stati Uniti che stabilisce la politica per la sorveglianza dei cittadini stranieri al di fuori degli Stati Uniti. La PPD-28 è stata emessa nel 2014 dall'allora Presidente Obama per stabilire criteri più rigorosi per la raccolta, l'uso e la conservazione delle informazioni raccolte dalle agenzie di intelligence statunitensi sui cittadini stranieri al di fuori degli Stati Uniti. La direttiva è stata creata per restringere l'utilizzo di dati raccolti attraverso la sorveglianza di massa e per garantire che le operazioni di intelligence siano condotte in modo conforme alla legge e ai principi di libertà e giustizia.

[23] Sezione 702 del *Foreign Intelligence Surveillance Act* (FISA) 50 U.S.C. § 1881a *Authorization of Program for Acquisition of Foreign Intelligence Information,* introdotta con *FISA Amendments Act* del 2008. La sez. 702 del FISA consente alle agenzie federali statunitensi di raccogliere informazioni sui soggetti esteri sospettati di attività di intelligence o di terrorismo. La disposizione è stata utilizzata per giustificare la raccolta di informazioni sui cittadini americani che comunicano con i soggetti esteri sospettati.

[24] Presidente degli Stati Uniti, *Executive Order 12333* del 4 Dicembre 1981, *United States intelligence activities*, vol. 46, 1981, 59941. L'*Executive Order* in questione stabilisce le politiche e le procedure per la raccolta, l'elaborazione, la conservazione e la disseminazione di informazioni raccolte dall'intelligence degli Stati Uniti. L'*Executive Order*, inoltre, stabilisce le responsabilità delle diverse agenzie governative per la gestione della raccolta e dell'utilizzo delle attività di intelligence ed è stato utilizzato come base legale per la sorveglianza di massa.

[25] *Schrems II* cit. par. 184.

[26] *Schrems I* cit. par. 94-95; *Digital Rights Ireland* cit. par. 39; *Tele2* cit. par. 123.

l'esercizio. Nella sentenza *Schrems I*, la Corte ha chiarito che "una normativa che consente alle autorità pubbliche di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche compromette l'essenza del diritto fondamentale al rispetto della vita privata, come garantito dall'art. 7 della Carta".[27]

Pertanto, seguendo il ragionamento della Corte, è la stessa raccolta in massa a non rispettare l'essenza dei diritti fondamentali in questione e, sebbene l'*Executive Order* prediliga la raccolta mirata, esso non esclude che la sorveglianza di massa possa comunque avvenire.

Ne consegue che, applicando i criteri di cui all'art. 52 della Carta, come interpretati dalla Corte di giustizia, alle modalità di accesso e utilizzo dei dati personali da parte delle autorità pubbliche statunitensi come riformate dall'*Executive Order*, si arriva alla conclusione che la sostanziale equivalenza rispetto ai requisiti del diritto europeo non viene raggiunta.

III. Art. 47 della Carta dei diritti fondamentali dell'Unione europea

Per quanto attiene all'art. 47 della Carta, il nuovo *Executive Order* istituisce un meccanismo di ricorso a due livelli: i cittadini UE potranno presentare reclamo al *Civil Liberties Protection Officer*, il quale emetterà una decisione che potrà essere appellata davanti alla *Data Protection Review Court*.[28]

Il *Civil Liberties Protection Officer* (CLPO) è incardinato nell'ufficio del Direttore della *National Intelligence*.[29] Il CLPO dovrà svolgere un'indagine preliminare indipendente sui reclami ricevuti, verificare se le garanzie dell'ordine esecutivo o altre leggi statunitensi in materia sono state violate e, nel caso, applicare le misure correttive appropriate,[30] tuttavia, non potrà comunicare al denunciante se esso è stato o meno oggetto di attività di *intelligence*.

La *Data Protection Review Court* (DPRC)[31] si compone di membri nominati dall'*Attorney General*, in consultazione con il Segretario e il Presidente del Dipartimento del commercio. I giudici in questione vengono scelti sulla base di specifiche qualifiche e possono essere licenziati unicamente per cause gravi. Al ricevimento della domanda di riesame, viene convocato un panel composto da tre giudici che dovranno valutare la decisione del CLPO. Nel giudizio, la DPRC è tenuta a nominare uno *special advocate*[32] – per il quale non vi è alcun requisito di indipendenza – che garantirà gli interessi del denunciante davanti alla Corte.

Rispetto al precedente meccanismo di mediazione vi sono miglioramenti significativi: a differenza del *Privacy Shield*, che non conteneva alcuna indicazione sulla vincolatività delle

[27] *Schrems I* cit. par. 94-95.

[28] *Executive Order* 14086 cit. 62290.

[29] *Ibid.*

[30] *Ibid.*

[31] Istituita grazie al titolo 28 *Code of Federal Regulations* (CFR) parte 201 che modifica i regolamenti del Dipartimento di giustizia.

[32] *Executive Order* 14086 cit. 62291.

decisioni del mediatore,[33] nell'*Executive Order* – e anche nella bozza di decisione di adeguatezza – viene sottolineata la vincolatività delle decisioni sia del CLPO che della Corte.

È però dubbio che tale nuovo meccanismo sia idoneo a garantire una tutela giurisdizionale effettiva sostanzialmente equivalente a quella assicurata dalla Carta di Nizza. Difatti, il meccanismo di ricorso previsto dall'*Executive Order* presenta delle criticità sia dal punto di vista dell'effettività del ricorso sia dal punto di vista delle garanzie di indipendenza del giudice.

Per quanto riguarda la prima criticità, la decisione della DPRC avrà ad oggetto la valutazione dell'attività svolta del CLPO a seguito del reclamo presentato dal titolare dei dati. In altre parole, la DPRC andrà a valutare la correttezza formale della procedura effettuata dal CLPO senza però riconoscere al ricorrente il diritto alla riparazione.[34] In particolare, il meccanismo previsto dall'*Executive Order* non dispone a favore dei ricorrenti il diritto di ottenere l'accesso, la ratifica o la cancellazione dei propri dati personali trattati dai servizi di intelligence o alcuna possibilità di chiedere il risarcimento dei danni,[35] come invece previsto nel contesto europeo dall'art. 82 GDPR.

Essendo il diritto ad una riparazione equa e proporzionata un requisito strutturale dell'art. 47 della Carta di Nizza in quanto volto ad assicurare l'effettività dei diritti individuali, è lecito dubitare del rispetto da parte del sistema statunitense del requisito della sostanziale uguaglianza al sistema europeo.

Con riferimento alla seconda criticità, la Corte di giustizia nella sua precedente giurisprudenza ha più volte indicato che la mancanza di indipendenza e imparzialità del giudice si verifica quando "le condizioni oggettive nelle quali è stato creato l'organo di cui trattasi e le caratteristiche del medesimo nonché il modo in cui i suoi membri sono stati nominati siano idonei a generare dubbi legittimi, nei singoli, quanto all'impermeabilità di detto organo rispetto a elementi esterni, in particolare rispetto a influenze dirette o indirette dei poteri legislativo ed esecutivo".[36] Il punto fondamentale che fa propendere per la non indipendenza della DPRC non è la nomina da parte dell'esecutivo – questione oramai risolta dalla Corte di giustizia, la quale nella recente sentenza *Getin Noble Bank S.A.*[37] ha indicato che il semplice fatto che un organo giudiziario comprenda un giudice nominato da un organo esecutivo non mette in discussione l'indipendenza e l'imparzialità di

[33] Il mediatore non aveva il potere di adottare decisioni vincolanti o di imporre rimedi effettivi, poteva unicamente formulare raccomandazioni per azioni correttive. Le decisioni del mediatore avevano natura puramente consultiva.

[34] In questo senso H Ruschemeier, 'Nothing new in the west? The executive order on US surveillance activities and the GDPR' (14 novembre 2022) European Law Blog www.europeanlawblog.eu.

[35] *Ibid.*

[36] Cause riunite C-585/18, C-624/18 e C-625/18 *A.K. c Krajowa Rada Sądownictwa e CP* e *DO c Sąd Najwyższy* ECLI:EU:C:2019:982 par. 172.

[37] Causa C-132/20 *BN e altri c Getin Noble Bank S.A.* ECLI:EU:C:2022:235 (di seguito *Getin Noble Bank*).

tale organo giudiziario[38] – ma la plausibile influenza da parte del potere esecutivo.[39] Sebbene nella bozza della decisione di adeguatezza venga sottolineata l'indipendenza della DPRC, quest'ultima è comunque incardinata nel potere esecutivo e non nel sistema giudiziario.[40] Alla luce di ciò, la DPRC non dispone dell'indipendenza di un organo giudiziario pienamente indipendente istituito ai sensi dell'art. 3 della Costituzione statunitense, bensì di un'indipendenza limitata che non soddisfa il test della sostanziale equivalenza. Utilizzando le parole del sig. Schrems, la soluzione proposta "non prevede un ricorso giudiziario, ma un organo di ricorso all'interno del ramo esecutivo che la CGUE ha ritenuto non solo sproporzionato ma anche una violazione dell'essenza dell'art. 47 della Carta, [...] l'approccio sembra essere meglio descritto come un *Ombudsperson Plus*".[41]

Un'altra argomentazione che supporta tale lettura è la dottrina del privilegio del segreto di Stato, confermata dalla Corte Suprema degli Stati Uniti nella recente sentenza *FBI c Fazaga*.[42] Con la sentenza in questione, i giudici statunitensi hanno ampliato il potere del governo degli Stati Uniti di invocare il segreto di stato nelle controversie riguardanti le attività di *intelligence* realizzate dalle proprie agenzie investigative. Qualora tale dottrina dovesse applicarsi alla *Data Protection Review Court* verrebbe resa in ultima analisi ancora più ardua la contestazione dei programmi di sorveglianza da parte dei soggetti europei interessati.

La sentenza in questione rende evidente la distanza tra la visione statunitense e la visione europea poiché, nonostante la disciplina del segreto di Stato rientri nell'ambito della sicurezza nazionale, che rimane di competenza degli Stati membri, l'Unione europea fornisce alcune indicazioni e requisiti in merito alla protezione di dati personali che possono essere interconnessi con le questioni di sicurezza nazionale. Ai sensi del GDPR,[43] qualsiasi trattamento di dati personali da parte delle autorità pubbliche per finalità di sicurezza nazionale deve essere soggetto a garanzie e limitazioni adeguate. Anche la

[38] *Getin Noble Bank* cit. para 132. In questo senso si veda anche E De Falco, 'Indipendenza della magistratura in Polonia: brevi note a margine della sentenza Getin Noble Bank S.A.' (5 ottobre 2022) I Post di AISDUE www.aisdue.eu.

[39] In questo senso la Corte di giustizia ha chiarito nella sentenza *Getin Noble Bank* che "è importante che i giudici si trovino al riparo da interventi o da pressioni esterne che possano mettere a repentaglio la loro indipendenza e la loro imparzialità. Le norme applicabili allo status dei giudici e all'esercizio delle loro funzioni di giudice devono, in particolare, consentire di escludere non solo qualsiasi influenza diretta, esercitata sotto forma di istruzioni, ma anche le forme di influenza più indiretta suscettibili di orientare le decisioni dei giudici riguardati, e devono dunque permettere di scongiurare il rischio della mancanza di un'immagine di indipendenza o di imparzialità, in tali giudici, che sia idonea a ledere la fiducia che la giustizia deve ispirare negli amministrati in una società democratica e in uno Stato di diritto".

[40] In questo senso, Risoluzione del Parlamento europeo P9_TA(2023)0204 dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati (2023/2501(RSP)).

[41] Noyb – European Center for Digital Rights*, Open Letter. Announcement of a New EU-US Personal Data Transfer Framework* www.noyb.eu.

[42] *Federal Bureau of Investigation et al. v. Fazaga et al.*, No. 20–828, 595 U.S. (2022) www.supremecourt.gov.

[43] Art. 23 (1) GDPR.

Corte di giustizia si è espressa in questo senso,[44] indicando che il diritto di accesso ai dati detenuti dalle autorità pubbliche costituisce un diritto fondamentale e, come tale, qualsiasi ingerenza a tale diritto non può essere generale, bensì deve essere interpretata in modo restrittivo e soggetta ad un esame rigoroso[45] così da garantire la conformità al diritto europeo. In generale, dunque, pur riconoscendo l'importanza della sicurezza nazionale e della protezione del segreto di stato, l'UE si impegna a salvaguardare la protezione dei dati personali che, nel contesto europeo, assurge a diritto fondamentale.

IV. Conclusioni

Alla luce dell'analisi svolta, nonostante gli sforzi e i notevoli cambiamenti occorsi nella legislazione statunitense, ad opinione di chi scrive, non può dirsi rispettato il requisito della sostanziale equivalenza alla normativa europea in materia, letta alla luce degli art. 7, 8 e 47 della Carta di Nizza.

Gli Stati Uniti non dispongono ancora di una legge federale sulla protezione dei dati ed il modello di regolazione rimane improntato all'aspetto economico e di sicurezza nazionale[46]. Sebbene l'instabilità giuridica circa i trasferimenti di dati personali tra Unione europea e Stati Uniti abbia generato importanti costi aggiuntivi ed oneri sia alle imprese europee che alle imprese statunitensi, la decisione di adeguatezza non può essere concessa se non per motivi giuridici. Allo stato attuale, non sembra di poter concludere che il processo di convergenza in atto tra i due sistemi sia in grado di soddisfare il requisito della sostanziale equivalenza stabilito dalla Corte di giustizia.

[44] Cause riunite C-37/20 e C-601/20 *WM c Luxembourg Business Registers* ECLI:EU:C:2022:91.

[45] *Ibid.* par. 39.

[46] Negli Stati Uniti vige un approccio di tipo utilitaristico dove i dati personali vengono qualificati come bene economico da poter vendere e comprare, pertanto, la privacy viene tutelata unicamente nell'ambito degli scambi commerciali.