BlogDUE

Gli ultimi sviluppi della saga sui trasferimenti di dati personali UE-USA: l'*Executive Order* firmato dal Presidente USA Biden il 7 ottobre 2022 e la proposta di decisione di adeguatezza presentata dalla Commissione UE il 13 dicembre 2022

Gabriele Rugani (Assegnista di ricerca post-dottorale in Diritto dell'Unione europea e Diritto internazionale – Università di Pisa) – 19 gennaio 2023

SOMMARIO: 1. Introduzione: i precedenti capitoli della saga, con l'annullamento di entrambe le decisioni di adeguatezza nei confronti degli USA. – 2. I tentativi per giungere all'adozione di una terza decisione di adeguatezza. – 3. L'*Executive Order* firmato dal Presidente USA Biden il 7 ottobre 2022. – 4. La proposta di decisione di adeguatezza presentata dalla Commissione UE il 13 dicembre 2022. – 5. Principali aspetti positivi e criticità dell'assetto che va delineandosi. – 6. Conclusioni: molti dubbi e un piccolo successo.

1. Negli ultimi mesi del 2022, la complessa vicenda riguardante i trasferimenti di dati personali tra Unione europea e Stati Uniti d'America ha vissuto due ulteriori, cruciali, sviluppi: il primo, datato 7 ottobre 2022, è la firma da parte del Presidente USA Joseph R. Biden Jr. dell'"*Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*"; il secondo, datato 13 dicembre 2022, è invece la proposta da parte della Commissione UE di una nuova decisione di adeguatezza da adottare nei confronti degli USA medesimi.

Per meglio comprendere l'importanza di tali momenti, è opportuno ricapitolare gli aspetti salienti della vicenda in questione. Come noto, ai sensi del Capo V del regolamento (UE) 2016/679 (il celebre GDPR), che sul punto riprende la disciplina della previgente direttiva 95/46/CE, il trasferimento di dati personali dall'UE verso un Paese terzo è ammesso se la Commissione ha adottato una "decisione di adeguatezza" nei confronti di tale Stato, cioè se ha deciso che quest'ultimo garantisce un livello di protezione dei dati personali "adeguato". In mancanza di una simile misura, il trasferimento è possibile solo in presenza di uno dei meccanismi alternativi del Capo V GDPR (segnatamente, le garanzie adeguate e le deroghe in specifiche situazioni), che sono tuttavia adoperabili solo in casi limitati.

Nei confronti degli Stati Uniti, una decisione di adeguatezza era stata adottata già nel 2000: ci si riferisce alla decisione "Approdo sicuro" o "*Safe Harbor*" (decisione 2000/520/CE), la quale andava a istituire un sistema che consentiva il trasferimento di dati personali verso quelle organizzazioni private USA che avessero autocertificato la propria adesione a determinati principi. Tuttavia, a seguito delle rivelazioni di Edward Snowden del 2013 sui programmi di sorveglianza di massa posti in essere dai servizi di *intelligence* degli USA, il giurista e attivista per la *privacy* austriaco Maximillian Schrems ha dato avvio a una vicenda giudiziaria che ha portato, nel 2015, all'annullamento della decisione "Approdo sicuro" da parte della Corte di giustizia dell'UE (sentenza della Corte del 6 ottobre 2015, causa C-362/14, *Schrems*). Nell'ordinamento USA, infatti, le deroghe alla tutela dei dati personali per motivi di sicurezza nazionale non operavano nei limiti dello stretto necessario. Si consentiva anzi alle autorità pubbliche di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche e non erano previste possibilità per il singolo di avvalersi di rimedi giuridici: era così pregiudicato il contenuto essenziale dei diritti fondamentali sanciti dalla Carta di Nizza agli artt. 7 (rispetto della vita privata e della vita familiare), 8 (protezione dei dati di carattere personale), nonché 47 (diritto a un ricorso effettivo e a un giudice imparziale).

La Commissione si è subito affrettata a colmare il vuoto creatosi, e ha adottato già nel 2016 la decisione "Scudo UE-USA per la privacy" o "*EU-US Privacy Shield*" (decisione di esecuzione (UE) 2016/1250): essa prevedeva un meccanismo pressoché analogo a quello della decisione "*Safe Harbor*", ma cercava di correggerne i principali difetti. Tale misura ha avuto però la medesima sorte della precedente: nel 2020, sempre a seguito dell'iniziativa di Schrems, il Giudice di Lussemburgo l'ha infatti dichiarata invalida, per ragioni simili a quelle viste poc'anzi (sentenza della Corte del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*). In particolare, le limitazioni ai diritti degli articoli 7 e 8 della Carta, derivanti dalla normativa USA in materia di sorveglianza a fini di sicurezza nazionale, non corrispondevano a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto UE, dall'art. 52, par. 1, della Carta stessa; non rispettavano, cioè, il principio di proporzionalità, in quanto non si limitavano allo stretto necessario. Inoltre, il *Privacy Shield* non forniva mezzi di ricorso di fronte a un organo in grado di offrire agli individui garanzie sostanzialmente equivalenti a quelle richieste dall'art. 47 della Carta.

Per la seconda volta, gli Stati Uniti si sono dunque trovati privi di una decisione di adeguatezza che consenta il trasferimento di dati personali dall'UE verso di loro, rendendosi conseguentemente necessario l'utilizzo dei ben più limitati meccanismi alternativi. Una situazione che permane anche nel momento in cui si scrive.

2. Ripercorsi sinteticamente i passaggi che hanno condotto all'annullamento di entrambe le previgenti decisioni di adeguatezza nei

confronti degli USA, è ora possibile concentrarsi sui tentativi attualmente in corso per giungere all'adozione di una terza misura che possa superare le criticità delle precedenti.

Già in data 25 marzo 2021, la Commissione UE ha dichiarato di aver intensificato i negoziati con il governo degli Stati Uniti al fine di addivenire a una versione del *Privacy Shield* rafforzata e rispettosa delle pronunce rese dalla Corte di giustizia nell'ambito della vicenda Schrems. Esattamente un anno dopo, il 25 marzo 2022, la Commissione e gli USA hanno annunciato congiuntamente di aver raggiunto un accordo di principio su un nuovo "*Trans-Atlantic Data Privacy Framework*". In particolare, gli Stati Uniti si sono impegnati a implementare riforme per rafforzare la *privacy* e le libertà civili degli individui nell'ambito delle attività di *intelligence* e, ancor più nello specifico, ad assicurare che tali attività siano necessarie e proporzionate al perseguimento di obiettivi di sicurezza nazionale ben definiti, nonché ad istituire opportuni meccanismi di ricorso e di vigilanza. Simili impegni si sarebbero poi concretizzati nell'adozione di un *Executive Order*, i.e. un provvedimento del Presidente USA, che avrebbe rappresentato la base della successiva valutazione di adeguatezza della Commissione.

L'*Executive Order*, invero, si è fatto attendere oltre sei mesi, tanto da suscitare *medio tempore* commenti critici da parte dello stesso Schrems (il quale ha affermato: "*It is astonishing that two democracies that agree on principles […] cannot come to a proper agreement. It seems, the US still supports the idea that non-US persons shouldn't have fundamental rights*"; v. NONE OF YOUR BUSINESS, *6 Months of "agreement in principle", EU-US agreement in fact still missing*, in noyb.eu/en, 25 September 2022); ma finalmente, come anticipato in apertura, in data 7 ottobre 2022 il Presidente Biden ha firmato il citato "*Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*", che può essere dunque di seguito analizzato.

3. L'*Executive Order* di cui trattasi (di seguito anche EO) si compone di cinque sezioni ("*Sections*"). La prima individua lo scopo ("*Purpose*") dell'EO, ovvero quello di introdurre limiti per le attività di *intelligence* USA, al fine di tutelare il legittimo interesse alla *privacy* degli individui.

Il cuore dell'EO è però rappresentato dalle sue sezioni 2 e 3. La sezione 2, intitolata "Attività di *intelligence* dei segnali" ("*Signals Intelligence Activities*"), elenca innanzitutto i "Principi" ("*Principles*") a cui simili attività devono attenersi (*sec*. 2.a): devono essere autorizzate a livello normativo (*sec*. 2.a.i); devono essere soggette a garanzie appropriate a tutela della *privacy* e delle libertà civili (*sec*. 2.a.ii), che assicurino che le attività in questione siano *necessarie* per promuovere una priorità di *intelligence* convalidata (*sec*. 2.a.ii.A) e siano *proporzionate* rispetto a tale priorità (*sec*. 2.a.ii.B); devono essere soggette a una rigorosa vigilanza sul rispetto dei suddetti principi (*sec*. 2.a.iii).

Dopo i "Principi" sono enumerati gli "Obiettivi" ("*Objectives*"; *sec*. 2.b): le attività di *intelligence*, infatti, possono essere condotte solo per perseguire

obiettivi legittimi ("*Legitimate objectives*") opportunamente specificati, come proteggere la sicurezza nazionale da minacce transfrontaliere, terrorismo, spionaggio, minacce informatiche e non solo (*sec*. 2.b.i); altri obiettivi sono invece espressamente proibiti, come sopprimere i diritti civili oppure svantaggiare alcune persone sulla base dell'etnia, della razza, del genere, dell'identità di genere, dell'orientamento sessuale o della religione (*sec*. 2.b.ii).

Si puntualizzano poi le salvaguardie a tutela della *privacy* e delle libertà civili ("*Privacy and civil liberties safeguards*"; *sec*. 2.c), facendo *inter alia* ulteriori riferimenti al principio di proporzionalità, nonché i meccanismi di vigilanza (*sec*. 2.d).

La sezione 3, invece, è interamente dedicata ai meccanismi di ricorso ("*Signals Intelligence Redress Mechanism*"), e prevede due nuove procedure. Innanzitutto, vi è la possibilità di rivolgersi alla figura indipendente del "*Civil Liberties Protection Officer*", o CLPO (*sec*. 3.c), che ha il compito di esaminare e indagare sui fatti contestati e, ove necessario, ordinare gli opportuni rimedi (*sec*. 3.c.i). In seconda istanza, il ricorrente può rivolgersi a una "*Data Protection Review Court*", o DPRC (*sec*. 3.d), nell'ambito della quale viene istituito un panel di tre giudici con il compito di esaminare la questione (*sec*. 3.d.i.B) e ordinare, eventualmente, gli opportuni rimedi (*sec*. 3.d.i.H). È previsto che sia le determinazioni del CLPO (*sec*. 3.c.ii) che quelle della DPRC (*sec*. 3.d.ii) abbiano effetto giuridico vincolante ("*binding effect*") per l'intera comunità di *intelligence*.

L'EO, infine, si conclude con una sezione dedicata alle "Definizioni" ("*Definitions*"; *sec*. 4), dove viene precisato il significato di espressioni come "opportuni rimedi" ("*appropriate remediation*"; *sec*. 4.a), *intelligence* (*sec*. 4.f), "comunità di *intelligence*" ("*intelligence community*"; *sec*. 4.g), nonché "sicurezza nazionale" ("*national security*"; *sec*. 4.h); e con una sezione dedicata alle "Previsioni generali" ("*General Provisions*"; *sec*. 5).

L'EO, giova ricordarlo, è stato poi ulteriormente integrato a stretto giro, in particolare attraverso il regolamento sulla DPRC ("*Regulation on the Data Protection Review Court*") emanato dal Procuratore generale USA Merrick Garland.

4. Ritenendo che con l'*Executive Order* gli USA abbiano efficacemente recepito nel proprio ordinamento gli impegni assunti, la Commissione UE, neanche due mesi dopo la firma dello stesso EO e segnatamente in data 13 dicembre 2022, ha presentato la "*Draft Adequacy Decision for the EU-US Data Privacy Framework*", ovverosia la proposta che dà avvio all'*iter* di adozione di una nuova decisione di adeguatezza.

La sua struttura ricalca, in grandissima parte, quella delle due precedenti decisioni di adeguatezza riguardanti gli Stati Uniti. L'art. 1, innanzitutto, sancisce che ai fini del GDPR gli USA assicurano un livello di protezione adeguato ai dati personali trasferiti dall'Unione alle organizzazioni statunitensi incluse nella "*Data Privacy Framework List*", amministrata e resa disponibile dal "*Department of Commerce*" USA.

Proprio come il *Safe Harbor* e il *Privacy Shield*, anche il nuovo *Data Privacy Framework* sarebbe dunque costituito da un insieme di principi a cui le organizzazioni USA potranno volontariamente aderire per ottenere la certificazione che consenta loro di ricevere e trattare dati personali provenienti dall'UE. È bene infatti ricordare come la Corte di giustizia avesse precisato come non fosse il sistema di autocertificazione in quanto tale a rendere le precedenti decisioni contrarie al diritto UE; esso può essere quindi replicato.

L'Allegato I alla proposta è denominato "*EU-U.S. Data Privacy Framework Principles issued by the U.S. Department of Commerce*", e contiene appunto l'elenco dei principi a cui aderire, tra cui: "Notifica" (concernente le informazioni da fornire agli interessati), "Scelta" (riguardante il consenso degli interessati), "Responsabilità in caso di ulteriore trasferimento", "Sicurezza", "Integrità dei dati e limitazione della finalità", diritto di "Accesso", "Ricorso, controllo e responsabilità"; vi sono poi anche "Principi supplementari". Pure l'elenco dei principi riprende in massima parte quello delle precedenti decisioni.

La proposta, infine, è completata da altri Allegati contenenti impegni e dichiarazioni ufficiali provenienti da varie autorità statunitensi (Allegati II-VII); essi costituiscono un altro elemento di similitudine con il passato.

Nei prossimi mesi, la proposta seguirà una procedura che prevede la consultazione del Comitato europeo per la protezione dei dati, nonché la necessità di un parere positivo da parte di un comitato composto da rappresentanti degli Stati membri. Solo a quel punto, la decisione di adeguatezza potrà essere definitivamente adottata.

5. L'assetto che va delineandosi presenta indubbi aspetti positivi, ma anche evidenti criticità.

Si parta dall'EO, e in particolare dai suoi aspetti meritori. Come ricordato da Guido Scorza, Componente del Garante italiano per la protezione dei dati personali, "con l'executive order in questione entrano nell'Ordinamento americano, concetti e principi di chiara impronta europea come quelli di necessità dei trattamenti […], proporzionalità, diritto dei cittadini europei a un ricorso per le ipotesi in cui sospettino una violazione della loro *privacy*, necessità per le agenzie di *intelligence* di più stringenti basi giuridiche prima di fare incetta di dati personali […]" (G. SCORZA, *Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire*, in *AgendaDigitale*, 10 ottobre 2022). Si tratta dunque per la normativa USA di un chiaro passo avanti nella direzione sperata dalle istituzioni UE.

È però opportuno mettere in evidenza anche alcuni dei più importanti aspetti problematici dell'EO. Il primo, di ordine generale, è sottolineato proprio dallo stesso Scorza e riguarda la scelta dello strumento giuridico rappresentato dall'*Executive Order*: infatti, "un ordine esecutivo […] non è una legge e non può modificare le leggi"; anzi, addirittura "nell'executive order firmato […] da Biden c'è scritto nero su bianco – ma sarebbe stato

comunque così – che non interviene sulla disciplina vigente incluse, tra le altre, proprio le leggi, "pietra dello scandalo" […]" (G. SCORZA, *op. cit.*), ovvero quelle che avevano indotto la Corte di giustizia ad assumere le già citate determinazioni (tra queste si può citare il *Foreign Intelligence Surveillance Act* o FISA). È dunque lecito chiedersi se uno strumento come l'EO possa essere sufficiente a risolvere la questione.

Vi sono, poi, svariate criticità che riguardano proprio il contenuto normativo dell'EO. Innanzitutto, è vero che l'EO consente le attività di *intelligence* solo là dove esse perseguano obiettivi legittimi, ma è anche vero che tali obiettivi sono formulati in modo assai ampio: le "minacce" ("*threats*") a cui si fa riferimento nella *sec*. 2.b.i possono ricomprendere una vasta casistica, e dunque può essere coinvolto un numero enorme di individui (sul punto v. H. RUSCHEMEIER, *Nothing new in the west? The executive order on US surveillance activities and the GDPR*, in *European Law Blog*, 14 November 2022); senza contare che il Presidente USA potrebbe autorizzare ulteriori aggiornamenti dell'elenco, alla luce di nuovi imperativi di sicurezza nazionale (*sec*. 2.b.i.B). Inoltre, anche se deve essere preferita una "raccolta mirata" ("*targeted collection*"), non è neppure del tutto esclusa una "raccolta in blocco" ("*bulk collection*") nei casi in cui gli obiettivi non possano essere raggiunti attraverso la prima (2.c.ii); il che rappresenta un grande elemento di divergenza rispetto ai principi del GDPR (v. H. RUSCHEMEIER, *op. cit.*).

Per quanto poi riguarda i "Principi" della *sec*. 2.a, se da un lato essi riprendono sul piano della terminologia quelli propri del diritto UE e della giurisprudenza della Corte di giustizia – si pensi alla "proporzionalità" – non vi è alcuna certezza sul fatto che dal punto di vista sostanziale il loro contenuto sia il medesimo (v. H. RUSCHEMEIER, *op. cit.*).

Svariati sono anche i rilievi che possono essere mossi in riferimento ai meccanismi di ricorso. Se ne sintetizzano, di seguito, alcuni dei più rilevanti. Innanzitutto, sia il CLPO (*sec*. 3.c.i.E.1) che la DPRC (*sec*. 3.d.i.H) possono dare informazione al ricorrente solo circa l'individuazione o meno di una violazione e, nel primo caso, circa il fatto che sono stati ordinati opportuni rimedi, ma tutto ciò senza confermare o smentire che il ricorrente sia stato sottoposto da parte degli USA ad attività di *intelligence* dei segnali ("*without confirming or denying that the complainant was subject to United States signals intelligence activities*"), una circostanza che solleva evidenti problemi sul piano della trasparenza. In secondo luogo, sia il CLPO che la DPRC sono organi interni all'esecutivo USA, fattore che chiaramente rischia di comprometterne l'indipendenza. Inoltre, anche se le determinazioni di CLPO e DPRC vengono definite come "vincolanti", esse lasciano in realtà il ricorrente senza alcun diritto soggettivo corrispondente. Vi è dunque motivo di dubitare che ci si trovi in presenza di garanzie sostanzialmente equivalenti a quelle richieste dall'art. 47 della Carta (sul punto v. H. RUSCHEMEIER, *op. cit.*).

Un cenno deve poi essere fatto alle criticità che caratterizzano la proposta di decisione di adeguatezza della Commissione UE. Infatti, anche

se l'annullamento di *Safe Harbor* e *Privacy Shield* non è dipeso tanto dalla loro struttura quanto dai summenzionati *deficit* dell'ordinamento USA, alcune somiglianze con le previgenti decisioni danno comunque adito a dubbi. Come rilevato da Francesco Pizzetti, già Presidente del Garante italiano per la protezione dei dati personali, nonostante si assuma che la Commissione federale per il commercio ("*Federal Trade Commission*" o FTC) possa intervenire più incisivamente sulla verifica delle autocertificazioni, lascia comunque perplessi il fatto che nello schema in questione resti ferma la remissione ai titolari dei trattamenti della responsabilità di autocertificare le misure adottate (F. PIZZETTI, *Troppo debole lo schema Ue per trasferimento dati verso gli Usa, cruciale il parere EDPB*, in *Agenda Digitale*, 19 dicembre 2022).

6. In conclusione, dall'analisi svolta appare più che mai chiaro come gli ultimi capitoli della saga sui trasferimenti transatlantici di dati personali siano tutto fuorché in grado di mettere la parola fine alla vicenda. Ciò, innanzitutto, perché occorrerà attendere lo sviluppo dell'*iter* di adozione della decisione di adeguatezza, per sapere se quest'ultima verrà effettivamente emanata e, in tal caso, con quali modifiche. Ma soprattutto perché, anche dopo l'eventuale adozione della decisione, si renderà assolutamente indispensabile monitorare l'assetto creatosi: sarà infatti necessario capire, in particolare, quanto stringenti siano i nuovi limiti imposti alle agenzie di *intelligence* USA; quanto i procedimenti di ricorso nel caso di possibili violazioni siano effettivamente accessibili; quanto saprà essere realmente indipendente la DPRC; e non solo (sul punto v. G. SCORZA, *op. cit.*).

I suddetti aspetti dovranno essere oggetto di continuo controllo da parte della Commissione UE che, lo si precisa, potrebbe anche decidere di sospendere, abrogare o modificare la decisione. E ancor di più, è assai probabile che simili profili possano essere oggetto di un nuovo sindacato da parte del Giudice di Lussemburgo. Su quest'ultimo punto non è irrilevante menzionare il fatto che Maximillian Schrems si è già esposto in modo molto netto sul nuovo quadro giuridico (NONE OF YOUR BUSINESS, *New US Executive Order unlikely to satisfy EU law*, in noyb.eu/en, 7 ottobre 2022), definendolo non in grado di soddisfare le condizioni richieste dal diritto dell'UE e ponendo l'accento sulle più significative criticità prese in esame nel presente contributo: *inter alia*, ha infatti espresso dubbi sul significato di "proporzionalità" ("*The EU and the US now agree on the use of the word 'proportionate' but seem to disagree on the meaning of it*"), e pure sul fatto che la DPRC rappresenti un mezzo di ricorso idoneo ("*it is clear that this 'court' is simply not a court*"); secondo Schrems, le principali problematiche non sarebbero state dunque risolte, e proprio per tale motivo ha già annunciato una nuova iniziativa giudiziaria per tornare di fronte alla Corte di giustizia ("*it seems that the core issues were not solved and it will be back to the CJEU sooner or later*").

Detto ciò, al di là di tutti i possibili dubbi e criticità permanenti, e anche al di là di un eventuale sindacato giurisdizionale sulla nuova decisione di adeguatezza, vi è comunque un fattore positivo che merita di essere evidenziato. L'Unione europea, anche se con fatica e poco per volta, sta infatti riuscendo a indurre gli Stati Uniti a modificare la propria normativa in materia di sorveglianza, rendendola progressivamente più vicina ai principi propri del diritto UE. Basti pensare che, già nel 2015, il c.d. *Freedom Act* era intervenuto con alcune modifiche (poi non rivelatesi decisive per evitare l'annullamento del *Privacy Shield*) che cercavano di ridurre i poteri di sorveglianza delle autorità pubbliche. Ora, l'*Executive Order* del Presidente Biden rappresenta in ogni caso un altro passo avanti. In definitiva, il fatto che gli USA siano stati indotti ad apportare simili modifiche normative è una conferma dell'influenza sulle normative dei Paesi terzi che l'UE esercita unilateralmente grazie alla propria posizione centrale nell'economia globale, il c.d. "*Brussels effect*" (sul punto v.: A. BRADFORD, *The Brussels Effect*, in *Northwestern University Law Review*, 2012, pp. 1-68; A. BRADFORD, *The Brussels effect: How the European Union rules the world*, Oxford, 2020): si può dunque parlare di un successo, ancorché piccolo e parziale, della strategia UE di esportare oltreconfine i propri standard.