Diritti civili e politici

EU-US Data Privacy Framework: *Much Ado About Nothing*?

Sommario: 1. Introduzione. – 2. La nozione di adeguatezza del livello di protezione dei dati personali. – 3. Il *Data Privacy Framework*. – 4. Il trattamento dei dati ad opera delle autorità federali di intelligence. – 5. Vie di ricorso amministrative e giurisdizionali. – 6. Conclusioni.

Commissione europea, decisione di esecuzione UE 2023/1795 a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali europea di *riferimento*, del 10 luglio 2023 (eur-lex.europa.eu/eli/dec_impl/2023/1795/oj)

1. La Commissione europea ha recentemente adottato la decisione UE 2023/1795, volta a consentire i flussi transfrontalieri di dati personali dall'Unione europea agli Stati Uniti d'America. Si tratta di un provvedimento che, pur necessario in considerazione delle pronunce della Corte di giustizia UE, nei casi *Schrems I e Schrems II* (di cui si dirà a breve), sulla precedente cornice normativa che tali flussi autorizzava, potrebbe porre questioni giuridiche di portata sostanzialmente analoga a quelle già sollevate dal giudice di Lussemburgo. Si consideri, infatti, che il meccanismo su cui si fonda tale decisione è analogo a quello previgente – e cioè l'adozione, da parte delle competenti autorità federali USA, di un sistema di principi sul trattamento dei dati cui gli operatori economici statunitensi, che vogliano ricevere dati dall'UE, possono aderire su base volontaria attraverso un'autocertificazione.

Con il presente lavoro, ci proponiamo, per un verso, di analizzare la genesi della decisione della Commissione sopra menzionata e, per l'altro, di verificarne la coerenza, *prima facie*, con l'ordinamento giuridico dell'Unione europea – tenendo in particolare considerazione il GDPR (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – regolamento generale sulla protezione dei dati, di seguito GDPR), gli art. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea e la giurisprudenza della Corte di giustizia, relativa alle condizioni di ammissibilità dei trasferimenti dei dati personali dall'Unione europea verso Paesi terzi.

Si effettuerà, innanzitutto, un rapido cenno all'insieme dei meccanismi, previsti dal summenzionato GDPR, che consentono di trasferire dati, elaborati da un soggetto stabilito sul territorio dell'UE, ad un ente che tali dati tratti in uno Stato terzo. In questo contesto, si darà conto del ruolo della Commissione europea nell'accertamento dell'adeguatezza del livello di protezione dei dati personali garantito nei singoli Stati non membri UE che vogliano ricevere dati da essa provenienti. Una volta chiariti i presupposti in presenza dei quali sia possibile che flussi transfrontalieri di dati verso Paesi terzi abbiano luogo, si cercherà di individuare le possibili criticità del nuovo *EU-US Data Privacy Framework*, al fine di determinarne la coerenza con il sistema europeo di *data protection* e, di conseguenza, le *chance* di superare il molto probabile vaglio della Corte di giustizia. A questo fine, non potendosi compiere un'analisi *ex professo* del sistema nel suo comples-

© Società editrice il Mulino
ISSN: 1971-7105

so, ci si dedicherà all'analisi degli aspetti *lato sensu* procedurali, e cioè relativi ai meccanismi di supervisione sul piano amministrativo e giurisdizionale che sono stati predisposti dalle autorità statunitensi per garantire il rispetto dei principi sostanziali sul trattamento dei dati che il cd. *Data Privacy Framework* (di seguito DPF) pone (principi che, come si dirà, tendono a coincidere con quelli desumibili dal GDPR).

2. L'Unione europea, come noto, si è dotata di una disciplina generale in materia di elaborazione di dati personali già nel 1995, con la cd. la direttiva dati (Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GU L 281 del 23.11.1995), poi abrogata dal GDPR, in vigore dal maggio del 2018. Si tenga conto del fatto che l'una e l'altro si fondano su una serie di principi sostanziali sul trattamento dei dati nonché su un nucleo di diritti degli interessati ad un trattamento per lo più coincidenti. Per ciò che ci interessa in questa sede, basti osservare che le modalità di trasferimento dei dati personali al di fuori dell'Unione europea, già previste agli art. 25 e ss. della direttiva dati sono, grosso modo, riprese dagli art. 45 e ss. del GDPR. Una tale constatazione è di particolare interesse ove si consideri che la giurisprudenza di Lussemburgo sui flussi transfrontalieri di dati può essere utilizzata quale parametro di legittimità delle decisioni di adeguatezza adottate dalla Commissione a prescindere dal regime giuridico vigente al momento dell'adozione delle stesse.

Come già accennato, il principio cardine della disciplina sui flussi transfrontalieri di dati personali è che questi, una volta trasferiti nel Paese terzo di destinazione, siano trattati garantendo un livello di tutela della privacy individuale *grossomodo equivalente* a quello garantito dall'ordinamento giuridico dell'UE (circa la nozione di equivalenza del livello di protezione dei dati si veda N. I. Theodorakis, "Cross Border Transfers under the GDPR: the Example of Transferring Data from the EU to the US", in *TTLF Working Papers* 2018, p. 7 ss.). Il GDPR, a tal proposito, dopo aver premesso un divieto generale di trasferimenti transfrontalieri che non avvengano in conformità con il Capo V dello stesso, opera una distinzione preliminare tra Stati che si possano considerare sicuri, in ragione di una decisione di adeguatezza da parte della Commissione europea, e Stati che, viceversa, non siano qualificabili come tali. In questo secondo caso, che non sarà oggetto di approfondimento in questa sede, basti accennare alla circostanza che è possibile per singoli operatori economici, stabiliti in Stati terzi non sicuri, ricevere dati personali elaborati nell'Unione europea, *inter alia*, attraverso l'adozione di norme vincolanti d'impresa, codici di condotta o la sottoscrizione di clausole contrattuali standard conformi al modello messo a punto dalla Commissione Europea (art. 46 ss. GDPR).

La nozione di adeguatezza del livello di protezione dei dati personali è, all'evidenza, il cardine attorno al quale ruota la questione della legittimità del trasferimento di dati dall'Unione europea agli Stati Uniti. A tal proposito, si deve, quindi, procedere all'individuazione dei parametri rilevanti che consentono alla Commissione europea di affermare che uno Stato terzo sia 'sicuro' dal punto di vista delle regole in tema di trattamento dei dati personali. L'art. 25, par. 6, della direttiva dati si limitava a prevedere che la Commissione tenesse in considerazione *legislazione nazionale* e *impegni internazionali* dello Stato terzo, per determinare il livello di adeguatezza della protezione dei dati «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona». Sul punto, peraltro, la Corte di giustizia ha espressamente affermato, nel caso *Schrems* (Corte di giustizia (Grande Sezione), *Maximillian Schrems contro Data Protection Commissioner*, Causa C-362/14, sentenza del 6 ottobre 2015, par. 73), che «è vero che il ter-

mine 'adeguato' figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia (… omissis…) l'espressione livello di protezione adeguato deve essere intesa 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» (corsivo nostro). Con tale pronuncia i giudici di Lussemburgo riconducono al concetto di adeguatezza non solo il livello di protezione dei dati ma anche, in connessione con questo, il livello di protezione dei diritti fondamentali (*rectius*, di quei diritti che possano subire una limitazione in ragione di un trattamento illecito di dati personali).

La Corte, in buona sostanza, esclude che il trasferimento di dati raccolti nell'UE verso Stati terzi possa risolversi in un vuoto o in un eccessivo affievolimento della tutela quanto al diritto degli interessati al trattamento alla protezione dei loro dati personali e dei diritti ad esso connessi. Di conseguenza, in tanto un flusso transfrontaliero di dati può aver luogo, in quanto lo Stato di destinazione garantisca una tutela dei diritti e delle libertà fondamentali che sia, nella sostanza, comparabile a quella garantita dall'ordinamento UE. La sostanziale equivalenza in discorso, implica che le limitazioni ai diritti fondamentali, nell'ordinamento del paese destinatario dei flussi di dati, rispondano, grosso modo, ai medesimi requisiti previsti dal diritto dell'Unione (in questo senso, T. Naef, *Data Protection without Data Protectionism*, Cham, 2023, p. 57).

Il GDPR, al contrario della direttiva dati, fornisce un elenco, invero, molto dettagliato degli elementi da esaminare ai fini della determinazione dell'adeguatezza del livello di protezione dei dati (si vedano, sul punto, le considerazioni di F. Velli, "The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements", in *European Papers* 2019, pp. 881-894, p. 883) – elementi, peraltro, riconducibili a tre categorie: il rispetto dei diritti umani e delle libertà fondamentali (art. 45, par. 2, lett. a); l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti (art. 45, par. 2, lett. b); gli impegni internazionali assunti dal paese terzo in questione (art. 45, par. 2, lett. c). La finalità di tale diversa tecnica normativa è, evidentemente, la limitazione della discrezionalità in capo alla Commissione, in sede di adozione di decisioni d'adeguatezza, come, tra l'altro, implicitamente confermato da quanto previsto dal successivo par. 4, che obbliga la Commissione stessa a controllare «su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni».

Come sopra accennato, la Commissione europea ha, negli anni, adottato tre diverse decisioni d'adeguatezza relative ai trasferimenti di dati personali dall'Unione europea verso gli USA. La successione tra tali provvedimenti, ovviamente legata all'annullamento degli stessi da parte dei giudici di Lussemburgo, può essere considerata epifenomeno della strutturale asimmetria tra il sistema di protezione dei dati personali vigente nell'Unione europea e quello nordamericano. Più precisamente, si deve constatare l'assenza di un sistema siffatto al livello dell'ordinamento federale USA. Per un verso, il legislatore statunitense non ha mai adottato uno strumento espressamente volto a disciplinare l'uso che si possa fare dei dati personali, e, per l'altro, diverse misure legislative prendono in considerazione soltanto alcuni aspetti della *data protection*, sovente in connessione con la natura (di autorità federale, appunto) del soggetto chiamato a trattare i dati. A ciò si aggiunga che alcuni degli Stati della federazione si stanno dotando di legislazioni (statali) in materia

di dati personali, con l'ulteriore conseguenza che le modalità di trattamento dei dati trasferiti dall'UE potrebbero variare a seconda dello Stato in cui è stabilito il destinatario dei dati stessi.

La conseguenza dell'assenza di una disciplina omnicomprensiva in materia di dati personali negli USA ha, quindi, comportato la necessità, per la Commissione europea, di negoziare a più riprese con le autorità federali, al fine di individuare un nucleo minimo di garanzie che potessero consentire alla stessa di affermare l'adeguatezza del livello di protezione dei dati personali negli Stati Uniti.

Si deve, infatti, considerare che il *Data Privacy Framework* è stato preceduto da due diversi sistemi, oggetto di negoziazione tra autorità UE e USA e quindi approvati dalla Commissione europea con proprie decisioni di adeguatezza, poi annullate da parte dei giudici di Lussemburgo. Pur non potendosi, in questa sede, approfondire tali sistemi, ci si limiterà a darne menzione al fine di richiamarli ove presentino punti di congruenza con il DPF. Il primo di essi, il cd. *Safe Harbor*, fu adottato dalla Commissione europea con decisione di adeguatezza del 2000 (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, in GU L 215 del 25.8.2000). Con la già menzionata sentenza *Schrems,* la Corte di giustizia ne ha dichiarato l'invalidità per contrasto – *inter alia* – con gli art. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (di seguito Carta di Nizza), all'esito di una puntuale analisi delle modalità di trattamento cui i dati, trasferiti dall'UE, sarebbero stati soggetti una volta elaborati negli USA. Particolare rilevanza è stata attribuita, in quella circostanza, alle modalità di accesso ai dati personali da parte delle autorità federali deputate alla sicurezza nazionale (sostanzialmente prive di limitazioni puntuali).

Per rimpiazzare il *Safe Harbor* fu, quindi, istituita una nuova base giuridica per i flussi di dati personali dall'UE agli Stati Uniti, il cd. *Privacy Shield* (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, in GU L 207 del 1.8.2016). Anche questa seconda decisione sull'adeguatezza del livello di protezione dei dati personali garantito dal *Privacy Shield* è stata oggetto di annullamento ad opera dei giudici di Lussemburgo (Corte di giustizia, *Data Protection Commissioner c. Maximilian Schrems e Facebook Ireland*, causa C-311/18, sentenza del 16 luglio 2020,), assumendo nuovamente come parametro di legittimità rilevanti gli art. 7, 8 e 47 della Carta di Nizza (sul punto, ci permettiamo di rinviare ad A. Terrasi, "Protection of Personal Data and Human Rights between the ECHR and the EU Legal Order", in *Legal Technology Transformation: a Practical Assessment*, A. Caligiuri (ed.), Napoli, 2020, p. 21-32, p. 26 ss.).

Pare opportuno osservare, sia pur incidentalmente, che entrambi gli strumenti giuridici oggetto di annullamento erano volti a creare un sistema attraverso il quale fosse possibile, per enti privati stabiliti nell'UE e ivi chiamati a trattare dati personali, trasferire lecitamente tali dati verso gli USA. Va da sé che le sopra menzionate pronunce dei giudici di Lussemburgo, annullando le decisioni sull'adeguatezza con cui la Commissione aveva approvato i relativi meccanismi di trasferimento dei dati, abbiano reso giuridicamente impossibile, per le imprese europee, essere origine di flussi transfrontalieri di dati verso gli USA.

3. Proprio al fine di colmare tale evidente lacuna giuridica, la Commissione ha recentemente adottato, come sopra accennato, un'ulteriore decisione sull'adeguatezza, avente ad oggetto la protezione dei dati personali garantita dal DPF. L'atto in discorso, peraltro, mostra una tecnica normativa 'ipertrofica', con oltre 60 pagine di considerando, innumerevoli allegati, e soltanto 4 articoli nella parte propriamente dispositiva.

Come accennato in premessa (e in ragione dell'eccezionale ampiezza della decisione sull'adeguatezza in commento) si limiterà l'analisi che segue ai soli punti che, *prima facie*, paiono critici, in ragione del possibile contrasto con il GDPR nonché con le sopra menzionate norme della Carta di Nizza, così come interpretati dalla Corte di giustizia nella giurisprudenza sopra riportata. Si cercherà, quindi, di dar conto delle eventuali discrasie tra le garanzie in materia di protezione dei dati personali che l'ordinamento UE prevede e quelle che discendono dall'applicazione degli impegni assunti dalle autorità federali USA.

A tal proposito, parrebbe potersi porre una questione logicamente preliminare, e cioè la natura giuridica delle dichiarazioni allegate alla decisione della Commissione (Comunicazione del *Secretary of Commerce* del 6 luglio 2023, all. II alla decisione della Commissione; Comunicazione della *International Trade Administration* del 12 dicembre 2022, all. III; Comunicazione della *Federal Trade Commission* del 9 giugno 2023, all. IV; Comunicazione del *Secretary of Transportation* del 6 luglio 2023, all. V; Lettera dell'*Office of Assistant Attorney General* del 23 giugno 2023, all. VI; Lettera dell'*Office of the Director of National Intelligence* del 9 dicembre 2022, all. VII). Si tratta, infatti, di strumenti che parrebbero sottendere l'assunzione di impegni unilaterali da parte dei dichiaranti. Non è, d'altronde, chiaro quale relazione possa esservi tra tali atti e la decisione sull'adeguatezza resa dalla Commissione stessa. A rigor di logica, la decisione in discorso si fonda sulle 'garanzie' contenute nelle dichiarazioni delle autorità federali USA. In altre parole, non pare sia ravvisabile un qualche nesso diretto tra la prima e le seconde e, all'evidenza, ciò non consente di affermare la natura convenzionale degli obblighi in materia di trattamento di cui si discute. Una tale considerazione, peraltro, non può che condurre a interrogarsi sulla rilevanza degli stessi in quanto 'obblighi internazionali' ai sensi dell'art. 45 GDPR.

Assumendo, ad ogni modo, che la congerie di atti promananti da diverse amministrazioni federali, per lo più riconducibili al Dipartimento del Commercio, al Dipartimento dei Trasporti e al Dipartimento di Giustizia, sia idonea a vincolare le autorità federali dichiaranti quanto alle modalità di trattamento dei dati ricadenti sotto l'ambito d'applicazione del DPF, ci si deve, comunque, interrogare sulla sussistenza di un livello di protezione di tali dati sostanzialmente equivalente a quello che deriva dall'ordinamento UE.

Si consideri che il DPF si fonda su due serie di principi, rispettivamente denominati *DPF Principles* e *Supplemental Principles*. L'insieme delle previsioni in discorso definisce le modalità di trattamento dei dati personali – provenienti dall'UE – da parte degli enti economici di diritto statunitense che autocertifichino al *Department of Commerce* la propria volontà di aderire al *Data Privacy Framework* (Le previsioni in discorso sono accluse alla decisione sull'adeguatezza in commento all'allegato I, *EU-US Privacy Framework Principles Issued by the U.S. Department of Commerce*). A tali tipologie di principi si aggiunge poi un allegato relativo ad un meccanismo arbitrale non obbligatorio cui gli interessati al trattamento possono ricorrere ove assumano che i propri diritti siano stati violati.

In termini generali, si può considerare che la formulazione dei principi in discorso da parte del Dipartimento del Commercio non solleva particolari criticità, quantomeno per ciò che concerne i principi sostanziali sul trattamento dei dati – basti osservare, in questa

sede, che tali principi costituiscono un *pendant* piuttosto fedele delle corrispondenti previsioni del GDPR sulle modalità di trattamento dei dati, dal principio di liceità dei trattamenti, a quello della finalità limitata a quello della sicurezza e dell'integrità dei dati. Considerazioni diverse e più articolate merita, invece la questione dell'accesso a un giudice che possa garantire il rispetto dei summenzionati principi sostanziali (sul punto si veda il par. 5).

Il DPF va, poi, posto a sistema con la legislazione federale che, pur incidentalmente, detti regole in tema di trattamento di dati personali nonché con un ordine esecutivo del Presidente USA, di cui si dirà dappresso, adottato per limitare l'accesso, prima tendenzialmente illimitato, delle autorità federali di intelligence ai dati in possesso di enti privati statunitensi. Quanto alle leggi federali in discorso, si consideri, poi, che i cittadini europei, i cui dati siano trasferiti negli USA, non rientrano nell'ambito d'applicazione *ratione personarum* di alcuni strumenti (si pensi allo *US Privacy Act* del 1974, applicabile soltanto ai cittadini o ai residenti di lungo periodo).

Dal *patchwork* del quadro normativo applicabile ai trattamenti di dati personali negli USA e dal DPF si può, finalmente, valutare se questo garantisce un livello di protezione dei diritti e delle libertà fondamentali sostanzialmente equivalente a quello che deriva dall'ordinamento dell'UE – e, conseguentemente, se la decisione sull'adeguatezza del livello di protezione dei dati adottata dalla Commissione sia conforme all'art. 45 GDPR e agli art. 7 e 8 e 47 della Carta di Nizza. Occorre operare una distinzione, a questo fine, tra le garanzie in tema di trattamento dei dati da parte delle imprese USA che ricevano dati personali dall'UE e trattino direttamente gli stessi e quelle relative ai cosiddetti *onward transfers*, con particolare riguardo al caso in cui i dati in discorso siano trasferiti ad autorità federali per finalità di sicurezza nazionale. La prima di tali questioni, in ragione della congruità tra i principi sostanziali sul trattamento contenuti nel DPF e quelli desumibili dal GDPR, si può porre, al più, con riguardo alla disponibilità di mezzi di ricorso amministrativo e giurisdizionale in capo agli individui i cui dati siano trasferiti in USA – e, sul punto, si tornerà brevemente al paragrafo 5. La seconda delle questioni summenzionate, in ragione della sua rilevanza sistematica, sarà oggetto di analisi nel paragrafo che segue.

4. Tra le maggiori criticità emerse in sede di scrutinio di legittimità delle decisioni relative ai due sistemi previgenti – *Safe Harbor e Privacy Shield* – va, innanzitutto, menzionata la disciplina delle modalità di accesso delle autorità federali ai dati, raccolti da enti economici siti negli USA e che pertenessero a cittadini UE, per finalità *lato sensu* di intelligence. Pare, quindi, opportuno procedere all'esame del DPF sotto questo profilo, tanto più che, come espressamente affermato dallo European Data Protection Board, «the DPF Principles to which the DPF organisations have to adhere remain essentially unchanged with regard to those applicable under the Privacy Shield» (EDPB, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, adottata il 28 febbraio 2023, p. 2). Si deve, poi, osservare che né i *DPF Principles* né i *Supplemental Principles* del DPF menzionano limiti e condizioni per il trattamento dei dati personali che gli enti economici USA trasferiscano alle autorità federali di intelligence. La finalità di tale omissione può essere, forse, rinvenuta nella volontà di escludere il rischio che le modalità di tutela amministrativa e giurisdizionale per i casi di errata o mancata applicazione dei principi del DPF potessero essere estese anche ai trattamenti di dati posti in essere da pubbliche autorità per finalità di sicurezza nazionale.

Si consideri che le autorità appena menzionate possono accedere a informazioni a carattere personale, trattate da enti economici stabiliti negli USA, sulla base del *Foreign Intelligence Surveillance Act* (d'ora innanzi FISA) o di altra normativa federale che riconosca tale facoltà per finalità di sicurezza nazionale. A ciò si aggiunga la possibilità di raccogliere dati personali al di fuori degli Stati Uniti, ad esempio i dati in transito dall'UE agli USA, sulla base dell'Ordine esecutivo presidenziale 12333 (*Executive Order 12333* of December 8, 1981, on *United States Intelligence Activities*, in ultimo emendato il 30 luglio 2008).

Al fine di regolamentare tanto l'accesso ai dati già trattati negli USA quanto quelli in transito – e a cagione della necessità di tener conto della già menzionata giurisprudenza della Corte di giustizia che, proprio in tema di accesso ai dati da parte delle autorità di intelligence, aveva invalidato i precedenti regimi di trattamento dei dati – il 7 ottobre 2022 il Presidente degli Stati Uniti ha adottato l'Ordine esecutivo 14086 (Executive Order 14086 of October 7, 2022, on *Enhancing Safeguards for United States Signals Intelligence Activities*). Tale ordine esecutivo, di conseguenza, intervenendo tanto sul FISA che sull'Ordine esecutivo 12333, «strenghtens the conditions, limitations and sefeguards that apply to all signals intelligence activities, regardless of where they take place» (in questo senso, la Commissione al considerando 124 della decisione d'adeguatezza in commento).

All'esito della revisione delle procedure che tutte le autorità di intelligence federali sono tenute a seguire quando chiamate a trattare dati personali ricadenti sotto l'ambito applicativo del DPF, conclusasi il 3 luglio 2023, il governo USA ha provveduto alla pubblicazione degli IC elements' policies and procedures to implement the privacy and civil liberties safeguards specified in Executive Order 14086 *Enhancing Safeguards for United States Signals Intelligence Activities* (www.intel.gov). Si consideri, peraltro, che tali procedure sono state adottate con la collaborazione di un organismo indipendente, il *Privacy and Civil Liberties Oversight Board*, di nomina presidenziale, e che il governo federale ha garantito che ogni attività di intelligence su dati provenienti dall'UE sia svolta su disposizione del Presidente degli Stati Uniti ovvero su altra base giuridica idonea e che essa si conformi a quanto previsto dal diritto statunitense, ivi compresa la Costituzione (sezione 2 (a)(i) dell'Ordine esecutivo 14086).

A prescindere dalla considerazione, invero scontata, che, in uno stato di diritto, qualsiasi attività svolta dalle pubbliche autorità – e quindi anche le attività di intelligence – debba essere svolta nel rispetto dei pertinenti requisiti ordinamentali, rimane poco chiaro se e in che misura i cittadini europei, i cui dati siano trattati dalle autorità federali, possano avvalersi del IV emendamento della Costituzione USA, se solo si considera che tali prerogative costituzionali sono solitamente invocabili soltanto dai cittadini USA o da chi ivi risieda da lungo tempo. In altre parole, il richiamo alla necessità che il trattamento di dati personali, trasferiti sulla base del DPF alle autorità federali, abbia luogo nel rispetto delle pertinenti previsioni costituzionali non pare idoneo ad ampliare l'ambito d'applicazione soggettivo delle relative garanzie – e il ragionamento può estendersi *tel quel* alle garanzie previste dalle leggi federali in materia di violazione della privacy.

Di gran lunga più apprezzabile è la previsione per cui le autorità di intelligence possono svolgere le proprie attività sui dati che arrivino dall'UE «to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized» (sezione 2(a)(ii)(B) E.O. 14086). Parrebbe, finalmente e dopo due pronunce del medesimo tenore da parte dei giudici di Lussemburgo, prospettarsi la necessità che, quando chiamate a decidere se effettuare operazioni su dati personali provenienti dall'Unione, le autorità federali effettuino un *bilanciamento* tra la rilevanza degli obiettivi

di intelligence perseguiti, da un lato, e l'impatto delle misure eventualmente adottate sulla privacy e sulle libertà civili degli interessati al trattamento, dall'altro. Come, d'altronde, chiarito nell'Ordine esecutivo, le attività svolte dalle autorità di intelligence sono soggette a supervisione, per garantire il rispetto dei principi di legalità, necessità e proporzionalità (*ibidem*).

All'evidenza, il rispetto dei principi summenzionati riposa sull'effettività della supervisione circa il rispetto dei requisiti previsti dall'Ordine esecutivo 14086. Un primo meccanismo di controllo discende dalla circostanza che la raccolta di dati personali da parte di enti federali per finalità di intelligence è disciplinata dalla sezione 702 del FISA ed è, quindi, soggetta alla supervisione della *Foreign Intelligence Surveillance Court* (di seguito FISC). Tale supervisione, però, non può essere esercitata su richiesta degli individui i cui dati personali siano trattati; viceversa, gli ufficiali incaricati dalle agenzie di intelligence dovranno riferire di ogni violazione circa il trattamento dei dati provenienti dall'UE al Dipartimento di giustizia o all'ODNI (*Office of the Director of National Intelligence*). Tali ultimi organismi dovranno, poi, adire la FISC. All'esito della valutazione della segnalazione ricevuta, la Corte potrà indicare tanto rimedi a carattere individuale che interventi strutturali.

La previsione più rilevante del provvedimento presidenziale, però, ha ad oggetto l'istituzione di un nuovo meccanismo di ricorso di cui gli individui, i cui dati personali siano trattati dalle autorità di intelligence, possono avvalersi (ai sensi della Sezione 5(h), gli individui hanno diritto a richiedere alle autorità giurisdizionali competenti l'applicazione delle garanzie previste dall'Ordine esecutivo 14086). A differenza di quanto previsto circa la competenza della FISC, l'Ordine esecutivo 14086 parrebbe, infatti, istituire un vero e proprio meccanismo di ricorso individuale alla *Data Protection Review Court* (dappresso DPRC). Ogni individuo che risieda nell'Unione europea può, infatti, ricorrere alla DPRC qualora reputi di aver subito una violazione del diritto statunitense applicabile (Executive Order 12333, Executive Order 14086, FISA), qualora ciò comprometta la tutela della privacy o delle libertà civili. Per rendere effettiva la via di ricorso, l'E.O. 14086 (sezione 4(d)(v)) prevede che l'interessato al trattamento possa rivolgersi direttamente all'autorità garante per i dati personali dello Stato membro UE competente. Sarà, poi, quest'ultima ad attivare la competenza della DPRC. Meno rassicurante – nella prospettiva della tutela effettiva della privacy – è la circostanza che le indagini relative ad ogni ricorso proveniente dall'UE siano affidate ad un organismo, facente capo all'esecutivo, il *Civil Liberties and Privacy Officer* dell'ODNI (d'ora innanzi *Officer*). Ciò che desta perplessità è, peraltro, la circostanza che tanto la constatazione dell'avvenuta violazione del diritto statunitense quanto la determinazione delle misure riparatorie siano affidate a tale organismo.

Ove il ricorrente, cui la decisione dell'*Officer* sia stata notificata attraverso il proprio garante per i dati personali, ritenga la stessa insoddisfacente, può finalmente ricorrere alla *Data Protection Review Court*. Si tratta, all'evidenza, di un meccanismo particolarmente complesso, che postula una dettagliata conoscenza del diritto USA applicabile e che, presumibilmente, non potrà essere attivato che in pochi casi (e da parte di interessati al trattamento che ne abbiano i mezzi economici).

Se, per un verso, si può riscontrare un miglioramento in termini di effettività della tutela giurisdizionale rispetto al *Privacy Shield* (nel cui quadro, il controllo sull'uso dei dati da parte delle autorità di intelligence era affidato ad un mediatore, funzionalmente dipendente dall'esecutivo federale), per l'altro, pare dubbio che il meccanismo bifasico *Officer – DPRC* possa essere ritenuto una via di ricorso effettiva ai sensi dell'art. 47 della

Carta di Nizza. Sotto questo profilo, si può forse considerare, in una sorta di giudizio prognostico sul probabile terzo atto della saga *Schrems*, che il *DPF* corre il rischio di non superare il vaglio di legittimità della Corte di giustizia. Una conferma indiretta della vulnerabilità dell'impianto normativo del *DPF*, quanto ai meccanismi di ricorso avverso i trattamenti di dati effettuati dalle autorità federali di intelligence, può desumersi dalla circostanza che la Commissione europea, in sede di redazione della decisione in commento, ha dedicato ampio spazio – nei considerando – alla procedura appena descritta per poi aggiungere che «redress avenues are available to all individuals (irrespective of nationality or place of residence) before ordinary U.S. Courts» (considerando n. 195). La questione è precisamente che il governo statunitense, in sede di negoziazione, non ha accettato di predisporre una via di ricorso aperta a tutti gli individui per quanto concerne i dati personali trasferiti dall'UE. Una tale assenza, nella prospettiva assunta dai giudici di Lussemburgo nella giurisprudenza già menzionata, può difficilmente essere colmata attraverso l'elaborazione di meccanismi spuri che coinvolgano tanto autorità funzionalmente legate al potere esecutivo che autorità giurisdizionali.

Nello stesso senso paiono andare le considerazioni dell'EDPB, secondo cui «the U.S. legal framework, when allowing for the collection of bulk data under Executive Order 12333, lacks the requirement of prior authorization by an independent authority, as required in the most recent jurisprudence of the ECtHR, nor does it provide for a systematic independent review ex post by a Court or an equivalent independent body» (Opinion 5/2023, già citata, p. 5). Quanto all'adeguatezza delle salvaguardie riconosciute agli individui rispetto ai trattamenti di dati da parte delle autorità di intelligence, pare potersi affermare che i cd. bulk transfers (trasferimenti massivi di dati) non sono ancora circondati da garanzie sufficienti e tale assenza – se si pone mente alla rilevanza di tale aspetto nella sentenza Schrems II (par. 183) – potrebbe risultare decisiva in sede di scrutinio giurisdizionale della decisione con cui la Commissione ha ritenuto che il DPF garantisca un'adeguata protezione dei dati personali, se si pone mente alla circostanza che tali trasferimenti massivi di dati verso le autorità di intelligence sono espressamente esclusi per quanto concerne i cittadini statunitensi e sono, invece, consentiti per quanto concerne gli interessati i cui dati provengano dall'UE.

5. Si è già fatto cenno alla circostanza che i Principi adottati dal Dipartimento del Commercio non disciplinano in alcun modo ciò che le pubbliche autorità federali possano fare con i dati personali trasferiti dall'UE a enti economici statunitensi e, quindi, trasmessi alle prime con un *onward transfer* né, per ciò che ci interessa, i rimedi – amministrativi o giurisdizionali – di cui un interessato al trattamento possa avvalersi qualora reputi illecito il trattamento dei propri dati da parte delle autorità federali stesse. Al contrario, i Principi del *DPF* dedicano particolare approfondimento ai meccanismi di tutela dei cittadini UE i cui dati siano trattati dalle imprese e organizzazioni USA che abbiano autocertificato la propria partecipazione al *Data Privacy Framework*. È, probabilmente, questo il più significativo progresso rispetto a quanto avveniva con il *Privacy Shield* e, *a fortiori*, con il *Safe Harbor*.

Come espressamente previsto all'allegato I della decisione sull'adeguatezza in commento, qualora un individuo ritenga che i propri dati personali, trattati nell'UE e quindi trasferiti ad aziende statunitensi, siano oggetto di trattamenti, da parte di queste ultime, che ledano i suoi diritti, ai sensi del *Recourse, Enforcement ad Liability Principle* (Principio 7, lett. a, n. 1), questi dovrà potersi avvalere di un «readily avalilable independent recourse mechanisms by which each individual's complaints and disputes are investigated

and expeditiously resolved». Agli enti economici aderenti al *DPF* viene riconosciuta la facoltà di scegliere un meccanismo di ricorso indipendente, sia esso nell'UE o negli USA. Si consideri che, sulla base delle previsioni dei *Priciples* adottati dal Department of Commerce, si possono prefigurare almeno 6 diverse tipologie di rimedi per l'interessato a un trattamento che reputi violati i propri diritti.

Secondo quanto previsto al *Supplemental Principle* 11, lett. d, un individuo i cui dati, raccolti in UE, siano trasferiti in USA e che ritenga tali siano stati trattati in maniera illecita, potrà innanzitutto rivolgersi all'ente importatore dei dati (è, infatti, obbligatoria, per gli operatori economici che aderiscano al DPF, l'istituzione di un meccanismo formale di valutazione dei ricorsi individuali). In secondo luogo, ci si potrà rivolgere a un *independent dispute resolution body*, cui il soggetto che tratta i dati abbia attribuito la competenza a conoscere eventuali doglianze da parte degli individui interessati. In tal caso, l'organismo di controllo scelto deve disporre del potere di comminare sanzioni o adottare provvedimenti che siano effettivamente idonei a garantire il rispetto dei principi del *DPF*. In caso di mancata esecuzione del provvedimento indicato dall'*independent dispute resolution body*, peraltro, questo è tenuto a segnalare tale omissione al *Department of Commerce* ovvero alla *Federal Trade Commission*.

È, poi, possibile, per gli interessati a un trattamento, indirizzare la propria doglianza direttamente ad una delle autorità garanti per i dati personali degli Stati membri UE (di seguito, garanti nazionali), competente in ragione del luogo ove si trovi l'individuo i cui dati vengano trattati (*EU-US Data Privacy Principles issued by the U.S. Department of Commerce*, sezione III.5.c). Una tale facoltà, però, può essere esercitata esclusivamente ove l'impresa aderente al *DPF* abbia espressamente accettato la supervisione da parte dei garanti nazionali ovvero qualora la questione abbia ad oggetto dati personali raccolti o trattati per finalità connesse alla gestione di risorse umane. A ben vedere, il caso da ultimo menzionato è l'unico rispetto al quale il *DPF* prevede una competenza necessaria dei garanti nazionali, con ciò *esternalizzando* il sindacato circa il rispetto del *Data Privacy Framework* alle autorità europee – a prescindere dalla questione dell'*enforcement* delle relative deliberazioni, necessariamente affidata alle autorità federali.

Qualora il provvedimento reso da un garante nazionale sia disatteso, infatti, l'inadempimento, da parte dell'impresa destinataria dei dati dall'UE, potrà condurre a una procedura innanzi alla *Federal Trade Commission* o, nei casi di *persistent failure to comply*, il Dipartimento del Commercio potrà espungere l'impresa in discorso da quelle che usufruiscono del regime di trasferimento dei dati nel contesto del *DPF*. Le altre tre modalità attraverso cui un individuo possa far valere una sua doglianza consistono nell'indirizzare un'istanza al Dipartimento del Commercio – *rectius*, al garante nazionale competente, il quale, a sua volta, girerà al primo l'istanza stessa; nel rivolgersi direttamente alla *Federal Trade Commission* (si tenga conto che la violazione dei principi del DPF è equiparata ad una pratica commerciale scorretta ai sensi della sezione 5 del *Federal Trade Commission Act*); nell'attivare, come *extrema ratio*, l'arbitrato obbligatorio del *EU-US Data Privacy Framework Panel* (disciplinato nell'allegato ai Principi del Dipartimento del Commercio).

Da questa necessariamente sintetica analisi emerge che il nuovo sistema, negoziato dalla Commissione con le competenti autorità statunitensi, non ha condotto alla previsione di vere e proprie vie di ricorso giurisdizionali. Rimangono accessibili i rimedi – questi realmente giurisdizionali – che l'ordinamento statunitense non riservi ai soli cittadini o residenti di lungo periodo, primo tra tutti il *Tort Law*.

La constatazione di tale carenza – strutturale – quanto alle possibilità per gli interessati a un trattamento di dati in USA di accedere a una Corte federale, non può non avere conseguenze in tema di valutazione dell'equivalenza del livello di protezione, ponendo mente a quanto prevede il già menzionato art. 47 della Carta di Nizza. Secondo la Corte di giustizia, d'altro canto, «legislation not providing for any possibility for an individual to pursue *legal remedies* in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to judicial protection, as enshrined in art. 47 of the Charter» (sentenza *Schrems*, già citata, par. 95, corsivo nostro). Secondo questa interpretazione, la presenza di rimedi, anche di carattere *lato sensu* amministrativo, potrebbe essere sufficiente a non compromettere l'essenza del diritto ad una tutela giurisdizionale effettiva, a meno di non voler interpretare l'espressione *legal remedies* – rimedi giuridici nella infelice traduzione in lingua italiana – come rimedi giurisdizionali in senso stretto – e cioè un vero e proprio diritto di accesso al giudice. Se l'interpretazione da darsi al *dictum* dei giudici di Lussemburgo fosse nel senso di comprendere anche i rimedi *lato sensu* amministrativi, si potrebbe reputare che, quantomeno con riguardo ai rimedi che i cittadini europei, i cui dati siano trasferiti in USA sulla base del DPF, hanno a disposizione nei confronti degli operatori economici che tali dati trattino, non vi siano particolari difformità in termini di garanzie procedurali.

Ad avviso di chi scrive, viceversa, lo standard desumibile dall'art. 47 della Carta di Nizza imporrebbe che, per far valere un diritto ivi tutelato, il titolare di tale diritto possa accedere a un giudice – con le relative garanzie in tema di indipendenza, imparzialità etc. Se questa fosse la reale portata precettiva della norma in discorso, si dovrebbe concludere che lo standard minimo di tutela di tale diritto, così come definito dalla summenzionata giurisprudenza della Corte di Lussemburgo, si affievolisca ai fini della determinazione dell'adeguatezza del livello di protezione garantito dall'ordinamento straniero verso cui sia legittimo inviare dati personali. In buona sostanza, le libertà e i diritti fondamentali, sul cui livello di tutela si fonda l'affermazione dell'equivalenza del livello di protezione, si troverebbero a ricevere – quantomeno con riguardo al diritto a una tutela giurisdizionale effettiva – una tutela *quasi* equivalente a quelle che discende dall'ordinamento dell'Unione europea, con ciò contraddicendo la ratio dell'art. 45 GDPR.

6. Con questa breve, e necessariamente sommaria, analisi del nuovo regime giuridico di trasferimento dei dati personali da parte di operatori economici UE verso operatori economici USA, si è cercato di dar conto delle possibili antinomie tra la decisione sull'adeguatezza che la Commissione ha reso al fine di approvare siffatto regime, da un lato, e il GDPR – in particolare gli art. 45 e 46 – e gli art. 7, 8 e 47 della Carta di Nizza, dall'altro.

Quanto ai principi che regolano, nel nuovo *Data Privacy Framework*, le modalità di trattamento dei dati personali da parte degli enti (privati) che tali dati ricevano negli Stati Uniti, si è già osservato come si possa ravvisare una sostanziale equivalenza con i principi sul trattamento contenuti nel GDPR. Se ne può concludere che, in presenza di una supervisione accurata delle autorità federali sul rispetto di tali principi ad opera degli operatori economici, inclusi nella *DPF List* sulla base di un'autocertificazione, il livello di protezione dei dati personali che scaturisce dall'applicazione del DPF è ragionevolmente congruo con quanto avviene nell'UE.

La questione centrale, a nostro avviso, attiene invece ai meccanismi di implementazione del DPF e di vigilanza sul rispetto dello stesso, in ragione del fatto che, come si è

accennato poc'anzi, un individuo, che risieda in uno Stato membro UE e che ritenga violata la propria privacy da un trattamento dei propri dati effettuato oltreoceano, non è necessariamente in grado di accedere a un giudice statunitense che possa imporre a chi tale trattamento abbia effettuato il ripristino della legalità violata.

Sempre in questa prospettiva *rimediale*, la più evidente lacuna nella tutela della privacy dei cittadini UE i cui dati siano trattati negli USA, attiene, ancora una volta e nonostante la Corte di giustizia sia intervenuta per ben due volte con decisioni del medesimo tenore (sentenze *Schrems* I e II), alle modalità di trattamento di tali dati per finalità di sicurezza nazionale da parte delle autorità federali. E ciò per due ordini di ragioni: innanzitutto perché trattare per scopi di intelligence dati raccolti per fini commerciali significa, in sostanza, derogare al principio della finalità limitata (e una tale deroga dovrebbe essere circondata da adeguate cautele) e, in secondo luogo, perché il privato non ha la certezza di poter adire un giudice federale in grado di rivedere le operazioni sui dati personali effettuati dalle autorità di intelligence. E ciò è tanto più grave in quanto i *bulk transfers*, come si è avuto modo di osservare, sono vietati negli USA quanto ai dati dei cittadini statunitensi ma sono viceversa ammessi con riguardo ai dati provenienti dall'UE.

Pur non volendo svolgere un a dir poco complesso giudizio prognostico, pare molto probabile che la Corte di giustizia sarà nuovamente chiamata a pronunciarsi sul regime applicabile ai flussi transfrontalieri di dati verso gli USA per finalità commerciali. Ove ciò fosse, le questioni già sollevate nella sentenza *Schrems II* rischierebbero di essere ritenute non risolte dalla Commissione europea, con la conseguenza della (terza) declaratoria di invalidità.

Alfredo Terrasi[*]

Abstract. EU-US Data Privacy Framework: Much Ado About Nothing?

The present paper deals with the recent Decision by the European Commission, defining a new Data Privacy Framework, applicable to transborder data flows from EU companies to US companies. Such a mechanism aims to overcome the case-law of the European Court of Justice on the former data flows systems (Safe Harbor and Privacy Shield). Whilst the substantive principles on data elaboration seem to comply with the EU legal standard – granting an equivalent protection to EU citizens' rights – the procedural guarantees stemming from the DPF could be still inconsistent with the above-mentioned standard. The main question, probably unsolved, regards the ways of redress for individuals whose data are transferred from the EU to a US companies and, then, onward transferred to federal intelligence authorities. One could, in fact, wonder whether the right of access to a judge is guaranteed or not by the DPF. Accordingly, it is quite plausible that the Data Privacy Framework will be brought to the ECJ in order to determine its consistency with GDPR, on the one hand, and the relevant provisions of the European Union Charter of Fundamental Rights, on the other.

Keywords: personal data; transborder data flows; legal remedies; intelligence activities; adequacy decision; equivalent level of protection.

[*] Ricercatore di Diritto internazionale nell'Università degli Studi di Palermo, Dipartimento di Giurisprudenza, Via Maqueda, 172 – 90133 Palermo, alfredo.terrasi@unipa.it