ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

13 GENNAIO 2021

La saga *Schrems* e la tutela dei diritti fondamentali

di Chiara Gentile
Dottoranda di ricerca in Diritto dell'Unione europea e ordinamenti nazionali
Università degli Studi di Ferrara

La saga *Schrems* e la tutela dei diritti fondamentali*

di Chiara Gentile
Dottoranda di ricerca in Diritto dell'Unione europea e ordinamenti nazionali
Università degli Studi di Ferrara

Abstract [It]: Il contributo si propone di delineare il quadro europeo della protezione dei dati personali e dei diritti fondamentali nel contesto dei trasferimenti dei dati all'estero, alla luce della saga *Schrems* e dei conseguenti risvolti pratici. Dopo aver ripercorso i passaggi salienti della sentenza *Schrems I* e l'evoluzione della normativa europea, si intende analizzare la più recente sentenza *Schrems II* ed evidenziarne gli aspetti innovativi e le maggiori criticità, prendendo in considerazione anche le pertinenti misure adottate dal Comitato europeo per la protezione dei dati.

Abstract [En]: The paper aims at outlining the European framework of the protection of personal data and fundamental rights in the context of the transfer of personal data abroad, in the light of the *Schrems* saga and its practical implications. After reviewing the main steps of the *Schrems I* judgment and the evolution of European Union law, it will analyze the most recent *Schrems II* judgment and highlight its innovative aspects and its most critical issues, taking into account also the relevant measures adopted by the European Data Protection Board.

1. Introduzione

Il trasferimento dei dati personali all'estero è stato oggetto di due importanti sentenze in ambito sovranazionale, ccdd. *Schrems I*[1] e *Schrems II*[2], in cui la Corte di giustizia dell'Unione europea (Corte) si è pronunciata sull'adeguatezza del livello di protezione dei dati personali garantito dagli Stati Uniti ai cittadini europei, riscontrando che la normativa statunitense non assicura un livello di protezione sostanzialmente equivalente a quello garantito dall'Unione a causa delle ingerenze nel diritto fondamentale alla privacy e dell'assenza di rimedi giurisdizionali effettivi. La cd. saga *Schrems* alimenta significativamente il dibattito sul rapporto tra libera circolazione dei dati personali e tutela dei diritti fondamentali, enfatizzandone gli aspetti più problematici che necessitano di ulteriori delucidazioni.

* Articolo sottoposto a referaggio.
[1] CGUE, 6.10.2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*.
[2] CGUE, 16.7.2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems*.

Il contributo intende ricostruire il quadro attuale della protezione dei dati personali e della tutela dei diritti fondamentali nel contesto dei trasferimenti dei dati all'estero, soffermandosi sui principi affermati nella saga *Schrems* e analizzandone le implicazioni e i risvolti pratici. Si richiameranno in via preliminare i passaggi significativi di *Schrems I*, con cui la Corte è stata investita, per la prima volta, della questione della tutela dei dati personali trasferiti verso gli Stati Uniti e ha invalidato la decisione della Commissione di esecuzione dell'accordo cd. «approdo sicuro». In secondo luogo, si ripercorrerà l'evoluzione, in seguito a *Schrems I*, del regime dei trasferimenti dei dati tra l'Unione europea e gli Stati Uniti, operato sulla base prima delle clausole contrattuali tipo di protezione dei dati e poi della decisione di esecuzione del nuovo accordo cd. «scudo per la privacy»; contestualmente, si considererà il passaggio dalla direttiva 95/46 al Regolamento generale per la protezione dei dati 2016/679 (RGPD). In terza istanza si compirà un'analisi dettagliata della sentenza *Schrems II*, con cui la Corte invalida la decisione di esecuzione dell'accordo «scudo per la privacy» e si focalizza sulle nuove disposizioni del RGPD, in particolare quelle concernenti i trasferimenti transfrontalieri dei dati e i poteri delle autorità nazionali di controllo. Se da un lato sono presenti chiari elementi di continuità rispetto alla precedente *Schrems I*, dall'altro *Schrems II* solleva nuovi problemi e lascia una serie di questioni irrisolte, su cui si tornerà nella seconda parte del contributo. Oltre alle maggiori criticità relative ai trasferimenti dei dati all'estero che emergono dalla saga *Schrems*, si esamineranno le recenti misure adottate dal Comitato europeo per la protezione dei dati in materia di circolazione e protezione dei dati personali e di tutela dei diritti fondamentali. Nelle riflessioni finali si prenderanno in considerazione gli effetti della declaratoria di invalidità dello «scudo per la privacy», che, per la seconda volta, lascia i trasferimenti dei dati personali verso gli Stati Uniti privi di una base giuridica *ad hoc*.

2. L'antefatto: *Schrems I*

In seguito alle dichiarazioni di Edward Snowden del 2013[3], da cui erano emerse gravi violazioni dei diritti fondamentali da parte della *National Security Agency* (NSA) statunitense nel corso di attività di sorveglianza globale sulle comunicazioni telefoniche e sul traffico di rete, Maximillian Schrems, cittadino austriaco, chiedeva al Commissario per la protezione dei dati irlandese (Commissario) di impedire a Facebook Ireland di trasferire i propri dati personali a Facebook Inc., negli Stati Uniti, per via dell'accesso libero e incondizionato dei servizi segreti americani ai dati contenuti nei server di Facebook Inc. Il trasferimento dei dati dall'Unione europea agli Stati Uniti avveniva sulla base della decisione di adeguatezza 2000/520

[3] G. GREENWALD, E. MACASKILL, *NSAPrism program taps in to user data of Apple, Google and others*, in *The Guardian*, 7.6.2013. Sul punto: F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it*, 26.6.2013.

della Commissione, cd. decisione «approdo sicuro», adottata ai sensi dell'art. 25, par. 6, dir. 95/46. Avverso il rigetto del Commissario, il sig. Schrems proponeva ricorso dinanzi alla *High Court*, la quale, rinvenendo possibili profili di contrasto con il diritto dell'Unione, rinviava alla Corte, chiedendo se e in quale misura l'art. 25, par. 6, dir. 95/46, letto alla luce degli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (Carta), consentisse all'autorità di controllo di uno Stato membro di esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà fondamentali, con riguardo al trattamento dei propri dati personali trasferiti verso un paese terzo sulla base di una decisione di adeguatezza della Commissione, allorché ritenesse che il diritto del paese terzo non garantisse un livello di protezione dei dati adeguato.

I punti salienti della sentenza *Schrems I* possono riassumersi come segue[4]. Anzitutto, la Corte riconosce alle autorità di controllo nazionali il potere, ai sensi dell'art. 28 dir. 95/46, di esaminare una domanda nei termini di cui sopra quando la persona lamenti che il diritto e la prassi in vigore nel paese terzo non garantiscono un livello di protezione adeguato; tuttavia, fintantoché la decisione di adeguatezza non sia stata dichiarata invalida dalla Corte, gli Stati membri e le autorità di controllo non possono adottare misure ad essa contrarie. In secondo luogo, la Corte precisa che l'ordinamento giuridico del paese terzo interessato dalla decisione della Commissione deve assicurare un livello di protezione dei dati non identico, bensì «sostanzialmente equivalente» a quello garantito dall'Unione, in forza della dir. 95/46, letta alla luce della Carta. Infine, la Corte dichiara invalida la decisione 2000/520 della Commissione, sostenendo che l'ordinamento statunitense non garantisce un livello di protezione adeguato dei dati personali, poiché, consentendo alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche, senza che gli individui interessati dispongano di alcun rimedio giuridico effettivo per accedere ai propri dati personali, oppure per ottenerne la revoca o la soppressione, viola il contenuto essenziale del diritto fondamentale al rispetto della vita privata, di cui all'art. 7 della Carta[5], e del diritto fondamentale a una tutela giurisdizionale effettiva, di cui all'art. 47 della Carta.

[4] Per un'attenta analisi si rinvia a O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, in *Medialaws*, 2018, pp. 138-163; C. LAM, *Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in* Schrems v. Irish Data Protection Commissioner, in *40 BCIntl&CompLRev*, 2017, pp. 1-13; R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. cost.*, 2016, pp. 289-307; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Diritto internazionale*, 2016, pp. 690-724; S. CRESPI, *La tutela dei dati personali UE a seguito della sentenza Schrems*, in *Eurojus*, 2.11.2015.

[5] La Corte non si pronuncia invece sull'interferenza con l'essenza del diritto alla tutela dati personali di cui all'art. 8 della Carta (cfr. V.M. PFISTERER, *The Right to Privacy – A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, in *GerLawJ*, 2019, 20, p. 732).

In *Schrems I* la Corte propende per un ampliamento della protezione dei dati personali, interpretando estensivamente le pertinenti disposizioni della dir. 95/46, alla luce della Carta[6], e conseguentemente enfatizza la supremazia valoriale dei diritti in essa sanciti[7]. Tale impostazione «fundamental rights oriented» segna l'abbandono della concezione mercantilistica della circolazione dei dati personali in favore di una maggiore tutela dei diritti fondamentali garantiti dall'Unione[8]. Il passaggio a tal proposito più significativo è quello relativo al giudizio dell'art. 25, par. 6, dir. 95/46, nella parte in cui richiede che il paese terzo assicuri un «livello di protezione adeguato» dei dati personali ivi trasferiti. La conversione del parametro di adeguatezza in quello di sostanziale equivalenza operato in *Schrems I* postula un'indagine comparativa tra forme di tutela previste nell'ordinamento straniero e quelle garantite a livello sovranazionale: l'obiettivo di assicurare la continuità del livello protezione dei dati tra l'Unione europea e il paese destinatario del trasferimento dei dati segna l'estensione delle garanzie sovranazionali al di fuori dei confini europei[9].

Vista la rilevanza delle questioni relative ai diritti fondamentali affrontate nella sentenza, il 13.4.2016 il Gruppo di lavoro "Articolo 29"[10] ha elaborato un documento in cui ha individuato quattro cd. garanzie essenziali europee[11]: *a*) il trattamento dei dati dovrebbe basarsi su norme chiare, precise e accessibili; *b*) si deve dimostrare la necessità e la proporzionalità delle interferenze nei diritti in relazione agli obiettivi legittimi perseguiti; *c*) dovrebbe esistere un meccanismo di controllo indipendente; *d*) l'individuo deve avere a disposizione rimedi effettivi[12]. Siffatte garanzie costituiscono un parametro guida per determinare se le interferenze nei diritti fondamentali siano legittime nel contesto di qualsiasi trattamento dei dati personali, includendo dunque i trasferimenti all'estero[13].

---

[6] O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel* reasoning *dei giudici di Lussemburgo*, in *Diritto dell'informazione e dell'informatica*, 2015, p. 747. Sottolineano gli autori che la Carta non era ancora stata approvata quando era entrata in vigore la dir. 95/46.

[7] Precisamente, agli artt. 7 e 8 della Carta (cfr. G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Diritto dell'informazione e dell'informatica*, pp. 782-783).

[8] Così O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di* digital privacy *come osservatorio privilegiato*, cit., p. 159.

[9] *Ibid.*, p. 156; O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel* reasoning *dei giudici di Lussemburgo*, cit., p. 752.

[10] Era il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati, previsto dall'art. 29 della dir. 95/46.

[11] Gruppo di lavoro "Articolo 29", *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*, in https://ec.europa.eu/, 13.4.2016. Tale documento contiene una valutazione complessiva delle conseguenze della sentenza *Schrems I* su tutti i trasferimenti di dati verso gli Stati Uniti. A tal fine, è stata presa in considerazione la giurisprudenza rilevante in materia di sorveglianza elettronica della Corte di giustizia, relativa agli articoli 7, 8 e 47 della Carta, e della Corte europea dei diritti dell'uomo, relativa all'art. 8 della Convenzione europea dei diritti dell'uomo.

[12] L'utilizzo del condizionale nelle lett. *a*) e *c*), e dell'indicativo nelle lett. *b*) e *d*), riflette l'utilizzo nella versione originale del documento, rispettivamente, di «should» e «need to» (*Ibid.*).

[13] *Ibid.*, p. 3.

3. Il trasferimento dei dati personali verso gli Stati Uniti e la tutela dei diritti fondamentali nel quadro normativo europeo

A partire dalla declaratoria di invalidità della decisione «approdo sicuro», il trasferimento dei dati personali tra Unione europea e Stati Uniti è rimasto privo di un quadro normativo *ad hoc*, ed è avvenuto sulla base delle clausole contrattuali tipo di protezione dei dati contenute nell'allegato alla decisione 2010/87 della Commissione del 5.2.2010, cd. decisione CPT, modificata dalla decisione di esecuzione 2016/2297 della Commissione del 16.12.2016.

Successivamente alla conclusione di un nuovo accordo con gli Stati Uniti, cd. accordo «scudo per la privacy», che introduce un sistema di autocertificazione, da parte di imprese americane registrate in un apposito elenco, secondo cui le proprie politiche sono in linea con i parametri fissati dall'accordo[14], la Commissione ha adottato, ai sensi dell'art. 25 dir. 95/46, la decisione di esecuzione 2016/1250, cd. decisione «scudo per la privacy», il 12.7.2016[15]. Tale decisione sancisce all'art. 1, par. 1 e 2, che gli Stati Uniti assicurano un livello di protezione adeguato dei dati personali trasferiti dall'Unione alle organizzazioni statunitensi nell'ambito dello «scudo», costituito dai principi emanati dal Dipartimento del Commercio degli Stati Uniti il 7.7.2016, riportati nell'allegato II, e dalle dichiarazioni e dagli impegni ufficiali riportati nei documenti di cui agli allegati I e III-VII.

Medio tempore, la dir. 95/46 è stata abrogata e sostituita dal Regolamento sulla protezione dei dati 2016/679 (RGPD) del 27.4.2016[16], divenuto pienamente applicabile il 25.5.2018: si è voluto predisporre un quadro normativo aperto al futuro e adeguato a fornire una maggiore tutela alle varie forme di trattamento dei

[14] Le caratteristiche dell'accordo «scudo per la privacy» sono esaminate da M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione* Schrems *della Corte di giustizia UE*, in *Diritto dell'Unione europea*, 2016, pp. 773-776; P. PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza* Schrems *e nel nuovo regolamento generale sulla protezione dei dati*, in *Diritto dell'informazione e dell'informatica*, 2015, pp. 827-864.

[15] Sulla decisione, si vedano Gruppo di lavoro "Articolo 29", *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, in *www.ec.europa.eu*, 13.4.2016; S. CRESPI, *La nuova proposta di decisione di adeguatezza della commissione europea riguardo agli Usa: lo scudo UE/USA per la privacy*, in *Eurojus*, 26.4.2016.

[16] Sulle ragioni per cui l'Unione europea ha preferito lo strumento del Regolamento e, in generale, sulle differenze tra la dir. 95/46 e il RGPD, si veda F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali*, vol. I (*Dalla Direttiva 95/46 al nuovo Regolamento europeo*), Torino, 2016 (soprattutto: Parte prima e Parte seconda). Per un'analisi del RGPD, si vedano, *ex multis*, G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Bologna, 2017; C. COLAPIETRO, L. CALIFANO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, vol. II (*Il regolamento europeo 2016/679*), Torino, 2016. Il RGPD si aggiunge ad altri due strumenti normativi volti a innovare il quadro normativo europeo in tema di tutela dei dati personali: la direttiva 2016/680 del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI; e la direttiva 2016/681 del 27.4.2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

dati, anche in previsione delle inevitabili evoluzioni della tecnologia digitale[17]. Il RGPD dà attuazione al diritto fondamentale alla protezione dei dati personali come riconosciuto nella Carta, all'art. 8, e nel Trattato sul funzionamento dell'Unione europea, all'art. 16[18]. Esso introduce maggiori garanzie, *inter alia*, per il trasferimento transfrontaliero dei dati[19] e rafforza i poteri e l'indipendenza delle autorità nazionali di controllo[20]. L'art. 1 RGPD dichiara il duplice oggetto del nuovo strumento normativo: la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati medesimi. Tali due ambiti di regolamentazione sono pari ordinati, senza che l'uno possa considerarsi prevalente sull'altro[21]. Il RGPD si propone, quindi, di tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, senza peraltro limitare la libera circolazione dei dati, nonché di contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica[22]. Si osservi, tuttavia, che ai sensi del considerando 2 RGPD i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali «*dovrebbero* rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali» (corsivo aggiunto): l'utilizzo del condizionale anziché dell'indicativo sembra suggerire l'assenza di una vera pari-ordinazione tra tutela dei diritti fondamentali e libera circolazione dei dati. Va da sé, infatti, che conciliare le due esigenze, intrinsecamente conflittuali, pone problemi interpretativi e applicativi non indifferenti[23].

4. *Schrems II*

Su invito del Commissario, il sig. Schrems ha riformulato la propria denuncia chiedendo che il trasferimento dei suoi dati personali verso Facebook Inc. fosse vietato o sospeso, facendo valere, in

[17] F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *Medialaws*, 2018, p. 109; P. GONNELLI, *Le misure correttive previste dall'art. 58, paragrafo 2, del GDPR, nel sistema sanzionatorio a tutela dei dati personali*, in F. ROSSI DAL POZZO, *Mercato Unico Digitale, dati personali e diritti fondamentali*, 2020, pp. 117-121.

[18] Considerando 1 RGPD; F. PIZZETTI, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 8.

[19] Per un'attenta analisi, cfr., *ex multis*, S. KIRSCHEN, *Il trattamento all'estero dei dati*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al GDPR, Regolamento EU n. 679/2016 e al d.lgs. n. 101/2018*, Milano, 2019, pp. 261-291; G.M. RICCIO, F. PEZZA, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, 2019, pp. 585-617.

[20] F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, cit., in particolare pp. 108-114. Si segnala, inoltre, che il Gruppo di lavoro "Articolo 29" è stato sostituito con il Comitato europeo per la protezione dei dati *ex* art. 94 RGPD.

[21] Così, *ex multis*, G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy: commentario*, Assago, 2018, p. 4.

[22] Cfr. art. 1, par. 2 e 3, e considerando 2 RGPD; L. DURST, *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al GDPR, Regolamento EU n. 679/2016 e al d.lgs. n. 101/2018*, Milano, 2019, p. 41.

[23] Su questo aspetto si tornerà *infra* (par. 6).

particolare, l'incompatibilità del trattamento dei dati da parte delle autorità statunitensi di *intelligence* con gli artt. 7, 8 e 47 della Carta. Nel corso delle proprie indagini il Commissario ha riscontrato il rischio che i dati fossero trattati in modo incompatibile con il diritto dell'Unione, dal momento che le clausole contrattuali tipo contenute nell'allegato alla decisione CPT, sulla base della quale era avvenuto il trasferimento, non vincolavano in alcun modo le autorità pubbliche statunitensi. Conseguentemente, il 31.5.2016 il Commissario ha presentato ricorso alla *High Court* affinché questa adisse la Corte.

Oltre a condividere le censure sollevate dal Commissario, la *High Court* ne rileva di ulteriori in relazione alla decisione «scudo per la privacy» della Commissione, e pertanto, in data 4.5.2018 rinvia alla Corte sottoponendole ben undici questioni pregiudiziali. In sostanza il giudice rimettente ritiene che l'ordinamento statunitense non assicuri un adeguato livello di protezione dei dati personali dei cittadini europei per via dell'assenza di limiti alle possibili ingerenze dei servizi segreti americani. I controversi atti normativi sono tre: il *Foreign Intelligence Surveillance Act* (FISA) nell'art. 702, l'*Executive Order* (E.O.) 12333 e la *Presidential Policy Directive* 28 (PPD-28).

L'art. 702 FISA consente all'*intelligence* nazionale di autorizzare, previa approvazione della Corte FISA, la sorveglianza di cittadini stranieri che si trovano al di fuori del territorio degli Stati Uniti. Su questo articolo si fondano i programmi di sorveglianza PRISM e UPSTREAM, nell'ambito dei quali le imprese di telecomunicazioni e i fornitori di servizi Internet sono tenuti a trasmettere alla NSA tutte le comunicazioni inviate e ricevute da un «selettore». L'E.O. 12333 consente alla NSA di accedere ai dati in transito verso gli Stati Uniti e di raccogliere e conservare tali dati prima che siano soggetti alle disposizioni del FISA. Le attività di *intelligence* dirette nei confronti di cittadini stranieri devono rispettare le misure dettate nella PPD-28, che tuttavia, secondo il giudice rimettente, non pone limiti alle operazioni delle autorità statunitensi se non richiedendo che siano «as tailored as feasible». Secondo quanto constatato da tale giudice, i cittadini dell'Unione non hanno accesso agli stessi mezzi di ricorso di cui dispongono i cittadini statunitensi contro i trattamenti di dati personali da parte delle autorità nazionali, e le attività della NSA basate sull'E.O. 12333 non sono soggette a controlli o ricorsi giurisdizionali ai sensi dell'art. 47 della Carta.

La risposta della Corte si articola in cinque sezioni, e prende in considerazione le disposizioni del nuovo RGPD, che sostanzialmente riproducono (e integrano) le pertinenti disposizioni della dir. 95/46.

4.1. Sicurezza nazionale e applicazione del Regolamento generale per la protezione dei dati

Anzitutto la *High Court* chiede se l'art. 2, par. 1 e par. 2, lett. *a*), *b*) e *d*), RGPD, che escludono l'applicabilità del RGPD al trattamento dei dati personali effettuato nel corso di una serie di attività proprie degli Stati

o delle autorità statali[24], in combinato disposto con l'art. 4, par. 2 TUE, secondo cui «la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro», costituiscano una base ostativa all'applicazione del RGPD qualora durante o in seguito al trasferimento dei dati tra operatori economici privati, dall'Unione verso un paese terzo, tali dati vengano ulteriormente trattati dalle autorità pubbliche del paese terzo per fini di sicurezza pubblica, di difesa e di sicurezza dello Stato.

La Corte ritiene, ai fini dell'interpretazione delle richiamate disposizioni dell'art. 2 RGPD, non pertinente l'art. 4, par. 2, TUE, dal momento che esso, nel rimettere la sicurezza nazionale alla competenza esclusiva dei singoli Stati, menziona i soli Stati membri dell'Unione, ed esclude inoltre l'applicazione al caso di specie dell'art. 2, par. 2, lett. *a*), *b*) e *d*), RGPD, poiché si riferiscono ad attività proprie di Stati o autorità statali, e non di operatori privati, quali Facebook Ireland e Facebook Inc. Presupposto per l'applicabilità del RGPD è il trattamento dei dati personali ai sensi dell'art. 4, par. 2, RGPD, che menziona, a titolo esemplificativo, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione», senza distinguere a seconda che ciò avvenga all'interno dell'Unione o verso un paese terzo. La possibilità che i dati trasferiti tra due operatori economici a fini commerciali subiscano, durante o in seguito al trasferimento, un trattamento ulteriore a fini di pubblica sicurezza, di difesa e di sicurezza dello Stato da parte delle autorità del paese interessato non osta all'applicazione del RGPD.

4.2. Il livello di protezione dei dati trasferiti verso paesi terzi

Il giudice rimettente interroga la Corte sul livello di protezione richiesto dall'art. 46, par. 1 e par. 2, lett. *c*), RGPD, nell'ambito di un trasferimento di dati personali verso un paese terzo sulla base di clausole tipo, e su quali elementi basarsi per verificare che esso sia effettivamente garantito. Il giudice chiede altresì se tale livello di protezione debba essere determinato alla luce del diritto dell'Unione, e/o della Convenzione europea dei diritti dell'uomo (CEDU) o del diritto interno degli Stati membri.

Ai sensi dell'art. 46, par. 1, RGPD, in assenza di una decisione di adeguatezza adottata dalla Commissione *ex* art. 45, par. 1, RGPD, il titolare o il responsabile del trattamento può trasferire dati personali verso un paese terzo solo se ha fornito «garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi». L'art. 46, par. 2, lett. *c*), RGPD, prevede che possono costituire «garanzie adeguate» le clausole tipo di protezione dei dati adottate dalla Commissione, quali sono le dodici clausole previste nell'allegato alla decisione CPT.

[24] Si tratta di attività che non rientrano nell'ambito di applicazione del diritto dell'Unione (lett. *a*) o che ricadono nell'ambito di applicazione del Titolo V, capo II, TUE (lett. *b*), oppure di attività aventi fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse (lett. *d*).

Il ragionamento seguito dalla Corte muove dall'art. 44 RGPD, che stabilisce il principio generale secondo cui le disposizioni del capo V, in cui sono collocati gli artt. 45 e 46, si applicano al fine di assicurare che il livello di protezione delle persone fisiche garantito dal RGPD non sia pregiudicato. In linea con quanto statuito in *Schrems I*[25], la Corte afferma che nel caso di una decisione di adeguatezza della Commissione, l'art. 45, par. 1, RGPD, letto congiuntamente al considerando 104, esige che il paese terzo garantisca un livello di protezione delle libertà e dei diritti fondamentali non identico, bensì sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza del RGPD, letto alla luce della Carta. La Corte estende detto requisito anche al caso in cui manchi una siffatta decisione della Commissione, richiamando in particolare il considerando 108, secondo cui le adeguate garanzie che il titolare o il responsabile del trattamento deve adottare conformemente all'art. 46, par. 1, devono «compensare la carenza di protezione dei dati in un paese terzo» per «assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione». Quanto ai parametri normativi da prendere in considerazione per verificare l'adeguatezza di tali garanzie, la Corte menziona le disposizioni del RGPD e della Carta, escludendo le fonti esterne: la CEDU, che non costituisce un atto giuridico formalmente integrato nell'ordinamento giuridico dell'Unione, e, in mancanza di un richiamo espresso, il diritto interno e le costituzioni degli Stati membri.

Infine, tra gli elementi su cui basarsi per valutare il livello di protezione dei dati, la Corte individua sia le clausole contrattuali convenute tra titolare o responsabile del trattamento stabilito nell'Unione e destinatario del trasferimento stabilito nel paese terzo, sia i fattori rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati, in modo non esaustivo, all'art. 45, par. 2, GDPR (lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la legislazione generale e settoriale e le misure attuative; la presenza di autorità di controllo indipendenti con poteri effettivi a garanzia del rispetto delle norme in materia di protezione dei dati; gli impegni internazionali assunti dal paese terzo).

4.3. I poteri correttivi delle autorità di controllo nazionali

La Corte è chiamata a pronunciarsi sull'interpretazione dell'art. 58, par. 2, lett. *f)* e *j)*, RGPD, onde stabilire se l'autorità di controllo nazionale è tenuta a esercitare i poteri correttivi ivi riconosciuti e, pertanto, a sospendere o vietare il trasferimento di dati personali verso un paese terzo effettuato sulla base delle clausole contrattuali tipo, allorché ritenga che tali clausole non siano o non possano essere rispettate nel paese terzo e che non possa garantirsi il livello di protezione richiesto dal diritto dell'Unione.

[25] *Schrems I*, par. 73.

La Corte risponde affermativamente, ponendo in capo all'autorità di controllo il dovere di sospendere o vietare il trasferimento di dati personali laddove il titolare o il responsabile del trattamento stabilito nel territorio dell'Unione non vi abbia già provveduto. L'adozione di clausole tipo ai sensi dell'art. 46, par. 2, lett. *c*), RGPD, non permette alla Commissione di limitare l'esercizio dei poteri che l'art. 58, par. 2, RGPD conferisce alle autorità nazionali. Queste ultime sono invece vincolate al rispetto di una decisione di adeguatezza di cui all'art. 45 RGPD, in presenza della quale non possono impedire il trasferimento di dati verso il paese terzo interessato, a meno che (e fintanto che) la Corte non ne dichiari l'invalidità. In termini analoghi a *Schrems I*[26], la Corte ribadisce che le autorità di controllo devono comunque poter esaminare, in piena indipendenza, eventuali reclami sollevati da persone fisiche relativi alla protezione dei loro diritti e, laddove ne ritengano fondate le doglianze, devono poter proporre ricorso dinanzi al giudice nazionale affinché proceda a un rinvio pregiudiziale diretto all'esame della validità della decisione di adeguatezza della Commissione.

4.4. Clausole contrattuali tipo e misure supplementari

La *High Court* chiede se il fatto che le clausole contrattuali vincolano solo le parti contraenti, e non anche le autorità nazionali del paese terzo, escluda che queste offrono garanzie adeguate ai sensi dell'art. 46 RGPD e, più precisamente, se la decisione CPT sia in violazione degli artt. 7, 8 e/o 47 della Carta.

La Corte muove dalla premessa secondo cui le clausole tipo potrebbero non costituire un mezzo sufficiente per garantire un'effettiva protezione dei dati personali laddove, per esempio, il diritto del paese terzo consentisse alle autorità statali di porre in essere attività ingerenti nei diritti individuali. Diversamente dalla decisione adottata ai sensi dell'art. 45 RGPD, in cui la Commissione constata che la normativa interna del paese terzo, specie quella relativa alla sicurezza nazionale e all'accesso delle autorità pubbliche ai dati personali, assicura effettivamente un livello di protezione dei dati adeguato, una decisione come la CPT non richiede una simile valutazione di carattere generale, spettando invece al titolare o responsabile del trattamento l'onere di verificare, caso per caso, che il paese terzo fornisca garanzie adeguate e che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Dal momento che la natura contrattuale delle clausole tipo non consente di vincolare le autorità pubbliche del paese terzo, la Corte pone in capo al titolare o al responsabile del trattamento, eventualmente in collaborazione con il destinatario del trasferimento, l'onere di integrare, ove necessario, dette clausole con misure supplementari[27], al fine di assicurare un livello di protezione adeguato dei dati personali.

[26] In particolare, *Schrems I*, par. 52-53, 57.

[27] La Corte richiama in particolare il considerando 109, RGPD, secondo cui: «la possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione [...] non dovrebbe precludere [...] di aggiungere altre clausole o garanzie supplementari».

Qualora ciò sia impossibile, il titolare o il responsabile, o in subordine l'autorità di controllo, deve sospendere o impedire il trasferimento.

Il fatto che una decisione adottata ai sensi dell'art. 46, par. 2, lett. *c*), RGPD non vincoli le autorità pubbliche non ne determina *ex se* l'invalidità laddove essa preveda meccanismi efficaci che garantiscano, in concreto, il livello di protezione richiesto dal diritto dell'Unione. La Corte si concentra quindi sulle singole clausole contenute nell'allegato alla decisione CPT, in virtù delle quali il titolare del trattamento dei dati personali stabilito nell'Unione e il destinatario del trasferimento nel paese terzo si impegnano a far sì che trattamento e trasferimento siano effettuati conformemente alla «normativa sulla protezione dei dati», in cui rientrano il RGPD e la Carta (clausole 4, lett. *a*) e *b*); 5, lett. *a*); 9; 11, par. 1). Come precisato dalla nota a piè di pagina relativa alla clausola 5, eventuali disposizioni vincolanti della legislazione dello Stato terzo «che non vanno oltre quanto è necessario» in una società democratica per salvaguardare, tra l'altro, la sicurezza dello Stato, la difesa e la sicurezza pubblica, non si pongono in contrasto con le suddette clausole tipo. Il destinatario si impegna a comunicare prontamente al titolare del trattamento la sua eventuale impossibilità di conformarsi agli obblighi contrattuali, nonché qualsiasi modificazione della normativa nazionale che possa pregiudicare le garanzie e gli obblighi previsti dalle clausole tipo (clausola 5, lett. *a*) e *b*)). In entrambi i casi, per conformarsi ai requisiti di cui all'art. 46, par. 1 e par. 2, lett. c), RGPD, letto congiuntamente agli artt. 7 e 8 della Carta, il titolare del trattamento è tenuto a sospendere il trasferimento di dati e/o risolvere il contratto, oppure, se intende proseguire il trasferimento o revocarne la sospensione, deve informare l'autorità di controllo competente, che può procedere a verifiche (clausola 4, lett. *g*)). Se il titolare del trasferimento comunica al responsabile del trattamento che la legislazione del paese terzo non gli consente di conformarsi alle clausole tipo, tutti i dati già trasferiti e le relative copie devono essere restituiti o distrutti (clausola 12).

Inoltre, la decisione CPT non impedisce all'autorità di controllo competente di interdire il trasferimento effettuato sulla base delle clausole tipo. Nel caso in cui non possa essere garantito un adeguato livello di protezione dei dati e gli operatori privati rimangano inerti, l'autorità di controllo è tenuta a sospendere o vietare il trasferimento (art. 58, par. 2, lett. *f*) e *j*), RGPD); se invece ritiene che i trasferimenti debbano, in generale, essere vietati verso un particolare paese terzo, essa può adire il Comitato europeo per la protezione dei dati (CEPD) affinché adotti una decisione vincolante *ex* art. 65, par. 1, lett. *c*), RGPD, così da evitare che le autorità nazionali di diversi Stati membri prendano posizioni divergenti.

Alla luce delle suddette considerazioni, la Corte conclude che la decisione CPT prevede meccanismi efficaci che garantiscono il livello di protezione richiesto dal diritto dell'Unione e ne esclude l'invalidità.

4.5. Decisione «scudo per la privacy» e rispetto dei diritti fondamentali

Infine, il giudice remittente chiede se il trasferimento verso gli Stati Uniti di dati personali sul fondamento delle clausole tipo violi i diritti garantiti dagli artt. 7 e/o 8 della Carta; se le restrizioni imposte dalla legge statunitense al diritto a un ricorso giurisdizionale effettivo rispettino il contenuto essenziale dell'art. 47 della Carta e, in caso affermativo, se siano proporzionate ai sensi dell'art. 52 della stessa, e se l'istituzione del Mediatore sia compatibile con l'art. 47; se e in quale misura la decisione «scudo per la privacy» vincoli le autorità di controllo nazionali[28].

La Corte esamina la decisione, soffermandosi anzitutto sulla deroga espressa al punto I.5 dell'allegato II, secondo cui l'adesione ai principi generali riportati nell'allegato può essere limitata «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia». Analogamente a quanto prevedeva la decisione «approdo sicuro» invalidata in *Schrems I*, la decisione «scudo per la privacy» sancisce il primato delle suddette esigenze sui principi generali e il conseguente obbligo delle organizzazioni statunitensi autocertificate che ricevono dati dall'Unione di disapplicare, senza limiti, i principi generali qualora interferiscano con tali esigenze. Si rendono pertanto possibili gravi ingerenze, per motivi di sicurezza nazionale, nei diritti fondamentali di coloro i cui dati personali siano trasferiti verso gli Stati Uniti – ingerenze che possono derivare dall'accesso ai dati da parte delle autorità di *intelligence* e dall'ulteriore utilizzo degli stessi nell'ambito dei programmi di sorveglianza PRISM e UPSTREAM.

Successivamente la Corte indaga sull'adeguatezza del livello di protezione dei dati ai sensi dell'art. 45 RGPD, letto alla luce degli artt. 7 e 8 della Carta. L'accesso ai dati personali e la loro comunicazione a un'autorità pubblica incidono sul diritto al rispetto della vita privata, di cui all'art. 7 della Carta, indipendentemente da quale sia l'utilizzo che l'autorità ne faccia o dall'eventuale natura sensibile dei dati, e costituiscono inoltre «trattamento di dati» ai sensi del successivo art. 8. Tuttavia – ribadisce la Corte – i diritti sanciti agli artt. 7 e 8 non si atteggiano a prerogative assolute, ma vanno considerati alla luce della loro funzione sociale. In questo contesto si colloca l'art. 52, par. 1, della Carta, che postula che le limitazioni dei diritti fondamentali rispettino i seguenti requisiti: da un lato, tali limitazioni devono essere previste dalla legge e devono rispettare il contenuto essenziale dei diritti (prima frase); dall'altro, esse possono essere apportate, nel rispetto del principio di proporzionalità, solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (seconda frase). Il requisito della proporzionalità si intende soddisfatto

[28] La decisione «scudo per la privacy» viene adottata in epoca successiva rispetto alle indagini del Commissario; tuttavia, sia il giudice di rinvio che la Corte sottolineano di essere tenuti a prendere in considerazione il mutamento delle circostanze derivanti dalla suddetta decisione e gli effetti vincolanti che ne scaturiscono.

se la legge che disciplina l'ingerenza contiene regole chiare e precise, che definiscano la portata e l'applicazione della misura interessata, e mette a disposizione degli individui garanzie per proteggere efficacemente i propri dati personali contro il rischio di abusi. Nel caso di specie, i programmi di sorveglianza basati sia sull'art. 702 FISA che sull'E.O. 12333 non incontrano alcuna restrizione nel contesto di attività di *intelligence* esterna, né esistono garanzie per i cittadini stranieri che ne sono potenzialmente oggetto. Tali programmi devono essere attuati in ossequio alla direttiva PPD-28, che se da un lato impone una serie di vincoli alle operazioni di *intelligence*, dall'altro consente di procedere alla raccolta in blocco di informazioni o dati senza conferire agli interessati diritti azionabili dinanzi ai giudici, contrariamente a quanto richiesto dall'art. 45, par. 2, lett. *a*), RGPD. Alla luce di tali considerazioni, la Corte esclude che sia assicurato un livello di protezione sostanzialmente equivalente a quello richiesto dall'art. 52, par. 1, seconda frase, della Carta.

Con riferimento all'art. 47 della Carta, la Corte prosegue sulle orme di *Schrems I*[29] e afferma che una normativa che non riconosce al singolo la possibilità di avvalersi di rimedi giuridici per accedere ai dati personali che lo riguardano, oppure per ottenerne la rettifica o la soppressione, non rispetta il contenuto essenziale del diritto fondamentale a una tutela giurisdizionale effettiva. A tale proposito la Commissione deve considerare i mezzi di «ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento» (art. 45, par. 2, lett. *a*), RGPD), e verificare che il paese terzo assicuri «un effettivo controllo indipendente della protezione dei dati» (considerando 104 RGPD). L'art. 702 FISA e l'E.O. 12333 non riconoscono agli interessati diritti azionabili dinanzi ai giudici, privandoli dunque di un ricorso effettivo.

Per ciò che concerne infine il Mediatore, nella decisione «scudo per la privacy» la Commissione stabilisce che tale figura permette di garantire un livello di protezione sostanzialmente equivalente a quello previsto dall'art. 47 della Carta. La Corte sottolinea diversi aspetti che mettono in dubbio l'indipendenza del Mediatore, e precisamente: esso riferisce direttamente al Segretario di Stato, che assicura che svolga la sua funzione con obiettività; forma parte integrante del Dipartimento di Stato degli Stati Uniti; è designato dal Segretario di Stato, senza che siano previste garanzie particolari sull'annullamento della nomina o sulla sua revoca. Inoltre, nonostante la decisione della Commissione menzioni un impegno del governo statunitense a far sì che i servizi di *intelligence* rettifichino qualsiasi violazione individuata dal Mediatore, non si evince con chiarezza se il Mediatore sia autorizzato ad adottare atti vincolanti nei loro confronti, né se le persone fisiche interessate dispongano di garanzie giuridiche. La Corte conclude per l'inadeguatezza del meccanismo di mediazione al rispetto dell'art. 47.

[29] *Schrems I*, par. 95.

In conclusione, la Corte dichiara invalido l'art. 1 della decisione «scudo per la privacy» perché incompatibile con l'art 45, par. 1, RGPD, letto alla luce degli artt. 7, 8 e 47 della Carta, e tale invalidità investe la decisione nella sua interezza.

5. Problematiche interpretative e applicative connesse alla protezione dei dati personali

Come emerge dalla precedente disamina di *Schrems II*, la Corte torna su alcuni principi affermati in *Schrems I* e ne integra la portata, ma al contempo lascia aperte una serie di questioni di primaria importanza nella disciplina della circolazione dei dati personali. Gli aspetti che suscitano maggiori perplessità sono: la vaghezza del concetto di sostanziale equivalenza e delle modalità concrete per determinarla; l'entità dell'onere conoscitivo degli ordinamenti stranieri imposto agli operatori economici privati e alle autorità nazionali di controllo; l'indeterminatezza delle misure supplementari (eventualmente) richieste ai suddetti operatori privati.

Innanzitutto, la Corte afferma che il livello di protezione dei dati personali garantito da un paese terzo deve essere sostanzialmente equivalente a quello assicurato dal diritto dell'Unione, individuando gli elementi in base ai quali compiere una siffatta valutazione nell'elenco non esaustivo di cui all'art. 45, par. 2, RGPD, e, quando il trasferimento dei dati ha luogo ai sensi dell'art. 46, par. 1 e par. 2, lett. *c*), anche nelle clausole contrattuali tipo: viene dunque riproposta la manipolazione del testo normativo, già compiuta in *Schrems I*, con la quale la Corte aveva ricavato dal concetto di adeguatezza espressamente utilizzato negli artt. 45 e 46 RGPD quello di equivalenza[30].

Tuttavia non è chiaro cosa si intenda, in concreto, con "sostanziale equivalenza". Taluni concetti richiamati dall'art. 45, par. 2, RGPD, quali "stato di diritto", "diritti umani" e "libertà fondamentali" sono estremamente ampi, «*open-textured*» e privi di «*universal meaning*»[31], e potrebbero prestarsi a interpretazioni o rigide e restrittive, al punto che solo pochi paesi terzi riuscirebbero a soddisfare lo *standard* di adeguatezza imposto dall'Unione europea, o, viceversa, vaghe e indefinite, che rischierebbero di non offrire garanzia alcuna.

Inoltre, la Corte limita al RGPD e alla Carta i parametri normativi di riferimento per l'accertamento del livello di protezione dei dati, escludendo espressamente il diritto interno degli Stati membri. Viene spontaneo chiedersi cosa accadrebbe se si verificasse una situazione in cui la tutela dei diritti fondamentali dei singoli, con riferimento al trattamento dei dati personali, fosse più incisiva a livello nazionale piuttosto che a livello sovranazionale. Se, per esempio, nel corso del trasferimento dei dati verso un paese terzo l'autorità di controllo di uno Stato membro ritenesse la protezione dei dati garantita da tale paese

[30] O. POLLICINO, *Diabolical Persistence. Thoughts on the Schrems II Decision*, in *VerfBlog*, 25.7.2020.
[31] J.X. DHONT, *Schrems II. The EU adequacy regime in existential crisis?*, in *MaastrichtJEurCompL*, 2019, p. 598.

conforme alle disposizioni del RGPD, lette alla luce della Carta, ma inferiore rispetto a quella assicurata dal diritto costituzionale interno, e proponesse ricorso davanti all'autorità giudiziaria, quest'ultima come dovrebbe comportarsi[32]?

Le maggiori criticità di *Schrems II*, tuttavia, riguardano la "privatizzazione" della valutazione del livello di protezione dei dati garantito dal paese terzo, che viene rimessa al titolare o al responsabile del trattamento stabilito nel territorio dell'Unione, e la revisione "decentralizzata" da parte delle autorità di controllo nazionali[33]. L'obbligo di sospendere o vietare il trasferimento dei dati se il paese terzo non garantisce un livello di protezione sostanzialmente equivalente a quello dell'Unione comporta un onere eccessivo per il titolare e il responsabile del trattamento, a cui sarà demandata la conoscenza approfondita dell'ordinamento giuridico straniero, nel suo insieme, e delle forme di tutela dei dati personali ivi previste. Possibili complicazioni potrebbero verificarsi con riguardo alla legislazione straniera in materia di sorveglianza[34], oppure nel caso in cui il destinatario del trasferimento sia in un paese non democratico o che non rispetta lo stato di diritto[35]. Un analogo onere conoscitivo grava anche sulle autorità di controllo nazionali, nel momento in cui sia ad esse richiesto di esercitare i propri poteri correttivi, con il rischio che le autorità di taluni Stati membri agiscano in modo più "protettivo" di altre, e dunque che venga a delinearsi un quadro europeo di tutela dei dati personali e dei diritti fondamentali individuali non uniforme[36]. Per scongiurare un simile scenario, la Corte opera una sorta di "ri-centralizzazione" del

[32] Con specifico riferimento all'Italia, nel caso in cui la violazione di un diritto fondamentale infranga, al contempo, sia le disposizioni della Costituzione sia quelle della Carta, la Corte costituzionale ha dapprima affermato la necessità di un intervento *erga omnes* della Corte medesima e, pertanto, il giudice è tenuto a sollevare «la questione di legittimità costituzionale, fatto salvo il ricorso, al rinvio pregiudiziale per le questioni di interpretazione o di invalidità del diritto dell'Unione» (sent. cost. 269/2017). Tale posizione è stata temperata nella giurisprudenza successiva, in cui la Corte parla di «opportunità» del suo intervento, fermo restando che «i giudici comuni possono sottoporre alla Corte di giustizia dell'Unione europea, sulla medesima disciplina, qualsiasi questione pregiudiziale a loro avviso necessaria» (sent. cost. 20/2019), «anche dopo il giudizio incidentale di legittimità costituzionale» (sent. cost. 63/2019). In tale contesto si colloca anche l'ultimo rinvio pregiudiziale sollevato dalla Corte costituzionale alla Corte di giustizia, ord. 117/2019.

[33] T. CHRISTAKIS, *After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, in *EuLawBlog*, 21.7.2020.

[34] Non è chiaro se tale indagine conoscitiva si estenda, oltre che alla normativa, anche alla *prassi* dei servizi segreti (cfr. J.P. MELTZER. *The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security*, in *VoxEu*, 5.8.2020).

[35] Così C. KUNER, *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, in *EuLawBlog*, 17.7.2020. Sul piano geopolitico, *Schrems II* avrà un impatto più grave sui flussi di dati verso la Cina, la Russia e altri stati autoritari, nonché, in seguito alla *Brexit*, sui flussi verso il Regno Unito (K. PROPP, P. SWIRE, *Geopolitical Implications of the European Court's Schrems II Decision*, in *LawfareBlog*, 17.7.2020).

[36] Parla di «tutela a macchia di leopardo» R. BIFULCO, *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno*, in *DPER online*, 2/2020, p. 7. Si consideri, per esempio, che subito dopo la sentenza *Schrems II* il Commissario tedesco per la protezione dei dati e la libertà di informazione ha richiesto ai responsabili del trattamento di trasferire in Europa i dati personali memorizzati negli Stati Uniti (*After "Schrems II": Europe needs digital independence*, press release, in www.datenschutz-berlin.de/, 17.7.2020).

giudizio di adeguatezza[37], incaricando il CEPD di coordinare le diverse autorità nazionali e risolvere eventuali conflitti, esercitando i poteri riconosciuti dagli artt. 64 e 65 RGPD.

La Corte impone al titolare o al responsabile del trattamento di integrare, se del caso, le clausole contrattuali tipo con misure supplementari, non specificando in cosa queste misure debbano consistere, né indicando la forma o il contenuto necessari affinché tali misure siano, in concreto, effettive o soddisfacenti[38]. Il CEPD ha adottato il 10.11.2020 delle apposite raccomandazioni per orientare le scelte operative degli operatori economici privati e cercare, così, di colmare il vuoto lasciato da *Schrems II* e di promuovere l'applicazione uniforme del RGPD[39]. Lo schema di azione che il CEPD raccomanda di seguire si articola in sei fasi. È anzitutto fondamentale tracciare il percorso di tutti i trasferimenti all'estero, e, in secondo luogo, assicurarsi che, in mancanza di una decisione *ex* art. 45 RGPD, siano soddisfatti i requisiti di cui all'art. 46 RGPD (e solo in caso di trasferimenti occasionali e non ripetitivi le deroghe di cui all'art. 49 RGPD). La terza fase consiste nel valutare se le garanzie di cui all'art. 46 RGPD siano effettive, oppure se la loro effettività possa essere compromessa dalla legislazione o dalla prassi del paese terzo. Più precisamente, si invita l'operatore privato a considerare le leggi del paese terzo che impongono obblighi di divulgazione dei dati personali alle autorità pubbliche o accordano a tali autorità poteri di accesso ai dati personali (per esempio, ai fini dell'applicazione del diritto penale, dell'esercizio dei poteri di vigilanza e per motivi di sicurezza nazionale)[40]; tuttavia, si puntualizza che se tali obblighi e poteri sono limitati a ciò che è necessario e proporzionato in una società democratica, essi *potrebbero* non interferire con il rispetto delle condizioni fissate dall'art. 46 RGPD[41]. Per l'accertamento dell'effettività dei rimedi giuridici o della proporzionalità delle ingerenze governative nei dati personali, alla luce degli artt. 47 e 52 della Carta, agli esportatori è chiesto di considerare anche gli altri elementi elencati nell'art. 45, par. 2, RGPD, quali lo stato di diritto e gli impegni internazionali dello Stato destinatario dei trasferimenti[42]. Inoltre, gli esportatori sono tenuti a conoscere anche la prassi locale e, in generale, le informazioni relative al paese terzo desumibili dalla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte

[37] Così T. CHRISTAKIS, *After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, cit.

[38] R.A. COSTELLO, Schrems II*: Everything is Illuminated?*, in *5 European Papers*, 2020, p. 1054.

[39] CEPD, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, in www.edpb.europa.eu, 10.11.2020. Precedentemente, il CEPD aveva istituito una *task force* avente il compito, tra l'altro, di elaborare raccomandazioni per i titolari e i responsabili del trattamento nell'individuazione e nell'attuazione di adeguate misure supplementari (CEPD, *37esima sessione plenaria: Linee-guida su titolare e responsabile del trattamento; Linee-guida sul targeting degli utenti dei social media; Task force sui reclami presentati a seguito della sentenza Schrems II*, 4.10.2020, reperibile sul sito del Garante privacy italiano).

[40] *Ibid.*, par. 36.

[41] Nella versione originale: «they *may* not impinge on the commitments contained in the Article 46 GDPR transfer tool you are relying on» (corsivo aggiunto), *Ibid.*, par. 36 ultima frase.

[42] *Ibid.*, par. 37-38.

europea dei diritti dell'uomo, dalle risoluzioni e relazioni di organizzazioni intergovernative (quali il Consiglio d'Europa e gli organismi e le agenzie delle Nazioni Unite), dalla giurisprudenza nazionale o dalle decisioni delle autorità amministrative indipendenti competenti in materia di protezione dei dati personali, dalle relazioni delle istituzioni accademiche e organizzazioni della società civile (ONG e associazioni)[43]. Qualora dalla valutazione della legislazione e della prassi del paese terzo risulti pregiudicata l'effettività delle garanzie di cui all'art 46 RGPD, nella quarta fase l'esportatore è tenuto ad adottare, in accordo con l'importatore, misure supplementari per assicurare la sostanziale equivalenza della protezione dei dati garantita nell'Unione. Siffatte misure possono essere di natura tecnica, contrattuale o organizzativa, e affinché si raggiunga lo *standard* di protezione europeo è possibile che debbano combinarsi misure di tipologie distinte, quali, per esempio: la trasmissione di «pseudonymised data»; l'inserimento di clausole contrattuali che impongono agli operatori obblighi di trasparenza o di adottare specifiche misure tecniche; l'impegno a documentare e registrare le richieste di accesso ai dati ricevute dalle autorità pubbliche e le relative risposte; l'attuazione di rigorose politiche interne sulla sicurezza dei dati[44]. Se non riesce a garantirsi un livello di protezione dei dati sostanzialmente equivalente a quello dell'Unione nonostante le misure supplementari, il trasferimento non può essere iniziato o, se in corso, deve essere sospeso o impedito; se l'operatore privato decide comunque di procedere, deve informare l'autorità di controllo nazionale che, se del caso, deve vietare il trasferimento. La quinta fase prevede la definizione delle regole procedurali necessarie per rendere operative ed effettive le singole misure supplementari adottate. Qualora intenda modificare le clausole di protezione dei dati o introduca misure in contraddizione con esse, l'esportatore deve chiedere l'autorizzazione all'autorità di controllo competente[45]. Infine, è richiesto agli operatori privati di monitorare costantemente gli sviluppi nel paese terzo che potrebbero influire sul livello di protezione dei dati ivi assicurato, ed è ribadito il dovere delle autorità di controllo nazionali di intervenire, in qualunque momento, nel caso di inadempienza degli operatori privati, nonché di coordinare le proprie azioni con il CEDP per garantire coerenza nell'applicazione del diritto dell'Unione in materia di protezione dei dati.

Le suddette raccomandazioni forniscono agli esportatori lo schema da seguire per determinare, se del caso, quali misure supplementari debbano essere adottate affinché i trasferimenti dei dati avvengano conformemente agli *standard* europei; eppure, dal momento che le misure supplementari non vincolano altri soggetti oltre alle parti contrattuali tra cui sono convenute, esse rischiano di non rivelarsi di grande utilità per impedire lo svolgimento di operazioni di sorveglianza o altre attività intrusive da parte delle

[43] *Ibid.*, par. 42-43; par. 138 (in allegato 3).
[44] *Ibid.*, par. 80, 97 ss., 99 ss., 127 ss., 135 ss. (in allegato 2).
[45] *Ibid.*, par. 57. Il ragionamento seguito in *Schrems II* per le clausole contrattuali tipo (art. 46, par. 2, lett. *c*) e *d*), RGPD) si estende anche agli altri strumenti menzionati dall'art. 46, par. 2, RGPD (*Ibid.*, par. 58-61).

autorità pubbliche del paese terzo. Se si considera, in particolare, che l'assenza di rimedi giurisdizionali effettivi è una delle ragioni che ha condotto alla declaratoria di invalidità della decisione «scudo per la privacy», risulta difficile immaginare garanzie suppletive che possano essere adottate da soggetti privati[46]. Si tenga presente, infine, che trattandosi di mere raccomandazioni, perciò non aventi carattere obbligatorio, esse non rappresentano lo strumento ideale per conseguire nella maniera più efficace l'applicazione uniforme del RGPD, come interpretato in *Schrems II*[47].

6. Il consolidamento della tutela dei diritti fondamentali

Sebbene il RGPD, come si è detto, ponga sullo stesso piano la libera circolazione dei dati personali e la tutela dei diritti fondamentali, vi è chi ha letto nella equivalenza prospettata tra privacy e libera circolazione dei dati un rapporto inevitabilmente conflittuale: la tensione in parte ineludibile fra tendenze più spiccatamente economicistiche ed esigenze di protezione dei diritti non può essere risolta che tramite un opportuno bilanciamento[48]. L'approccio seguito in *Schrems II* conferma l'intenzione della Corte, già manifestata in *Schrems I*, di voler rafforzare la tutela dei diritti fondamentali nel contesto dei trasferimenti all'estero dei dati personali: se già *Schrems I* aveva conferito all'art. 7 della Carta una dimensione particolare, costituendo una tappa importante nella costruzione di un diritto che, in parallelo alla crescita e allo sviluppo della tecnologia, sta assumendo un ruolo centrale nell'azione dell'Unione europea[49], *Schrems II* segna un'evoluzione delle argomentazioni ivi prospettate, con ulteriori ricadute sulla dogmatica dei diritti fondamentali.

In *Schrems II* la Corte espande e articola il ragionamento intorno ai diritti al rispetto della vita privata e al trattamento dei dati personali, affermando che non sono prerogative assolute, ma vanno considerati alla luce della loro funzione sociale, e che eventuali ingerenze si giustificano solo se rispettose del contenuto essenziale dei diritti (art. 52, par. 1, prima frase, della Carta) e del principio di proporzionalità (art. 52, par. 2, seconda frase, della Carta). Il giudizio sulla proporzionalità in particolare rappresenta un elemento di assoluta novità rispetto alla precedente sentenza del 2015: in *Schrems I* la Corte, pur riscontrando che non è limitata allo stretto necessario una normativa che autorizzi in maniera generale (senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito) la conservazione dei dati trasferiti dall'Unione

[46] T. CHRISTAKIS, *After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, cit.

[47] Si segnala, per completezza, che in data 29.10.2020 il Garante europeo per la protezione dei dati personali ha predisposto una strategia (*Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling*) volta ad assicurare che le istituzioni, gli organi e gli organismi dell'Unione europea agiscano nel rispetto di *Schrems II*.

[48] L. DURST, *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, cit., pp. 59-60. L'autrice richiama il pensiero di Rodotà, che si interrogava su quanto il RGPD proponesse un bilanciamento diverso a vantaggio dei diritti fondamentali, rispetto alle priorità tradizionalmente accordate ad altre esigenze quali sicurezza e mercato.

[49] R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, cit., pp. 298-299.

verso gli Stati Uniti, poneva l'accento sull'esigenza che una siffatta normativa non pregiudicasse il contenuto essenziale del diritto al rispetto della vita privata come garantito dall'art. 7 della Carta[50]. Analogamente, l'assenza di rimedi giuridici effettivi era stata ritenuta violativa del contenuto essenziale del diritto a una tutela giurisdizionale effettiva di cui all'art. 47 della Carta[51]. In *Schrems II*, invece, la Corte, da una parte, nella valutazione delle ingerenze nei diritti di cui agli artt. 7 e 8, decide di esaminare solamente il principio di proporzionalità, non ritenendo necessario verificare preliminarmente il rispetto, da parte degli Stati Uniti, delle condizioni fissate dall'art. 52, par. 1, prima frase; dall'altra, con riguardo all'art. 47, concentra il proprio giudizio sul contenuto essenziale del diritto. Il percorso argomentativo seguito in *Schrems II* non sembra del tutto lineare, poiché prima la Corte riconosce che le ingerenze dei servizi segreti statunitensi nei dati personali trasferiti non sono bilanciate dal riconoscimento di un controllo giurisdizionale, in contrasto con il principio di proporzionalità, ma alla fine, quando passa a considerare l'art. 47, conclude che la mancanza di rimedi giuridici per gli interessati costituisce violazione del contenuto essenziale del diritto a una tutela giurisdizionale effettiva, senza più considerare la proporzionalità: se a esser stato violato è il contenuto essenziale, non si intende per quale motivo la Corte afferma di voler condurre l'analisi alla luce dell'art. 52, par. 1, seconda frase[52].

In seguito a *Schrems II* il CEPD ha aggiornato, con nuove raccomandazioni[53], il documento elaborato dal Gruppo di lavoro "Articolo 29" nel 2016, al fine di fornire elementi utili per valutare se le attività di *intelligence* condotte dalle autorità di un paese terzo si traducano in ingerenze nei diritti fondamentali legittime. Nelle raccomandazioni si rimarca che eventuali limitazioni ai diritti di cui agli artt. 7 e 8 della Carta devono, nel rispetto del principio di proporzionalità, circoscriversi a quanto strettamente necessario in una società democratica ed essere bilanciate dall'interesse generale perseguito[54]; in secondo luogo, si integrano le informazioni contenute nel documento del 2016 con le più recenti sentenze in materia di sorveglianza elettronica della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo[55]. Il CEPD ribadisce che, nel contesto dei trasferimenti internazionali di dati personali, le

[50] *Schrems I*, par. 93-94. Non è da escludere che in *Schrems I* la Corte abbia voluto evitare il giudizio sulla proporzionalità della limitazione del diritto fondamentale alla privacy, come garantito dalla Carta, per via di un interesse esterno, quale la sicurezza nazionale degli Stati Uniti (cfr. M. BRKAN, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, in *GerLawJ*, 2019, 20, p. 875).

[51] *Schrems I*, par. 95.

[52] *Schrems II*, par. 178, 187-194; R. BIFULCO, *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno*, cit., pp. 15-16.

[53] CEPD, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, in www.edpb.europa.eu, 10.11.2020.

[54] *Ibid.*, par. 18-22.

[55] *Ibid.*, par. 24-47.

quattro garanzie essenziali europee sono un punto di riferimento nella valutazione delle interferenze nei diritti fondamentali[56].

Un'osservazione finale attiene all'applicazione spaziale dei diritti fondamentai sanciti nella Carta. In *Schrems II*, nonostante la dichiarazione di invalidità riguardi una decisione della Commissione, l'esame della (in)adeguatezza del regime statunitense di protezione dei dati personali verte su condotte esterne, poste in essere da autorità pubbliche straniere al di fuori del territorio dell'Unione: la Corte analizza dettagliatamente la legislazione statunitense e le forme di tutela riconosciute ai cittadini europei nell'ambito delle operazioni di *intelligence*, operando un confronto con le garanzie individuali assicurate dalla Carta, sulla base di quella che sembra un'applicazione extraterritoriale dei diritti fondamentali. Inoltre, il principio di sostanziale equivalenza implicitamente impone a quei paesi che intendano scambiare dati con soggetti stabiliti negli Stati membri un obbligo di adeguamento della propria normativa nazionale a quella europea, di fatto estendendo la tutela dei diritti fondamentali assicurata dall'Unione al di là dei propri confini territoriali. Dalla saga *Schrems*, e specialmente da *Schrems II*, emerge che nel momento in cui i dati personali si spostano verso paesi terzi deve garantirsi continuità al livello di protezione assicurato nell'Unione, e quindi l'extraterritorialità dei diritti fondamentali riguarda essenzialmente i trasferimenti dei dati all'estero; in questo modo, tuttavia, non si tiene in debita considerazione un profilo ulteriore che dimostra il bisogno di estendere i diritti fondamentali al di fuori dei confini europei: la sorveglianza esterna[57]. Nell'ambito delle operazioni di sorveglianza esterna condotte dagli Stati Uniti, la cittadinanza, la residenza o la presenza di un individuo sul territorio statunitense sono elementi dirimenti per il godimento del diritto alla privacy e l'esercizio di rimedi giurisdizionali effettivi, e infatti i cittadini europei rimangono sprovvisti di una tutela equivalente a quella riconosciuta all'interno dell'Unione. In definitiva, *Schrems II* potrebbe costituire il punto di partenza di un dibattito più articolato sull'applicazione extraterritoriale dei diritti fondamentali.

7. Quale futuro per il trasferimento dei dati personali verso gli Stati Uniti?

La Corte sostiene che l'invalidità con effetto immediato della decisione «scudo per la privacy» non crea alcuna lacuna giuridica, dal momento che in mancanza di una decisione della Commissione *ex* art. 45 RGPD o di garanzie adeguate *ex* art. 46 RGPD, i trasferimenti transfrontalieri di dati possono avvenire alle condizioni indicate nell'art. 49 RGPD[58], che ammette in via derogatoria il trasferimento su consenso

[56] *Ibid.*, par. 56.
[57] M. TZANOU, Schrems I *and* Schrems II*: Assessing the Case for the Extraterritoriality of EU Fundamental Rights*, in https://papers.ssrn.com/, 13.10.2020, pp. 19-20 (destinato a *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart Publishing, in corso di pubblicazione).
[58] *Schrems II*, par. 202.

espresso dell'interessato oppure nei casi di necessità ivi elencati[59]. Detta soluzione è difficilmente condivisibile perché in contrasto con le linee guida del CEPD[60], secondo cui le deroghe sancite nell'art. 49 RGPD non forniscono una tutela e garanzie adeguate per il trasferimento dei dati personali ed espongono a maggiori rischi i diritti e le libertà fondamentali degli interessati. Conseguentemente tali deroghe possono trovare applicazione solamente per trasferimenti "occasionali" o "non ripetitivi"[61] e l'esportatore deve valutare se il trasferimento possa considerarsi necessario rispetto al fine perseguito (cd. test di necessità)[62]. Nelle FAQ pubblicate dal CEPD il 23.7.2020 si precisa ulteriormente che l'art. 49, specie per la deroga di cui alla lett. *d*) per «importanti motivi di interesse pubblico», non autorizza trasferimenti sistematici o su larga scala, richiedendo l'osservanza del principio generale secondo cui l'applicazione delle deroghe dovrà essere limitata a situazioni specifiche, strettamente necessarie, e non divenire la regola[63]. Dunque le deroghe di cui all'art. 49, non essendo designate per i trasferimenti strutturali e continuativi[64], non possono colmare il vuoto che segue all'invalidazione della decisione «scudo per la privacy»[65]. A tale riguardo è auspicabile un intervento tempestivo della Commissione, quale potrebbe essere la conclusione di un nuovo accordo con gli Stati Uniti per regolamentare il trasferimento dei dati personali[66].

Si osservi tuttavia che l'accordo «scudo per la privacy» non ha ovviato ai problemi che presentava l'accordo «approdo sicuro», in particolare per la preminenza delle esigenze di sicurezza nazionale sulla protezione dei dati personali dei cittadini europei e la contestuale assenza di rimedi giuridici effettivi[67]. Il combinato delle sentenze *Schrems I* e *Schrems II* evidenzia la perdurante inadeguatezza della normativa

[59] L'art. 49 RGPD consente il trasferimento dei dati personali all'estero se vi è «consent or necessity», cfr. CHANDER, *Is Data Localization a Solution for* Schrems II*?*, in *JIEL*, 2020, p. 775.

[60] CEPD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, in https://edpb.europa.eu/, 25.5.2018. Analoghe line guida sono contenute in Gruppo di lavoro "Articolo 29", *Guidelines on Article 49 of Regulation 2016/679*, in https://ec.europa.eu/, 6.2.2018.

[61] Soluzione ribadita in CEPD, *Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, in https://edpb.europa.eu/, 17.7.2019.

[62] CEPD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, cit., pp. 4-5. Detto test di necessità deve essere applicato per valutare la possibilità del ricorso alle deroghe di cui all'art. 49, par. 1, lett. *b*), *c*), *d*), *e*) ed *f*) RGPD.

[63] CEPD, *FAQ*, in https://edpb.europa.eu/, 23.7.2020.

[64] J.X. DHONT, *Schrems II. The EU adequacy regime in existential crisis?*, cit.

[65] C. KUNER, *Schrems II Re-Examined*, in *VerfBlog*, 25.8.2020.

[66] All'indomani di *Schrems II* il Dipartimento del Commercio degli Stati Uniti e la Commissione europea hanno annunciato di aver avviato le discussioni per un nuovo accordo sui trasferimenti dei dati (cfr. *Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*, in https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836, 10.8.2020). Inoltre, il Dipartimento del Commercio degli Stati Uniti ha da subito dichiarato che le imprese autocertificate statunitensi avrebbero continuato ad essere tenute a rispettare i principi sanciti nell'accordo «scudo per la privacy» (cfr. *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows*, in https://www.commerce.gov/, 16.7.2020; ribadito nelle *FAQ* pubblicate il 31.7.2020 e successivamente aggiornate, reperibili in https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update).

[67] O. POLLICINO, *Diabolical Persistence. Thoughts on the Schrems II Decision*, cit.

statunitense a garantire un livello di protezione dei dati sostanzialmente equivalente a quello assicurato dal RGPD, letto alla luce della Carta[68]. È pertanto verosimile che se gli Stati Uniti non apporteranno modifiche all'attuale normativa nazionale, revisionando l'art. 702 FISA, l'E.O. 12333 e/o la direttiva PPD-28, oppure introducendo nuove misure che permettano di allinearsi ai dettami della Corte, non potrà concludersi un nuovo accordo o comunque la Commissione non potrà adottare una nuova decisione di adeguatezza[69].

[68] È soprattutto la mancanza di mezzi di ricorso effettivi che rende inadeguata la protezione dei dati personali negli Stati Uniti. Tale posizione è fortemente criticata, *ex multis*, da Swire e Daskal, che sostengono che i paesi dell'Unione non garantiscono, a loro volta, un controllo giurisdizionale delle operazioni di *intelligence* esterna (J. DASKAL, *What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers*, in www.justsecurity.org, 17.7.2020).

[69] In questo senso, cfr. S. TEWARI, *Schrems II – A brief history, an analysis and the way forward*, in *VerfBlog*, 25.7.2020. Con particolare riferimento al diritto a un ricorso effettivo, gli Stati Uniti dovrebbero assicurare, da un lato, un'indagine attendibile sulle attività di sorveglianza al fine di garantire la protezione dei diritti degli interessati, e, dall'altro, la possibilità di ricorrere a un organo giurisdizionale indipendente che possa porre rimedio alle eventuali violazioni dei diritti (cfr. K. PROPP, P. SWIRE, *Lessons from* Schrems II *About Redress*, in *LawfareBlog*, 13.8.2020. Gli autori suggeriscono che ad effettuare le indagini sia l'*Office of Privacy and Civil Liberties*, e che il controllo giurisdizionale sia svolto in prima istanza dalla *Foreign Intelligence Surveillance Court*, in seconda istanza dalla *Foreign Intelligence Surveillance Court of Review* e, infine, dalla *Supreme Court*).