Ricerche giuridiche e-ISSN 2281-6100
Vol. 6 – Num. 1 – Giugno 2017

L'invalidità del *Safe Harbor* Agreement
Nuovi scenari per la tutela della *privacy* nell'ambito del trasferimento transfrontaliero dei dati

Fabiana Accardo
(Dottoranda di ricerca in Diritto, mercato e persona nell'Università Ca' Foscari Venezia)

Abstract The purpose of this article is that to explain the impact of the landmark decision *Schrems* c. Data Protection Commissioner *[Ireland]* - delivered on 7 October 2015 (Case C-362/2014 EU) by the Court of Justice - on the European scenario. Starting from a brief analysis of the major outcomes originated from the pronunciation of the Court of Justice, it then tries to study the level of criticality that the *Safe Harbor* Agreement and the subsequently adequacy Commission decision 2000/520/EC – that has been invalidated with *Schrems* judgment – have provoked before this pronunciation on the matter of safeguarding personal *privacy* of european citizens when their personal data are transferred outside the European Union, in particular the reference is at the US context. Moreover it focuses on the most important aspects of the new EU-US agreement called *Privacy Shield*: it can be really considered the safest solution for data sharing in the light of the closer implementation of the Regulation (EU) 2016/679, which will take the place of the Directive 95 /46/CE on the EU data protection law?

Keywords *Schrems* judgement. EU protection data law. *Privacy Shield*. Regulation (EU) 2016/679.

1 Brevi cenni sulla sentenza *Schrems c. Data Protection Commissioner [Ireland]*

La nota sentenza *Schrems*[1] ha costituito un importante tassello nella giurisprudenza della Corte di Giustizia dell'Unione europea con riferimento alla tutela transnazionale dei dati personali.

1 Corte Giust. UE, 7 ottobre 2015, in causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*.

DOI 10.30687/Rg/2281-6100/2018/01/007
Submitted: 2017-12-01 | Accepted: 2018-04-16

La vicenda è stata affrontata da gran parte della dottrina giuridica[2] e trae origine dal ricorso presentato da parte un cittadino austriaco, Maximilian Schrems avanti l'Autorità garante dei dati personali irlandese: in particolare si lamentava l'assenza dell'adeguata protezione dei propri dati da parte del *social network Facebook* – a cui era iscritto da diversi anni – nel trasferimento di suddetti dati verso il territorio degli Stati Uniti, dove la società *Facebook Inc.* ha sede e dove gli stessi sono oggetto di trattamento[3]. Il signor Maximilian *Schrems* chiedeva, dunque, l'intervento dell'Autorità al fine di verificare la correttezza di tali trasferimenti transnazionali, e se del caso, vietarli.

La questione sollevata era problematica e di lì a poco avrebbe destato un forte interesse, con rilevanti conseguenze nella gestione dei rapporti tra Unione Europea e Stati Uniti. La richiesta del signor *Schrems* veniva respinta dal Garante della Privacy irlandese, poiché riteneva di non avere la competenza per esaminare la richiesta del ricorrente, considerata la presenza di una decisione della Commissione[4] in cui si stabiliva l'adeguatezza del sistema statunitense dei *Safe Harbour Principles* – c.d. "approdo sicuro" – alla luce dell'art 25, par. 6 della direttiva 95/46/CE[5].

Il signor *Schrems* adiva, successivamente, l'autorità giudiziaria irlan-

2 Tra i più, affrontano il tema approfondendo la questione fattuale e i profili legati alle conseguenze derivanti dalla pronuncia della Corte di Giustizia: A. Giattini, *La tutela dei dati personali davanti alla Corte di giustizia UE: il caso Schrems e l'invalidità del sistema di "approdo sicuro", in Diritti umani e diritto internazionale,* vol. 10, n. 1, 2016 pp. 247- 254; P. Piroddi, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, G. Resta, V. Zeno Zencovich (a cura di), 2016; S. Sica, V. D'Antonio, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in *La protezione transnazionale dei dati personali*, *op. cit.*, pp. 137-167.

3 Come meglio specifica la Corte di Giustizia nella sentenza al punto 27: "Chiunque risieda nel territorio dell'Unione e desideri utilizzare *Facebook* è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con *Facebook Ireland*, una controllata di *Facebook Inc.*, situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di *Facebook* residenti nel territorio dell'Unione vengono trasferiti, in tutto o in parte, su server di *Facebook Inc.* ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di trattamento". Ciò spiega la ragione per cui il ricorrente si è rivolto, in primo luogo, al Garante della Privacy irlandese al fine di tutelare i diritti sui propri dati personali.

4 Decisione 2000/520/CE della Commissione, 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.

5 La direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, disciplinante la tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è stata attualmente abrogata dal nuovo Regolamento UE 2016/679 del Parlamento e del Consiglio, il quale si applicherà a partire dal 25 maggio 2018. Come noto, l'art. 25, par. 1 dell'abrogata direttiva prevede un generale divieto di trasferimento di dati personali verso i paesi terzi, a meno che il paese verso cui il dato deve essere trasferito non garantisca un livello di protezione "adeguato". In questo contesto, la

dese (*High Court*) contro la legittimità della decisione del Garante; nel valutare la questione, la Corte d'Appello riteneva che il Garante della privacy avrebbe dovuto istruire la causa in considerazione delle principi costituzionali della Carta Irlandese[6] e della normativa nazionale relativa alla protezione dei dati[7].

Tuttavia il riferimento al solo diritto nazionale non era sufficiente affinché la Corte adita giudicasse la questione. Ed invero, la materia della tutela dei dati personali era disciplinata dal diritto dell'Unione Europea, in particolare dalla direttiva n. 95/46/CE, alla luce della quale il Garante della *privacy* irlandese aveva respinto la denuncia del ricorrente per «essersi scrupolosamente attenuto alla lettera della direttiva 95/46/CE e della decisione 2000/520/CE»[8], che era vincolante per gli Stati membri.

A fronte di ciò, la *High Court* decideva di sospendere il procedimento per operare un rinvio pregiudiziale, sottoponendo due domande alla Corte di Giustizia: l'una relativa all'interpretazione dell'art. 25, par. 1 e 6, sul criterio di "adeguatezza"[9] della legislazione dello Stato terzo affinché il trasferimento dei dati personali da uno Stato membro dell'Unione risul-

Commissione, attraverso una specifica decisione, può stabilire che lo Stato terzo in questione abbia raggiunto il livello di protezione adeguato.

6 La *High Court* si riferiva, in particolare, alle norme costituzionali quali il rispetto della dignità umana, libertà della persona (preambolo), autonomia personale (articolo 40, paragrafo 3), inviolabilità del domicilio (articolo 40, paragrafo 5) e protezione della vita familiare (articolo 41).

7 Nelle conclusioni dell'Avvocato generale Yves Bot si fa riferimento alla legge sulla protezione dei dati (*Data Protection Act)* del 1988, successivamente modificata dalla legge sulla protezione dei dati del 2003 (*Data Protection Amendment Act*), il cui art. 11, comma 1 disciplina il trasferimento dei dati personali verso Paesi terzi, prevedendo che «il commissario deve risolvere la questione dell'adeguatezza della protezione dei dati nello Stato terzo in conformità ad una constatazione dell'Unione effettuata dalla Commissione [...]. Ne consegue che il commissario non potrebbe discostarsi da una siffatta constatazione. Poiché la Commissione, nella sua decisione 2000/520/CE, ha constatato che gli Stati Uniti garantiscono un livello di protezione adeguato».

8 Conclusioni dell'Avvocato generale Yves Bot, punto 42.

9 Con riguardo al concetto di "adeguatezza", la direttiva 95/46/CE non lo definisce puntualmente, indicando solo in maniera esemplificativa alcune circostanze da valutare nel constatare che il livello di protezione sia adeguato (ci si riferisce, ad esempio, alla natura dei dati, alla finalità del trattamento, o ancora alle norme di diritto vigenti nel paese terzo destinatario del trasferimento). Il c.d. *Article 29 Working Party* (A29/WP ha cercato di dirimere tale incertezza terminologica sostenendo che l'adeguatezza dovesse intendersi, non tanto come sinonimo di "equivalenza", che esige una completezza nella similarità legislativa tra sistemi differenti; quanto piuttosto nel senso di effettiva protezione delle persone fisiche i cui dati sono oggetto di trattamento in un paese terzo. D. Pittella, *Trasferimento verso paesi terzi*, in *La nuova disciplina europea della privacy*, S. Sica, V. D'Antonio, G.M. Riccio (a cura di), Padova, 2016, p. 261 ss. A proposito del concetto di "adeguatezza", discute più nel dettaglio P. Piroddi, *op. cit.*, p. 190 ss.

tasse legittimo, a ciò conseguiva la necessità di interpretare l'art. 28[10] della direttiva e, dunque, se tra le competenze delle Autorità nazionali di controllo vi fosse anche quella di esaminare le domande sul trasferimento di dati personali verso Paesi terzi, pur in presenza di una decisione di adeguatezza della Commissione; l'altra strettamente connessa alla prima domanda pregiudiziale, e consistente nel giudizio relativo all'accertamento della validità della decisione 2000/520/CE.

Anzitutto era, dunque, necessario chiarire se le autorità nazionali di controllo potessero in qualche modo discostarsi dalla suddetta decisione di adeguatezza.

A questo proposito, la Corte premetteva, ai sensi dell'art. 288 TFUE, l'assoluta vincolatività della decisione della Commissione per gli Stati membri, e che – in questi casi – le autorità di controllo nazionali non siano di per sé legittimate a vietare i trasferimenti di dati personali verso i Paesi terzi.

Elaborate tali – e dovute – premesse, la Corte di Lussemburgo affrontava la prima delle due domande sottoposte alla sua attenzione[11], risolvendola alla luce degli artt. 7[12], 8[13] e 47[14] della Carta dei diritti fondamentali dell'Unione europea: il solo fatto della presenza di una decisione di adeguatezza vincolante non può ostare a che il Garante – investito di una doglianza – esamini le denunce presentate dai cittadini, in quanto in capo allo stesso sussiste "potere-dovere"[15] di indagare se effettivamente il soggetto ricorrente faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato[16]. Le autorità di controllo di ciascun Stato membro sono da considerarsi "guardiani"[17] dei diritti individuali e, pertanto, l'effetto vincolante delle decisioni adottate dalla Commissione non può escludere lo svolgimento di indagini su eventuali violazioni dei diritti

10 L'art. 28 della direttiva 95/46/CE disciplina i poteri delle autorità di controllo di ciascun Stato membro.

11 Riferita all'interpretazione degli artt. 25, co. 1, 6, e 28 della direttiva 95/46/CE.

12 L'art. 7 della Carta di Nizza disciplina il rispetto della vita privata e della vita familiare, in cui rientrano anche il domicilio e le comunicazioni.

13 L'art. 8 sancisce, invece, la protezione dei dati di carattere personale, che devono essere trattati secondo un principio di lealtà e finalità determinate o, comunque, in base al consenso dell'interessato o di un fondamento legittimo previsto dalla legge.

14 L'art. 47 prevede il diritto al ricorso effettivo e a un giudice imparziale.

15 Così D. Pittella, *op. cit.*, p. 265.

16 Cfr. Corte Giust. UE, 7 ottobre 2015, in causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*, punto 66.

17 Così M.L. Flóres Rojas, *Legal implication after Schrems case: are we trading fundamental rights?*, in *Information & Communication Technology Law*, vol. 25, n. 3, 2016, p. 299.

fondamentali, conseguenti ad un possibile trasferimento di dati illegittimo verso un Paese terzo[18].

Una risoluzione di tal tipo, orientata sulla scorta giustificativa del principio di piena indipendenza delle Autorità di controllo nazionali, in osservanza dei poteri di cui è investita ai sensi dell'art. 28 della direttiva è volto a consentire un effettivo esercizio delle funzioni loro attribuite. Il tutto letto alla luce del più ampio quadro normativo fornito dal combinato disposto degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione Europea.

La seconda questione – sui *Safe Harbor Principles* – indissolubilmente legata alla prima sarà, invece, analizzata nel proseguo del presente lavoro con l'intento di affrontare alcuni dei profili problematici e le relative conseguenze da essa derivanti nel panorama europeo ed extra-europeo.

2 Le criticità della decisione 2000/520/CE

Con la sentenza *Schrems* è definitivamente crollato il "ponte" transatlantico dei *Safe Harbor Principles*[19], che per lungo tempo aveva operato in favore delle organizzazioni statunitensi e adottato sulla base dell'art. 25, par. 6 della direttiva 95/46/CE[20].

Il sistema delineato voleva regolare i rapporti tra Unione europea – attenta alla tutela e alla protezione dei dati personali dei cittadini appartenenti agli Stati membri[21] – e Stati Uniti, spesso destinatari del trattamento di tali dati da parte delle proprie imprese private e di altre organizzazioni ivi stabilite.

Ed invero, la portata del sistema di tutela dei dati personali in Europa assume tratti molto differenti rispetto a quello statunitense, anzitutto per quel concerne i suoi presupposti. Se negli USA vige un generale principio che permette il trattamento dei dati, a meno che tale operazione non causi un pregiudizio al soggetto interessato o sia limitata da disposizioni

18 In questo senso si esprime l'Avvocato generale Yves Bot nelle sue conclusioni al caso *Schrems*, punto 85.

19 Il *Safe Harbor Agreement* – elaborato dal *U.S. Departement of Commerce* il 21 luglio del 2000 – è stato adottato dalla Commissione con decisione di adeguatezza 2000/520/CE.

20 Così S. Sica, V. D'Antonio, *op. cit.*, p. 139.

21 Per approfondire il profilo delle tutele offerte nella Carta europea dei diritti fondamentali, con particolare riferimento al caso *Schrems* e al percorso argomentativo seguito dalla Corte di Giustizia a tal fine, si rinvia a G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali, in La protezione transnazionale dei dati personali*, *op. cit.*, p. 117 ss., con particolare riferimento ai § 2, 2.1; O. Pollicino – M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *La protezione transnazionale dei dati*, *op. cit.*, p. 73 e ss.

regolamentari; in UE il presupposto prevede, all'opposto, un divieto generale di trattamento dei dati a meno che non sussistano basi legali che lo consentano.

Varia anche la definizione concettuale di "dato personale" che nel panorama europeo è rappresentato da qualsiasi informazione che riguarda una persona fisica identificata o identificabile[22], mentre la regolamentazione statunitense tutela quelle informazioni di soggetti già identificati, lasciando dunque privi di tutela i soggetti interessati, nel caso in cui la persona sia anche identificabile tramite i sempre più intrusivi meccanismi di profilazione[23].

Inoltre, differiscono anche i limiti legati all'autonomia contrattuale sulla protezione dei dati personali, poiché nel panorama statunitense sono presenti dei meccanismi per fissare standard di protezione dei dati, che consentono un ampio grado di manovra – tramite lo strumento contrattuale – per superare gli interessi alla riservatezza dei dati personali; diversamente nell'ambito dell'Unione non è possibile derogare agli obblighi previsti dalla direttiva sulla tutela dei dati, laddove ciò restringa i diritti fondamentali fissati dalla stessa, per cui un'eventuale deroga al trattamento dei dati può avvenire solo sulla base delle sue disposizioni[24].

Infine, nella lista degli elementi di diversità tra il sistema statunitense e quello tratteggiato in ambito europeo, occorre sottolineare la differenza rispetto al controllo sulla tutela dei dati: in Europa è prevista la presenza di Autorità nazionali di controllo indipendenti, a cui sono affidati ampi poteri per implementare la disciplina europea prevista dalla direttiva e applicare le normative sulla protezione dei dati personali; negli Stati Uniti tale funzione è, invece, delegata alla *Federal Trade Commission* (FTC)[25], che condivide alcuni dei poteri utilizzati dalle Autorità nazionali europee, ma a differenza di queste ultime, non ha una giurisdizione estesa nei confronti di tutte le imprese statunitensi. Da ciò consegue una più limitata capacità di *enforcement* dei poteri della FTC, circoscritti sostanzialmente

22 Cfr. art. 2, co. 1, lett. *a)* della direttiva 95/46/CE.

23 Cfr. M. L. Flórez Rojas, *op. cit.*, p. 294.

24 Ad esempio con rifermento al trasferimento transnazionale dei dati è la direttiva 95/46/CE che all'art. 26, par. 1, fissa le deroghe consentite nel caso in cui il trasferimento dei dati personali non garantisca il livello adeguato ai sensi dell'articolo precedente.

25 Si tratta dell'Autorità indipendente fondata dal *Federal Commission Trade Act*, con il principale scopo di promuovere la protezione dei consumatori, eliminare e prevenire le pratiche commerciali scorrette. È competente nella repressione degli abusi che potrebbero influenzare la scelta del consumatore, affettandone la capacità nell'espressione della stessa. Nell'ambito della propria competenza, indaga sulle false dichiarazioni di adesione a *Safe Harbor* sulla non osservanza dei principi da parte di imprese che ne sono membri. In particolare, nello specifico caso di applicazione dei principi nei confronti di vettori aerei, l'organismo competente è il *Department of Transportation*, `http://www.agcm.it/resto-del-mondo-e-icn/normativa-a-tutela-del-consumatore-in-europa-e-usa.html`.

al solo ambito di linee guida sulle corrette pratiche di informazione sulla protezione della *privacy*.

L'obiettivo dell'accordo UE-US era, dunque, adeguare il frammentato scenario normativo statunitense, caratterizzato principalmente da un approccio settoriale proveniente da differenti fonti di tipo federale, statale e autoregolamentare, alle disposizioni presenti nel più unitario e ordinato panorama europeo, la cui regolamentazione – come anticipato – è più articolata e garantista.

Pertanto, si tentava di diminuire l'incertezza sulla sicurezza del trasferimento e trattamento dei dati personali dall'Europa verso gli Stati Uniti e al tempo stesso incoraggiare, sviluppare, promuovere il commercio internazionale tra i due Paesi.

La decisione di adeguatezza della Commissione 2000/520/CE prevedeva una serie di principi generali - già dettagliatamente e ampiamente affrontati in innumerevoli contributi sul tema[26]– e completati attraverso una serie di c.d. *Frequently Asked Questions and Aswers* (FAQ), che si ponevano quale strumento integrativo a fini applicativi e interpretativi dei principi[27].

La struttura così elaborata ha da sempre destato una serie di critiche, dovute a rilevanti limiti oggettivi riscontrati nella prassi applicativa del *Safe Harbor*. Criticità che sono state dettagliatamente esaminate dalla Corte di Giustizia e che, certamente, hanno influito nella dichiarazione di invalidità del sistema siffatto.

Prima di procedere all'analisi delle argomentazioni che hanno giustificato la decisione *Schrems*, è necessario indicare alcuni degli aspetti che sono stati contestati.

Anzitutto, l'applicazione dei *Safe Harbor Principles* era prevista limitatamente per le organizzazioni operanti nei settori di competenza della *Federal Trade Commission* o del *Department of Transportation*. Da ciò ne è derivata l'esclusione per tutte quelle imprese che prevedevano un controllo della loro attività da parte di autorità differenti dalla FTC: ad esempio è il caso delle imprese di telecomunicazioni, cui Autorità di riferimento è la *Federal Communication Commission* (FCC), così come previsto nel *Communication Act*; o ancora istituti bancari, casse di risparmio e unioni di credito, per cui competenti sono il *Federal Reserve Board*, l'*Office of*

26 Con riferimento a questo profilo, si rinvia tra i più a S. Sica e V. D'Antonio, *op. cit.*, pp. 145-155, in cui è analizzano nel dettaglio la struttura dell'accordo, descrivendo i principi caratterizzanti il *Safe Harbour Agreement*, tra cui: *notice principle, choice principle, acces principle, onward transfer principle, security principle, data integrity principle, enforcement principle*.

27 *Ivi*, p. 149 ss. L'a. inizia una digressione sulle FAQ più importanti, sul loro contenuto e sul ruolo di implementazione dei *Safe Harbour Principles*, per applicarli al meglio nel processo di assimilazione e combinazione tra le tutele previste nell'ordinamento statunitense e nel modello comunitario della direttiva 95/46/CE.

Trift Supervisor e dal *Nation Credit Union Administration Board*. Si tratta di casi in cui il flusso di informazioni è spesso ingente, e il cui controllo non essendo spettante alla *Federal Trade Commission* non rientrava nell'ambito di applicazione dei *Principles*.

Descritto il limite oggettivo, i dubbi circa l'effettività del sistema hanno fatto riferimento anche al meccanismo di implementazione su cui si basa la tutela dei dati trasferiti da uno Stato europeo verso gli Stati Uniti, consistente nel c.d. *self-certification scheme*: ciascuna impresa privata statunitense poteva decidere volontariamente se aderirvi e nel caso in cui ciò avvenisse l'operatore si vincolava in primo luogo a informare i soggetti dello scopo per cui le informazioni raccolte venivano usate e che a tal fine fossero rilevanti; secondariamente a consentire l'accesso ai dati, e successivamente assicurare la possibilità per l'interessato di modificare tali dati[28]. Il tutto comprendeva solo quei dati traferiti dopo l'adesione all'approdo sicuro e ciò era sufficiente per creare una presunzione di adeguatezza della tutela dei dati importati dall'Unione europea, considerato che lo stesso *Safe Harbor Agreement* era stato ritenuto – da parte della Commissione – l'accordo che al meglio potesse assicurare la salvaguardia delle informazioni relative ai cittadini europei.

Ulteriori punti critici sono stati individuati nella presenza della c.d. *supremacy clause*, la quale mostra un'altra limitazione posta in essere dal sistema sinora tratteggiato: il diritto statunitense si poneva in ogni caso in una posizione di supremazia rispetto all'accordo. Nell'allegato I, relativo ai principi dell'approdo sicuro, la decisione 2000/520/CE disponeva una deroga alla loro applicazione in alcuni casi particolari: esigenze di sicurezza nazionale, interesse pubblico o inerente all'amministrazione della giustizia; in caso di disposizioni legislative, regolamentari o decisioni giurisdizionali che contrastino con i suddetti principi, o ancora in caso di autorizzazioni esplicite che consentano alle imprese aderenti all'accordo di soddisfare interessi superiori tutelati da tale autorizzazione; infine nel caso in cui sia la stessa direttiva – 95/46/CE – o la legislazione degli Stati

28 A questo proposito, si rinvia a quanto previsto dalla stessa decisione 2000/520/CE all'art. 1 par. 3: «[…] Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera a), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera b)». Quale specificazione del contenuto, ricorre la *FAQ 6*: «Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate.[…] Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro».

membri a rendere possibili delle eccezioni o eventuali deroghe[29].

Ciò comportava, dunque, una deroga al sistema di *Safe Harbor* da parte delle imprese aderenti all'accordo ogniqualvolta sussistessero situazioni giustificate da esigenze "superiori", considerando, inoltre, che le pubbliche autorità non erano tenute al rispetto dei principi suddetti.

A fronte di tali profili problematici, la Commissione aveva già espresso qualche accorgimento con due comunicazioni adottate nel 2013[30], in cui si osservava una preoccupazione sempre maggiore sul livello di tutela dei dati personali dei cittadini dell'Unione Europea trasferiti verso gli Stati Uniti nell'ambito del sistema di "approdo sicuro", per via della sua natura volontaria e dichiarativa. Evidente era la carenza nell'attuazione effettiva della decisione 2000/520/CE, poiché talune imprese statunitensi – seppur certificate – non rispettavano i principi di "approdo sicuro"; si aggiungeva inoltre che tale sistema «era utilizzato come una sorta di "interfaccia" per il trasferimento di dati personali di cittadini europei verso gli Usa, da parte delle imprese private, tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi[31]».

Dunque, l'applicazione del sistema secondo tali modalità comportava un rilevante nocumento nei confronti dei diritti fondamentali dei cittadini europei.

Nella comunicazione *COM (2013) 847 fina*l, sul funzionamento di *Safe Harbor*, la Commissione sottolineava che «i principali beneficiari delle garanzie previste dal diritto americano sono i cittadini statunitensi o le persone che risiedono legalmente negli USA», e che tra le imprese che aderivano ai principi di "approdo sicuro" rientravano anche alcune società fortemente attive nel settore di Internet - *Google, Facebook, Microsoft, Apple, Yahoo* – le quali trasferivano un ingente numero di dati personali di cittadini europei verso gli Stati Uniti, i cui server erano, qui, ubicati. Il tutto vedeva alla base le precedenti rivelazioni sull'utilizzo del programma *PRISM*[32], che rifletteva seri dubbi sulla validità del *Safe Harbor* Agreement,

29 Decisione 2000/520/CE, allegato I. Le autorizzazioni di cui alla lett. *c)* dell'allegato I, sono esplicitate all'allegato IV della decisione, capo B), recante il titolo *"Autorizzazioni legali esplicite"*.

30 Si fa riferimento alle comunicazioni del 27 novembre 2013: *COM (2013) 846 fina*l e *COM (2013) 847 final*. L'una relativa al ripristino di un clima di fiducia negli scambi di dati fra UE e USA; l'altra inerente al funzionamento di "approdo sicuro "dal punto di cittadini dell'UE e delle società ivi stabilite.

31 Cfr. *COM (2013) 846 final*, punto 3.2.

32 L'acronimo *PRISM* indica un programma di raccolta di informazioni su larga scala, in particolare si fa riferimento al c.d. scandalo *"Datagate"*, sulle rivelazioni di Edward Snodwen sull'attività di sorveglianza elettronica di massa da parte della *National Security Agency* (NSA), che aveva consentito alle autorità pubbliche statunitensi di accedere indiscriminatamente e in modo generalizzato alle informazioni derivanti dal traffico elettronico di dati personali non solo di cittadini statunitensi, ma anche di cittadini europei, o ivi residenti.

essendo diventato lo stesso «una delle piattaforme di accesso delle pubbliche autorità di intelligence alla raccolta di dati personali inizialmente trattati nell'Unione europea»[33], con la possibilità, dunque, che società aderenti al sistema di "approdo sicuro" permettessero – a causa di disposizioni legislative in deroga all'applicazione dei Principi - l'accesso e il trattamento di tali dati da parte delle autorità statunitensi, oltre il necessario e proporzionato bisogno per rispondere alle esigenze di sicurezza nazionale.

Nell'affrontare la validità della decisione della Commissione, la Corte di Giustizia torna nuovamente sul concetto di "adeguatezza", previsto dall'art. 25, par. 6 della direttiva 95/46/CE.

L'art. 1, par. 1 della decisione 2000/520/CE – in ossequio al disposto della direttiva – afferma che il sistema di *Safe Harbour* garantisce «un livello adeguato di protezione dei dati personali trasferiti dalla Comunità [*rectius* Unione] a organizzazioni aventi sede negli Stati Uniti». La Corte ricorda che il livello di tutela "adeguato" esige una "sostanziale equivalenza"[34], necessaria era dunque l'effettività della legislazione nazionale del paese terzo rispetto all'obiettivo europeo della tutela.

Il fatto, poi, che tali strumenti risultassero differenti da quelli attuati all'interno dell'Unione non era rilevante ai fini dell'efficacia, nella prassi, di tali mezzi[35].

A questo proposito, vengono esaminati gli articoli 1 e 3 della decisione 2000/520/CE. Con riferimento all'art. 1, la Corte ha ritenuto che il meccanismo di autocertificazione delle imprese private, tramite adesione volontaria ai principi[36], non risulta di per sé contrario all'attuazione del requisito di "adeguatezza" previsto dall'art. 25, par. 6 della direttiva, ma al tempo stesso l'affidabilità di tale sistema può sussistere solo se siano predisposti degli efficaci strumenti di sanzione nel caso di violazione dei principi

P. Piroddi, *op. cit.*, p. 182. Sul punto si veda anche C. Comella, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza Safe Harbor della Corte di giustizia dell'Unione Europea*, in *La protezione transnazionale dei dati*, p. 49 ss., con particolare riferimento alla questione *"Datagate"*; B. Carotti, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa*, in *Giornale di diritto amministrativo*, 3/2016, p. 334 ss.

33 Cit. *COM (2013) 847 fina*l, punto 7.

34 Come già ampiamente discusso dall'*Article 29 Working Party*.

35 Cfr. Corte Giust. UE, 7 ottobre 2015, in causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*, punto 74.

36 Decisione 2000/520/CE, art. 1, par. 3: «Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera a), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera b)».

che assicurano la protezione dei dati personali[37]. Ebbene, la problematica maggiore si pone per quel che concerne l'accesso da parte delle pubbliche autorità al contenuto delle comunicazioni elettroniche, contenenti dati personali inerenti al fondamentale diritto sul rispetto della vita privata[38].

È, dunque, possibile affermare che il sistema di *Safe Harbor*, disegnato in territorio statunitense, assicuri una protezione dei dati effettiva a livello normativo?

In realtà, gli allegati alla decisione di adeguatezza del *Safe Harbor* non contenevano norme statali tese a limitare le ingerenze di autorità pubbliche nei diritti fondamentali dei soggetti i cui dati venivano traferiti dall'Unione europea verso gli Stati Uniti, né tantomeno vi era l'esistenza di una concreta tutela giuridica avverso l'accesso indiscriminato[39] da parte delle stesse; a rendere ancora più chiaro il quadro di tale sistema si aggiunga che – in determinate situazioni[40] - anche le imprese aderenti all'accordo potevano derogare agli impegni assunti.

Dato che i ricorsi all'arbitrato privato o al procedimento di competenza della FTC si limitavano alle sole controversie derivanti da «atti o pratiche sleali e ingannevoli in materia commerciale o collegata al commercio, ed essa non si estende pertanto alla raccolta e all'impiego di informazioni personali a fini non commerciali»[41], ne risultava che il singolo non aveva alcuna concreta opportunità di avvalersi di rimedi giuridici nei confronti delle forze di intelligence statunitense, al fine di tutelare i propri dati dopo il trasferimento, tramite la rettifica o la cancellazione degli stessi.

Quest'impossibilità contrastava con il fondamentale diritto sancito all'art. 47 della Carta di Nizza, inerente alla tutela giurisdizionale effet-

37 Cfr. Corte Giust. UE, 7 ottobre 2015, in causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*, punto 81.

38 Tutelato all'art. 7 della Corta europea dei diritti fondamentali.

39 Il profilo relativo ai sistemi di sorveglianza di massa indiscriminati era già stato affrontato dalla Corte di Giustizia con la sentenza *Digital Rights Ireland Seitlinger e a.* (C-293/12) decisa l'8 aprile 2014, per la quale si rinvia fra i più a G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *La protezione dei dati transnazionali*, *op. cit.*, p. 23 ss.

40 Già previamente ricordati e coincidenti con motivi di sicurezza nazionale, interesse pubblico; disposizioni legislative o regolamentari, decisioni giurisdizionali con obblighi contrastanti con i *Safe Harbour principles*, nel caso di autorizzazioni esplicitamente previste (come nel caso dell'allegato IV, titolo B, della decisione stessa), o ancora nel caso in cui sia la stessa direttiva europea che renda possibili tali eccezioni o deroghe. Quest'ultimo caso si riferisce alle deroghe previste dall'art. 26, par. 1 della direttiva 95/46/CE, con particolare riferimento alle *Model Contract Clauses* (MCC) e *Corporate Binding Rules* (CBR), sul cui tema riflette dettagliatamente G. M. Riccio, *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement*, in *La protezione transnazionale dei dati*, *op. cit.*, p. 215 ss.

41 Cit. conclusioni dell'Avvocato generale Yves Bot, punto 204.

tiva. Alla luce di queste riflessioni, la Corte ha ritenuto che «la decisione 2000/520/CE non ha affermato che gli Stati Uniti d'America "garantiscono" effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali»[42], conseguendone quindi, la sua invalidità.

Strettamente collegata è la successiva analisi dell'art. 3[43], relativo ai poteri di sospensione dei flussi delle Autorità garanti competenti nella protezione dei dati personali degli Stati membri in caso di trasferimenti transfrontalieri.

La sospensione dei flussi di dati verso le imprese statunitensi da parte dei Garanti nazionali – nell'esercizio dei propri poteri previsti dall'art. 28 della direttiva 95/46/CE – era possibile laddove, una volta verificato da parte degli enti governativi la violazione dei principi di "approdo sicuro", vi fossero ragionevoli motivi per ritenere che l'organismo statunitense competente dell'esecuzione non avesse adottato – né adottasse in futuro – le adeguate misure per porre termine a suddetta violazione, e dunque che continuare il trasferimento provocasse in concreto dei seri danni agli interessati. Limitazione di flussi che, in ogni caso, doveva essere contenuta per il periodo strettamente necessario a ripristinare la tutela relativa alla sicurezza dei dati.

Condizioni di questo genere sono state ritenute chiaramente restrittive per l'azione delle autorità nazionali degli Stati membri, poiché di fatto non consentivano il legittimo uso dei poteri loro spettanti, al punto tale da giustificare le argomentazioni circa l'invalidità del disposto dell'art. 3 da parte della Corte di Giustizia, con conseguente estensione a tutta la decisione vista l'inseparabilità delle due norme rispetto al sistema complessivamente considerato.

42 Cit. Corte Giust. UE, 7 ottobre 2015, in causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*, punto 97.

43 Decisione 2000/520/CE, art. 3: «[…] le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui: a) gli enti governativi degli Stati Uniti di cui all'allegato VII della presente decisione, o un organismo indipendente di ricorso ai sensi della lettera a) del «principio di esecuzione» di cui all'allegato I della presente decisione abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ; oppure b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare. La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ci sia stato notificato alle competenti autorità dell'UE.»

2.1 Segue: Il *Privacy Shield*: un nuovo inizio?

La decisione sul caso *Schrems* ha influito sulla definizione delle trattative riguardanti un nuovo accordo tra UE e USA, c.d. *Privacy Shield*[44], il cui scopo è quello di apportare una maggior chiarezza giuridica nel flusso transfrontaliero dei dati personali e adeguare la disciplina alle linee guida già fornite nelle comunicazioni della Commissione nel 2013, avvalorate anche nelle argomentazioni della Corte di Giustizia.

Questo accordo si è posto l'ambizioso obiettivo di uniformare le garanzie nell'ambito della tutela dei dati personali traferiti dall'Unione europea verso gli Stati Uniti, inserendo elementi di innovazione misti a profili di continuità rispetto al *Safe Harbor*, per offrire una maggiore chiarezza e certezza giuridica tra i Paesi.

Alla stregua del precedente accordo, il *Privacy Shield* si basa su un meccanismo di autocertificazione «in base al quale l'organizzazione statunitense s'impegna a rispettare un insieme di principi in materia di *privacy*, ossia i principi del regime dello Scudo UE-USA per la *privacy*, comprensivi dei principi supplementari, emanati dal Dipartimento del Commercio degli USA»[45], prevedendo però nuovi obblighi più stringenti per le imprese private, tali da avere una maggior vincolatività dal punto di vista giuridico[46]. I pilastri fondamentali dell'accordo possono essere esemplificati considerando differenti profili: i rinnovati obblighi per le imprese, le garanzie sull'accesso ai dati personali da parte delle autorità pubbliche statunitensi, la rafforzata tutela giuridica dei diritti individuali dei soggetti interessati e la fase di monitoraggio degli impegni assunti con il sistema di autocertificazione.

Gli obblighi più stringenti imposti alle imprese si basano sui principi già elaborati nel previo accordo, avendo cura di rispettarli con maggior trasparenza, in particolare il Dipartimento del Commercio statunitense si è impegnato a elaborare un elenco delle società private aderenti ai principi del *Privacy Shield* al fine di metterlo a disposizione del pubblico; allo stesso modo le imprese dovranno indicare – tramite collegamento ipertestuale - il sito web del Dipartimento del Commercio in cui è reperibile la lista di tali adesioni, esplicitando anche una *privacy policy* che dia una chiara informativa ai soggetti sulla possibilità di effettuare reclami inerenti all'utilizzo

44 La 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, ha statuito l'adeguatezza della protezione offerta dal regime dello Scudo UE-USA per la *privacy*.

45 Cit. Decisione di esecuzione (UE) 2016/1250, considerando 14.

46 Cfr. P. Pirrodi, *op. cit.* p. 196. Nello stesso senso le considerazioni di S. Sica, V. D'Antonio, *op. cit.*, p. 165 ss.

dei propri dati personali[47] e – se del caso – rispondervi tempestivamente.

Fondamentale è, inoltre, l'innalzamento del livello di responsabilità di tali organizzazioni per ciò che concerne l'ulteriore trasferimento dei dati a terzi soggetti non aderenti al *Privacy Shield* o in altri Paesi terzi, prevedendo un obbligo ferreo nell'applicazione dei principi sulla scelta dell'eventuale trattamento e dell'informativa sullo stesso, delimitando l'ambito di utilizzo dei dati a una finalità determinata che non sia incompatibile con quegli scopi per cui erano state raccolte in origine o con quelle successivamente autorizzate dall'effettivo consenso dell'interessato.

Per ciò che concerne l'accesso ai dati per le pubbliche autorità statunitensi sono previste specifiche garanzie e meccanismi di controllo, con una serie di limitazioni a tali accessi, in modo da impedirne un'ingerenza illecita e prevenire il rischio di abusi. Una direttiva presidenziale dell'ex Presidente Barack Obama (PPD-28) segnalava già delle limitazioni all'attività di sorveglianza di massa, con la possibilità di effettuare una raccolta dei dati solo laddove ciò fosse basato sulla legge o su un'autorizzazione presidenziale e, comunque, nel rispetto della Costituzione. Il considerando 72 della decisione di adeguatezza della Commissione riporta il contenuto di tale direttiva presidenziale, in cui è previsto che «la raccolta in blocco è effettuata solo quando, "in base a considerazioni tecniche o operative", non risulta possibile procedere alla rilevazione mirata con il filtro di discriminanti, ossia di un identificatore associato a un obiettivo specifico [...]»[48]. Successivamente, nel considerando 75, si prevede che le limitazioni poste dalla PPD-28 siano di particolare interesse nell'ambito di applicazione del nuovo Scudo USA-UE, nel caso in cui la raccolta dei dati personali avvenga al di fuori degli Stati Uniti durante il transito degli stessi dal territorio dell'Unione europea.

Strettamente collegato ai primi due pilastri, è il tema dell'effettività della tutela dei diritti individuali – in ossequio con quanto affermato dall'orientamento della Corte di Giustizia con la sentenza *Schrems* – dei soggetti: si prospettano diversi meccanismi di ricorso avverso le violazioni sulla protezione dei dati, tra cui reclami nei confronti dell'impresa, la quale deve rispondere entro 45 giorni dalla richiesta dell'interessato; accesso gratuito alle ADR; la possibilità di utilizzare il c.d. *Privacy Shield Panel*, consistente in un collegio arbitrale che attraverso una decisione esecutiva si pone l'obiettivo di fermare la situazione pregiudizievole per il soggetto interessato[49]; è segnalata, inoltre, la possibilità di rivolgersi all'Autorità

47 A. Mantelero, *I flussi di dati transfrontalieri e le scelte delle imprese tra* Safe Horbour *e* Privacy Shield, in *La protezione transnazionale dei dati*, *op. cit.*, p. 265.

48 Cit. Decisione di esecuzione (UE) 2016/1250, considerando 72.

49 Previsto dall'allegato 2 della decisione di esecuzione (UE) 2016/1250, recante il titolo "Modello arbitrale".

nazionale garante della protezione dei dati dello Stato membro dell'interessato, che con il coordinamento e la cooperazione del *Department of Commerce e Federal Trade Commission*, effettuerà degli accertamenti su eventuali reclami ancora pendenti effettuati da cittadini dell'Unione.

In ossequio degli impegni assunti con il *Privacy Shield*, il governo statunitense ha creato un particolare strumento di ricorso amministrativo per verificare la correttezza nelle attività dei servizi di *intelligence* nella raccolta – ed eventuale trattamento – dei dati, e che è rappresentato dalla figura del c.d. *Ombudperson*[50], un soggetto indipendente che si occupa di ricevere reclami da parte dei singoli e al quale spettano poteri di indagine e di vigilanza, in modo tale da porre rimedio alle situazione di irregolarità in cui siano incorse le pubbliche autorità[51].

Quarto pilastro è, poi, rappresentato dai meccanismi di monitoraggio dell'accordo, attraverso una revisione annuale congiunta da parte della Commissione europea e dal *Department of Commerce* coinvolgendo di esperti e servizi di sicurezza statunitensi e delle Autorità europee per la protezione dei dati. Sui risultati di tale revisione, la Commissione europea ha il compito di stilare una relazione pubblica al Parlamento e al Consiglio sull'andamento dell'esecuzione dell'accordo. Ciò si pone chiaramente in ossequio alle necessità espresse dalla sentenza *Schrems*[52].

Il *Privacy Shield* si configura, da una parte come un sistema nuovo che la Commissione ha ritenuto in grado di tutelare il trasferimento dei dati verso gli Stati Uniti, assicurando che lo "scudo" predisposto dall'*U.S. Department of Commerce* prevedesse un livello adeguato; dall'altra ha provocato dubbi relativi alla concreta effettività dei nuovi rimedi posti allo scopo[53], con particolare riferimento al ruolo dell'*Ombudperson*, il quale

50 Tale figura descritta nella decisione di esecuzione (UE) 2016/1250, in particolare dal considerando 116 al considerando 122, in cui sono dettagliatamente indicate le competenze e i meccanismi di funzionamento dell'attività del mediatore.

51 Cfr. S. Crespi, *La nouvelle décision d'adéquation (Privacy Shield) pour les transferts des données personnelles de l'Union européenne vers les États-Unis*, in *Journal de droit européen*, 2016, p. 261. In riferimento a questi aspetti si veda anche 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 *Rivista di diritto internazionale*, 3/2016, p. 721, in cui l'*Ombudperson* è descritto come «figura *sui generis*, alto funzionario chiamato ad assicurarsi che le denunce dei singoli siano informati se le leggi degli Stati Uniti applicabili siano state rispettate o, qualora così non fosse, se le violazioni riscontrate siano cessate».

52 Il riferimento va al paragrafo 76 della sentenza, in cui la Corte aveva ritenuto che spettasse alla Commissione valutare con cadenze periodiche la constatazione dell'adeguatezza del livello di protezione del Paese terzo, considerato il fatto che le garanzie fornite dal Paese terzo sono sempre suscettibili evolversi nel tempo.

53 In questa direzione, fra tutti, si pongono A. Mantelero, *op. cit.*, p. 266; P. Piroddi, *op. cit.*, p. 198; M. L. Flóres Rojas, *op. cit.*, p. 307.

pur essendo indipendente e terzo, rimane comunque figura incardinata all'interno del Dipartimento di Stato[54]. Da ciò conseguono, pertanto, legittime preoccupazioni sull'effettività del rimedio e del suo impatto sulla protezione dei dati personali dei soggetti.

3 Il nuovo Regolamento europeo 679/2016 sulla protezione dei dati personali nell'ottica del trasferimento transnazionale dei dati

Il *Privacy Shield* deve, però, essere inserito in un panorama giuridico più ampio, vista la prossima applicazione del Regolamento europeo 2016/679[55] che introduce una disciplina il cui obiettivo primario consiste nell'uniformare la materia relativa alla tutela dei dati personali e alla loro libera circolazione per assicurare un livello di protezione equivalente in tutti gli Stati membri.

Il nuovo Regolamento si occupa di regolare il trasferimento dei dati verso Paesi terzi o verso organizzazioni internazionali[56], riproponendo gli orientamenti giurisprudenziali affermatisi nelle argomentazioni elaborate dalla Corte di Giustizia al fine di migliorare lo scenario europeo relativo alla tutela dei diritti fondamentali. In particolare, centrale è l'ambito di applicazione territoriale della regolamentazione europea. L'art. 3 reg. cit.[57] segnala, infatti, una novità rilevante in materia di protezione dei dati, poiché al comma 2 dello stesso è prevista la sua l'applicazione anche nel caso in cui il soggetto titolare o responsabile del trattamento dei dati non sia stabilito nell'Unione, e ciò in particolare avviene in due specifiche situazioni: da una parte nel caso di offerta di beni o prestazione di servizi a soggetti che siano residenti in uno Stato membro; dall'altra nel caso di un'attività di monitoraggio del comportamento dell'interessato, nella misura in cui tale comportamento abbia comunque luogo nell'Unione. In questa prima disposizione è possibile notare un netto scostamento rispetto alla precedente disciplina europea relativa alla *privacy*, in quanto il classico principio dello stabilimento – sui cui era basata la direttiva 95/46/CE, art.

54 In quanto nominato dallo stesso Dipartimento, come indicato dal considerando 116 della decisione di esecuzione della Commissione.

55 Entrato in vigore il 24 maggio 2016 e direttamente applicabile negli Stati membri dal 25 maggio 2018.

56 Regolamento (UE) 2016/679, capo V, artt. 44-50.

57 L'art. 3, co. 1 del Regolamento così dispone: «Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.»

4 – viene reso più flessibile per accogliere un "approccio orientato verso i destinatari del servizio"[58], estendendo dunque il suo ambito di applicazione, con una maggiore attenzione nei confronti della tutela dei soggetti interessati dal trattamento dei dati.

Se tale disposizione riguarda l'aspetto più generale dell'operatività del nuovo Regolamento sulla disciplina della *privacy*, è bene tratteggiare alcuni punti focali di specifiche disposizioni dedicate ai trasferimenti transnazionali, al fine di individuare le novità che si pongono come base giuridica del *Privacy Shield* in continuità con l'esigenza di proporre un "modello forte" di tutela della *privacy*.

L'art. 45 reg. cit. basa la possibilità di effettuare i trasferimenti verso Paesi terzi riportando nuovamente – come già prevedeva la direttiva 95/46/CE – il livello di "adeguatezza" nella tutela dei soggetti, da leggersi però alla luce delle conclusioni raggiunte nella sentenza *Schrems*. Ed invero, pur mantenendo la necessità che la Commissione elabori una decisione di adeguatezza del livello di protezione presente nel Paese terzo in cui i dati sono trasferiti, ciò che muta è la sostanziale manifestazione di questo parametro, perché i giudici di Lussemburgo chiariscono che l'"adeguatezza" si relaziona con una garanzia di "effettiva tutela" delle persone fisiche i cui dati vengono trattati e che pertanto debba essere "sostanzialmente equivalente" alla disciplina europea. Il concetto di adeguatezza è, dunque, rivisto alla luce della pronuncia chiarendo in modo puntuali e più rigoroso gli elementi da valutare per porre in essere la decisione da parte della Commissione, tra di essi sono indicati: la tutela di diritti e libertà fondamentali, rimedi giurisdizionali previsti per la risoluzione di violazioni dei diritti stessi, la pertinente legislazione settoriale e generale, l'esistenza ed effettivo funzionamento di un'autorità indipendente a protezione dei dati personali nel Paese terzo con efficaci poteri sull'organizzazione internazionale destinataria dei dati; sono anche valutati gli impegni internazionali assunti dal Paese terzo dalle organizzazione che raccolgono i dati personali e strumenti giuridici vincolanti per la loro salvaguardia[59]. Il tutto coronato da disposizioni tese a riaffermare e rafforzare la condizione di "piena indipendenza" delle Autorità nazionali di protezione dei dati, da una parte si confermano i poteri di esame delle doglianze dei cittadini europei – pur in presenza di una decisione della Commissione ritenuta valida – che in *Schrems* erano stati fermamente sostenuti dalla Corte, sulla base dell'interpretazione dell'art. 28 della direttiva 95/46/CE; dall'altra questo rafforzamento comporta una concreta possibilità di creare esiti

58 M. G. Stanzione, *Genesi ed ambito di applicazione*, in M.G. Stanzione, *Genesi ed ambito di applicazione*, in *La nuova disciplina della privacy*, *op. cit.*, p. 30 ss.

59 Cfr. F. Jault-Seseke, C. Zolynski, *Le règlement 2016/679/UE relatif aux données personnelles*, in *Recueil Dalloz*, n. 32/2016, p. 1878.

contraddittori nelle decisioni delle Autorità di controllo, visto il permanere dell'assoggettamento di tali organi alle decisioni vincolanti della Commissione. Ciò provoca, pertanto, una situazione di incertezza nell'applicazione del Regolamento che dovrebbe essere bilanciata dalla cooperazione non solo tra le Autorità nazionali, ma anche tra le stesse e la Commissione[60], al fine di evitare che il parametro della "piena indipendenza" comporti un'eccessiva discrezionalità delle Autorità nazionali e la contraddittorietà della loro azione rispetto all'indirizzo dato dalla Commissione.

Nella panoramica dei principali profili della nuova disciplina sulla *privacy*, il *Privacy Shield* deve essere armonizzato con il Regolamento UE 2016/679, in considerazione del fatto che la sua elaborazione sia avvenuta sulla base giuridica dell'abrogata direttiva; a tal proposito è la disciplina regolamentare che con una norma di diritto transitorio[61] ha affermato che le decisioni di adeguatezza adottate dalla Commissione devono ritenersi valide e in vigore fino al momento in cui non siano ulteriormente modificate, sostituite o abrogate nuovamente dalla Commissione stessa nel caso in cui il funzionamento dello "Scudo" non garantisca più il livello adeguato di protezione dei dati trasferiti dall'Unione europea verso le organizzazioni presenti sul territorio statunitense; e per questa ragione risulta fondamentale l'attività di monitoraggio e revisione annuale dell'accordo recentemente avvenuto[62].

4 Conclusioni

Le riflessioni sinora svolte hanno tracciato il quadro d'insieme dell'attuale regolazione in riferimento allo specifico tema dei trasferimenti transnazionali verso Paesi terzi a partire dall'emblematico caso *Schrems* per arrivare all'implementazione dell'accordo *EU-U.S. Privacy Shield* e al suo inserimento all'interno della nuova disciplina inerente al Regolamento UE 2016/679.

L'impatto della pronuncia analizzata ha avuto effetti rilevanti, in particolare perché ha contribuito a fare chiarezza sul tanto dibattuto *Safe Harbor Agreement* sancendone, infine, l'invalidità alla luce delle lacune presentate

60 Così P. Piroddi, *op. cit.*, p. 204.

61 Il riferimento è all'art. 45, co. 9: «Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo.»

62 Con riferimento a quest'aspetto, si specifica che la revisione da parte della Commissione si è tenuta a Washington DC nel periodo di settembre al fine di verificarne il corretto funzionamento. Con riferimento ai primi risultati di tale controllo si rinvia a: `http://europa.eu/rapid/press-release_STATEMENT-17-3342_en.htm`.

dall'accordo che non consentiva un'idonea tutela nell'ottica prevista dal quadro europeo della direttiva 95/46/CE.

Nella prospettiva europea i dati personali hanno certamente un ruolo fondamentale nell'espansione del commercio internazionale verso altri paesi – anche se non appartenenti all'Unione – ma in questo contesto centrale è la loro tutela, intesa come diritto fondamentale individuale e in alcun modo negoziabile; totalmente diversa la concezione nello scenario d'oltreoceano, in cui la rilevanza data agli scambi internazionali rischia di prendere il sopravvento, relegando i dati personali a mera "merce" per favorire il traffico transnazionale.

Sulla base di questi presupposti, la Corte ha tentato di ristabilire il livello di protezione dei dati personali nei trasferimenti che coinvolgono Paesi terzi, fornendo delle linee guida su cui basare il successivo accordo regolatore della materia.

Il percorso per l'elaborazione del *Privacy Shield*, i cui negoziati erano già in corso all'epoca della decisione, sembra aver recepito – secondo quanto confermato dalla Commissione stessa con la sua decisione di adeguatezza del 12 luglio 2016[63] – i principi sviluppati in *Schrems*, rappresentando un ulteriore passo verso lo schema di rigida tutela dei diritti fondamentali e sicurezza nei trasferimenti che si pone di realizzare l'Unione europea nei confronti dei suoi cittadini.

Medesimo obiettivo si è imposto il nuovo Regolamento UE 2016/679, che propone un modello forte di salvaguardia del diritto fondamentale sancito dall'art. 8 della Carta di Nizza con l'intento di incrementare l'effettività della tutela attraverso un'opera non più consistente nella mera armonizzazione delle legislazioni nazionali, ma nell'uniformazione della disciplina e a tal fine lo strumento prescelto è quello del regolamento, direttamente applicabile negli Stati membri dal maggio 2018.

In questo contesto è inserito il *Privacy Shield*, il quale deve armonizzarsi con la più generale disciplina del nuovo Regolamento, ed invero in riferimento a questo aspetto è arrivato il *placet* della Commissione che lo ha ritenuto meritevole di rispettare il parametro della "sostanziale equivalenza" rispetto al modello europeo.

Anche questo accordo non è stato esente da critiche, anzi ne è stata contestata la scarsa coercitività, tanto da ricordare in alcuni suoi tratti il suo predecessore, proprio per questa ragione ritenuto dallo stesso ricorrente Maximilian *Schrems* un "*soft update of Safe Harbour*"[64]. I dubbi sono ancor maggiori se si pensa, in particolare, alla possibilità che il *Privacy Shield* possa essere minato a causa dei recenti sviluppi sulla tutela della

63 Decisione di esecuzione (UE) 2016/1250 della Commissione.

64 M. *Schrems*, *The Privacy Shield is a Soft Update of the Safe Habor*, in *EDPL*, n. 2/2016, p. 148 ss.

privacy nel panorama statunitense. Con l'elezione del Presidente Donald Trump, gli impegni statuiti nel nuovo accordo hanno rischiato di vacillare, a causa dell'emanazione dell'ordine esecutivo presidenziale n. 13768[65], in materia della pubblica sicurezza, con cui si prevede che le pubbliche autorità – sulla base del *Privacy Act* – devono assicurare le *privacy policies* nei confronti dei cittadini statunitensi, escludendo invece i "non cittadini"[66].

Alla luce di questi ultimi sviluppi, la Commissione europea ha fatto chiarezza sulla sorte dell'intesa raggiunta con le controparti statunitensi, che hanno, però, assicurato l'impegno nel rispetto del *Privacy Shield*[67].

Ancor più recentemente – nel settembre scorso – si è svolta la prima revisione sul funzionamento dello Scudo Ue-Usa: qui, la Commissione ha confermato la sussistenza delle garanzie fornite dall'adeguato livello di tutela dell'ordinamento statunitense, in quanto sono stati predisposti gli strumenti necessari per porre in essere una solida cooperazione tra le autorità degli Stati.

Nonostante le incertezze e le criticità del nuovo Scudo, il *Privacy Shield* – tra luci e ombre – è riuscito ad inserirsi legittimamente tra le maglie del quadro comune segnato dall'attuale regolamentazione europea, costituendo un fondamentale tassello nella materia inerente la tutela dei dati personali nei trasferimenti transfrontalieri al fine di rispondere alle sempre maggiori esigenze di sicurezza alla luce della continua crescita economica e degli sviluppi tecnologici negli scambi internazionali.

65 Si tratta dell'ordine esecutivo 13768 del 25 gennaio 2017, *Enhancing Public Safety in the Interior of the United States*, https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02102.pdf.

66 Sul punto si rinvia a A. Butler, *Whither Privacy Shield under Pressure?*, in *EDPL*, n. 1/2017, p. 111 e ss.

67 Come risulta anche dalla relazione sulla revisione e monitoraggio del *Privacy Shield*, per il Report completo si rinvia a http://europa.eu/rapid/press-release_IP-17-3966_it.htm.