Salvatore Sica - Virgilio D'Antonio

Verso il Privacy Shield*: il tramonto dei* Safe Harbour Privacy Principles

Sommario: Premessa. – 1. Il trasferimento di dati tra Europa e Stati Uniti: dalla raccomandazione OECD alla direttiva 95/46/CE. – 2. I *Safe Harbour Privacy Principles*. – 2.1. I principi codificati. – 2.2. Le FAQ. – 2.3. Ambito di applicazione e «self certification scheme». – 2.4. La «supremacy clause» in favore del diritto statunitense. – 3. I poteri della *Federal Trade Commission*, quelli delle *Data Protection Authorities* europee e la responsabilità aquiliana. – Conclusioni: dai *Safe Harbour Principles* verso il *Privacy Shield*, passando attraverso *Schrems*.

Premessa

Con una evidente accelerazione dei negoziati indotta dalla sentenza Schrems, nei primissimi giorni di febbraio 2016, Stati Uniti ed Unione europea hanno raggiunto un nuovo accordo volto a regolare i flussi transfrontalieri di dati tra i due ordinamenti: si tratta del cd. «EU-US Privacy Shield». L'intesa nasce, dunque, sulle ceneri del precedente quadro di regole concordate, indicate generalmente come «Safe Harbour Privacy Principles», in vigore da oltre un decennio e, nell'ottobre 2015, ritenute dalla Corte di Giustizia EU non sufficientemente garantiste per la tutela della riservatezza dei cittadini europei.

I *principles* costituiscono indubbiamente la base di partenza anche dell'attuale *Privacy Shield*: essi trovavano il proprio fondamento giuridico immediato nella direttiva 95/46/CE, che, all'art. 25, comma 1, nell'affrontare la disciplina dei trasferimenti di dati personali oltre i confini dell'Unione Europea, impone, quale standard di tutela per gli interessati, che il paese importatore garantisca ai flussi di informazioni un «livello di protezione adeguato»[1].

[1*] Il presente contributo, pur se unitariamente concepito dai due autori, deve così essere attribuito nelle sue singole parti: S. Sica: Premessa e § 1 – V. D'Antonio §§ 2/3 e Conclusioni. Il diritto comunitario in materia di privacy si caratterizza per la progressiva elaborazione, dottrinale prima ancora che giurisprudenziale e legislativa, di un quadro di

Il trasferimento di dati personali dall'area giuridica europea verso paesi terzi è, da sempre, circondato da particolari garanzie, in ragione del fatto che l'esportazione extraeuropea dei dati personali finisce per comportare, nella maggior parte delle occasioni, la transizione delle informazioni da un'area giuridica ad elevato grado di protezione per il diritto alla riservatezza verso ordinamenti ove il *right of privacy* non è circondato dalle medesime garanzie[2].

La scelta di *policy* dell'Unione, sotto questo profilo, è stata quella di porsi quale modello forte di tutela della riservatezza, imponendo a qualunque esportatore di dati personali di origine comunitaria di confrontarsi con lo schema normativo europeo, garantendo alle informazioni in transito un livello di tutela particolarmente elevato, modellato appunto sul paradigma della direttiva 95/46/CE[3].

Tanto è avvenuto anche nei rapporti tra Unione Europea e Stati Uniti, nella misura in cui l'ordinamento statunitense, pur presentando una lunga e consolidata tradizione di tutela del *right to privacy*, è caratterizzato dall'assenza di una regolamentazione unitaria e generale in materia, con una congerie di interventi settoriali (di matrice federale e statale, nonché autoregolamentare). Tale impostazione complessiva dello scenario norma-

principi forti. Hanno contribuito, tra gli altri, nella dottrina italiana a delineare questo nucleo centrale di principi D. Messinetti, voce «*Personalità (diritti della)*», in *Enc. dir.*, Milano 1983, XXXIII, 355 ss.; P. Rescigno, voce «*Personalità (diritti della)*», in *Enc. giur. Treccani*, Roma, 1990, XXIII, 2 ss.; V. Zeno-Zencovich, voce «*Personalità (diritti della)*», in *Digesto civ.*, Torino, 1995, XIII, 430 ss.; S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583 ss., nonché G. Alpa, *Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto alla identità personale*, in *Giur. merito*, 1989, 464 ss.

[2] Vedi P.M. Schwartz, *The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures, in 126 Harv. L. Rev.* 1966 (2012-2013), il quale, rispetto alla genesi dei Safe Harbour Principles, evidenzia che «*at the start of July 2000, the Commission released the final text of the «Safe Harbor Arrangement» and a series of supporting documents. That same month, the EU Parliament rejected the agreement in a nonbinding resolution before the Commission approved it on July 25, 2000*».

[3] In questi termini, A. Mantelero, Data protection ed attività di impresa. Verso dove guardano gli USA?, in Dir. Inf. 2011, 457 ss., il quale (a pag. 457) evidenzia come il modello comunitario «*grazie ad un'acuta scelta di strategia normativa,[sia]stato esportato al di fuori dei confini dell'Unione, adottato o usato come esempio per legislazioni di diverse nazioni, ed è divenuto in ogni caso parametro necessario di confronto*». Per una ricostruzione dell'evoluzione del concetto di privacy negli Stati Uniti, si vedano A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974; S. Rodotà, Tecnologie e diritti, Bologna, 1995, 19, e, più in generale, R.A. Posner, *Privacy, Secrecy, and Reputation,* in *28 Buffalo Law Rev.* 1 (1979), con approfonditi studi di matrice sociologica e comparatistica.

tivo, accompagnata dalla predilezione, soprattutto nei rapporti di consumo, per la valorizzazione dell'autonomia privata e della negoziabilità delle garanzie connesse alla tutela della riservatezza, contribuisce a determinare la non equipararabilità della protezione offerta dall'ordinamento USA ai rigorosi standard comunitari.

La necessità di definire un quadro organico di principi, in analogia con il modello europeo, pur nel contesto dell'approccio settoriale statunitense, portò all'elaborazione di una serie di regole generali che, ove rispettate dal singolo esportatore di dati personali dall'Europa verso gli Stati Uniti, avrebbe consentito allo stesso di superare la soglia di adeguatezza di tutela imposta dalla direttiva 95/46/CE[4].

Tali principi, definiti appunto «Safe Harbour Privacy Principles», venero poi cristallizzati con la decisione 2000/520, adottata dalla Commissione sulla base dell'art. 25, par. 6, direttiva cit., creando così una presunzione di adeguatezza di tutela in favore di quegli operatori statunitensi che si fossero impegnati, tramite specifica ed esplicita accettazione, al rispetto degli stessi[5].

Con l'adozione dello strumento dei *principles* (implementato tramite diversi documenti ulteriori tra i quali le *Frequently Asked Questions* - FAQ applicative, pubblicate dalla *Federal Trade Commission*) venne creato, pertanto, un vero e proprio 'ponte' preferenziale in favore delle organizzazioni americane, così da consentire e favorire il perdurare dello scambio di dati (anche nel contesto del medesimo gruppo industriale e, soprattutto, attraverso il *web*).

Dopo numerosi scricchiolii, tuttavia, questo 'ponte' è infine crollato il 6 ottobre 2015, quando la Corte di Giustizia, ponendo un tassello fondamentale in un dibattito iniziato già negli anni '80 dello scorso secolo, ha sancito, con la cd. «sentenza *Schrems*», resa nel caso C-362/14, l'invalidità della decisione 2000/520/CE della Commissione europea, facendo così cadere la presunzione di adeguatezza di tutela insita nel rispetto dei *Safe Harbour Principles* e tracciando una linea di cesura nei rapporti tra Stati Uniti ed Unione Europea nel quadro della promozione di strumenti di *soft-law* atti a regolare il trasferimento transfrontaliero dei dati[6].

[4] Tra gli altri, A. Bradford, *The Brussels Effect, in 107 Nw. U. L. Rev. I* (2012), nonché D. Scheer, *For Your Eyes Only – Europe's New High-Tech Role: Playing Privacy Cop to the World,* Wall St. J., Oct. 10, 2003

[5] Sul punto, sia consentito rinviare a V. D'Antonio, *Il trasferimento dei dati all'estero*, *comm.* sub *artt. 42 – 45*, in P. Stanzione – S. Sica (a cura di), *La nuova disciplina della privacy*, Milano, 2004, 155 ss.

[6] Sulle diversità di approccio alla materia dell'ordinamento comunitario e di quello statu-

1. Il trasferimento di dati tra Europa e Stati Uniti: dalla raccomandazione OECD alla direttiva 95/46/CE.

Il primo importante accordo internazionale sul tema della circolazione transfrontaliera di dati personali venne definito nel 1980 dall'Organizzazione per la cooperazione e lo sviluppo economico (OECD), con la raccomandazione del Consiglio che dettava le linee guida in materia di «*Protection of Privacy and Transborder Flows of Personal Data*»[7].

L'atto, di natura non vincolante, è stato emendato soltanto nel 2013[8] e traccia alcuni principi-chiave per il governo della *digital privacy* i quali, seppur sintetizzati in una fase di sviluppo ancora embrionale della cd. società dell'informazione, hanno sensibilmente influenzato i successivi sviluppi normativi registrati in materia.

La raccomandazione sancisce, in primo luogo, otto principi generali applicabili alle legislazioni nazionali, attinenti: *a*) la limitazione della raccolta di dati personali (liceità, idoneità, consenso dell'interessato); *b*) la qualità dei dati (pertinenza rispetto agli scopi, accuratezza, completezza ed aggiornamento); *c*) l'indicazione dello scopo della raccolta (tipologia, adeguatezza temporale); *d*) la limitazione dell'utilizzo (scopo per cui sono stati raccolti, consenso dell'interessato o ordine dell'autorità giudiziaria); *e*) le garanzie sulla sicurezza (misure ragionevoli contro ogni rischio di perdita, accesso non autorizzato, distruzione, uso, modificazione o divulgazione; *f*) la trasparenza; *g*) i diritti dell'interessato (comunicazione, accesso, motivi del diniego, rettifica); *h*) la responsabilità del *data-controller*[9].

Quanto al trasferimento transnazionale dei dati, l'OCSE invitava gli Stati membri ad adottare tutte le misure appropriate e ragionevoli per garantire un flusso ininterrotto e sicuro di dati, in conformità ai principi sopra menzionati ed alle legislazioni nazionali. Emerge, pertanto, una generale tendenza ad incentivare i traffici transfrontalieri di informazioni e, per converso, la precisa scelta di *policy* volta a non ostacolarne lo sviluppo con normative settoriali eccessivamente protettive[10].

---

nitense, si vedano C.J. Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, 1992, nonché del medesimo Autore, *Regulating Privacy*, New York, 1992.

[7] OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 settembre 1980 - C(80)58/FINAL.

[8] OECD, 11 luglio 2013 - C(2013)79. Vedi ancora V. D'Antonio, *Il trasferimento dei dati all'estero*, cit., 160.

[9] Vedi B. Markesinis, Protecting Privacy, Oxford, 1999.

[10] Si veda ad es. *Guidelines Governing the Protection of Privacy and Transborder Flows of*

Soltanto qualche mese dopo l'adozione della raccomandazione, il Consiglio d'Europa ratificò la Convenzione sulla protezione degli individui con riguardo al trattamento automatico di dati personali (c.d. Convenzione di Strasburgo)[11].

La Convenzione ricalca i principi generali tracciati in sede OCSE (qualità del trattamento, tipologia dei dati, sicurezza, diritti dell'interessato, rimedi e sanzioni[12]), affermando poi, all'art. 12, la generale liceità dei trasferimenti di dati da un paese membro all'altro effettuati in ossequio alle precedenti prescrizioni, fatta eccezione per quei casi in cui le legislazioni nazionali non prevedano una protezione rafforzata per determinate categorie di dati o, ancora, il trasferimento sia diretto ad uno Stato che non abbia sottoscritto la Convenzione attraverso l'intermediazione fittizia di un paese aderente[13].

Come è noto, i provvedimenti appena menzionati hanno rappresentato l'*humus* all'interno del quale è maturato il sistema di principi che confluirà poi nella direttiva 95/46/CE: quest'ultima, infatti, prende le mosse proprio da tali primi sforzi regolamentativi e, con riguardo ai *transborder data flows,* detta il principio generale per cui ogni trasferimento è consentito soltanto qualora il paese terzo garantisca un «adeguato livello di protezione» (*ex* art. 25 e considerando 57 dir. cit.). In questo senso, l'elevato grado di tutela declamato al considerando 10 si estende, seppur temperato dal parametro dell'adeguatezza, anche al di fuori del territorio

Personal Data, cit., n. 18: «*Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection*».

[11] Council of Europe, *Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data*, 28 gennaio 1981, European Treaty Series - No. 108.

[12] *Ibidem*, artt. 4-11.

[13] *Ibidem*, art. 12: «*The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2: a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection; b) when the transfer is made from its territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph*».

dell'Unione, come d'altronde è stato ribadito dai giudici della Grande sezione nella sentenza in commento[14].

In effetti, la disposizione comunitaria dedicata ai flussi transfrontalieri di dati, sulla base del parametro dell'adeguatezza del livello di protezione garantito dal Paese terzo, identifica diversi percorsi che possono condurre alla verifica della sussistenza di siffatto livello di tutela[15]. In tal senso, se un ordinamento extraeuropeo presenta un grado di protezione adeguato «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona»[16], la Commissione può adottare, sulla base dell'art. 25, par. 6, della direttiva 95/46, una decisione che, in buona sostanza, 'certifichi' l'adeguatezza della tutela garantita ai dati personali dal Paese terzo[17].

Al contrario, per quegli ordinamenti che non presentino un livello di protezione adeguato ai sensi del comma 2 dell'art. 25 della direttiva 95/46, la Commissione avvia negoziati per porre rimedio alla situazione e, *medio tempore*, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati verso il paese terzo in questione.

All'esito dei negoziati previsti dalla normativa comunitaria e degli impegni eventualmente assunti in tale sede (come della legislazione nazionale o degli impegni internazionali del Paese terzo), la Commissione

[14] CGE Grande sez., 6 ottobre 2015, causa C-362/14, par. 66: *«In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato»*.

[15] Secondo quanto stabilito dall'art. 25, par. 2, direttiva 95/46, l'adeguatezza del livello di protezione garantito da un paese terzo è valutata – secondo un elenco non esaustivo (cfr. par. 70 della decisione) - con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

[16] Così par. 71 della decisione.

[17] Peraltro, come ribadito al par. 50 della decisione, *«la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata […] vuoi dagli Stati membri vuoi dalla Commissione»*. In tema, vedi anche Riccardo e Rosario Imperiali, *Il trasferimento all'estero dei dati personali. Modalità e soluzioni contrattuali per il flusso dei dati nel mondo economico*, Roma, 2003, ed ivi ampi riferimenti di bibliografia.

può valutare positivamente il livello di tutela garantito ai dati personali ed adottare una decisione favorevole alla circolazione extraeuropea degli stessi.

In questo caso, come ribadito anche nella sentenza *Schrems*, gli Stati membri sono tenuti ad adottare tutte le misure necessarie per conformarsi alla decisione della Commissione, favorendo i trasferimenti di dati personali verso il Paese terzo da essa interessato.

Ora, nella disciplina dei flussi extraeuropei, una delle 'vie' principali è quella che conduce i dati personali verso gli Stati Uniti, ordinamento che, ove confrontato con quello comunitario sotto il profilo della tutela della riservatezza, presenta una serie di 'lacune' che conducono verso un giudizio di inadeguatezza da parte della Commissione europea. I motivi, altre alla già sottolineata differenza di approccio alla materia, sono molteplici: tra l'altro, la privacy non è computata nel novero dei diritti fondamentali come avviene nella Convenzione europea per la salvaguardia dei diritti dell'uomo all'art. 8. Il sistema normativo settoriale, proprio del modello USA, presenta, poi, sotto il profilo della tutela del contesto privato (il *Privacy Act*, di fatto, riguarda soltanto il trattamento dei dati da parte degli uffici governativi), una protezione della *individual privacy* non generale e complessiva, bensì segmentato e da completare sulla base delle previsioni particolari (anche di natura autoregolamentare) dedicate a specifici ambiti nei quali, statisticamente, risulta maggiore l'incidenza nella vita privata degli individui[18].

[18] Si pensi, ad esempio, al settore degli investimenti finanziari ed a quello delle assicurazioni. Come osservato, è fuor di dubbio che esistano profonde divergenze di vedute, in materia di tutela del *right of privacy*, fra Europa e USA, dovute principalmente alla diversità di tradizione giuridica ed al differente sviluppo storico della disciplina in tema di privacy. Fondamentale, nella storia della dottrina statunitense in materia, è lo scritto di S.Warren – L. Brandeis, *The Right to Privacy,* in *4 Harvard Law Rev.* 193 (1890). Di notevole interesse anche Westin, *Privacy and Freedom*, New York, 1967, ed E. Aldermann – C. Kennedy, *Right to privacy*, New York, 1995, nonché E. Lawson, voce «*Privacy*», in *Encyclopaedia of Human Rights*, 2ª ed., Washington, 1996, 1194. Gli Stati Uniti, in effetti, sono generalmente favorevoli all'associazione fra soluzioni di mercato e tutela giuridica mirata per settori di particolare delicatezza (ad esempio: dati relativi a minori, cartelle sanitarie, informazioni bancarie) con una visione generale del diritto alla riservatezza molto liberale; l'Unione Europea, al contrario, predilige la definizione di un solido quadro giuridico di riferimento che potenzi il diritto dei singoli di intervenire sui dati personali che li riguardano. Gli USA, infatti, nonostante siano fra le prime nazioni ad aver adottato norme a tutela della privacy contro gli abusi del settore pubblico (grazie al *Privacy Act* del 1974), risultano attualmente molto più restii ad affrontare i numerosi rischi per la riservatezza che possono venire dal settore privato. Basti pensare che dei ventiquattro Paesi membri che hanno adottato le Linee-guida in materia di privacy

L'assenza, dunque, non soltanto di un sistema di principi generali come quello comunitario (il cosiddetto sistema *«one size fits all»*), ma di una stessa normativa di settore in grado di tutelare a pieno i soggetti privati (non soltanto statunitensi, ma anche comunitari, nel caso di trasferimento dei dati personali oltreoceano) ha condotto, per aggirare l'insufficienza delle garanzie per la persona, all'adozione dei *Safe Harbour Principles*, confluiti nella decisione 2000/520 adottata ai sensi dell'art. 25, par. 6, direttiva 95/46[19].

dell'OCSE, nel 1980, soltanto gli USA e la Turchia non hanno ancora approvato norme di legge o compiuto passi significativi in vista dell'approvazione di norme generali di riferimento in materia di privacy.

[19] Va detto, ad ogni modo, che sebbene le divergenze tra i due sistemi giuridici sembrassero, dopo l'accordo, all'apparenza superate, recentemente ed ancor prima della sentenza Schrems, il confronto si è riacceso, riproponendo il concreto pericolo del blocco dei flussi di dati globali, dei rapporti commerciali e dello sviluppo del commercio elettronico. Il nodo fondamentale è dato dal fatto che una parte della dottrina (e dell'opinione pubblica) statunitense ritiene che la disciplina europea in materia, così come i principi elaborati in sede di accordo, possano pregiudicare un'ampia gamma di transazioni via web, di natura finanziaria o per altri scopi, compromettendo la possibilità per le imprese USA di commercializzare beni e servizi entro i confini dell'Unione. In tema, v. P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, in 1*53 U. Pa. L. Rev.* 1975, 1986-87 (2005), nonché R. Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, in *54 Hastings L.J.* 1183 (2003).

2. I Safe Harbour Privacy Principles

Il lavoro di redazione dei *Safe Harbour Privacy Principles*[20] prende le mosse alcuni anni dopo l'entrata in vigore della c.d. direttiva privacy del '95 e vede impegnati il governo statunitense e le istituzioni comunitarie in una fitta trattativa della durata di circa due anni al cui termine, nel luglio del 2000, venne siglato l'accordo.

La finalità di questo *agreement*, come esplicitamente dichiarato dal *Department of Commerce* statunitense, è quella di «*diminish this uncertainty and provide a more predictable framework for such data transfers*», così da incoraggiare, promuovere e sviluppare il commercio internazionale e gli scambi commerciali fra Stati Uniti ed Unione Europea[21].

Il complesso di principi recepito nella decisione 2000/520/CE è destinato ad essere utilizzato esclusivamente da organizzazioni (non necessariamente imprese) statunitensi che intendano importare dati personali dall'Unione Europea al fine di conformarsi, giovandosi di un meccanismo presuntivo, al livello di protezione *adeguato* che la direttiva comunitaria

[20] U.S. Department of Commerce, *Safe Harbor Privacy Principles*, 21 luglio 2000, il cui testo completo è consultabile all'URL: http://www.export.gov/safeharbor/eu/eg_main_018475.asp/. La Decisione n. 2000/520 della Commissione europea si compone essenzialmente dei seguenti allegati: 1) i «Principi di approdo sicuro (*Safe Harbour*)», 2) le «Domande più frequenti (FAQ)», 3) l'«Applicazione (*enforcement*) dell'approdo sicuro», 4) il documento recante la «Tutela della riservatezza e risarcimento dei danni, autorizzazioni legali, fusioni, acquisizioni secondo la legge degli Stati Uniti», 5) e 6) un carteggio intercorso tra le Autorità governative degli Stati Uniti e la Commissione europea relativo a chiarimenti su specifiche questioni in materia di tutela della riservatezza. La decisione in parola è stata recepita, nell'ordinamento italiano, con la deliberazione del Garante Privacy del 10 ottobre 2001 n. 36 «*Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti, effettuati in base ai «Principi di approdo sicuro in materia di riservatezza» applicati in conformità alle «Domande più frequenti» (FAQ) ed all'ulteriore documentazione allegata alla Decisione della Commissione europea del 26 luglio 2000, n, 2000/520/CE*» (pubblicato in G.U. n. 275 del 26/11/2001). Sul provvedimento di recepimento adottato dal Garante si vedano, tra gli altri, Guerinoni – Bascelli, *Trasferimenti di dati personali all'estero. Il nuovo quadro normativo nazionale e le nuove regole comunitarie, in I Contratti*, 7, 2002, 74 ss., e Stumpo, *Osservatorio di diritto comunitario: il trasferimento dei dati fuori dalla UE*, in *Dir. e prat. soc.*, 4, 2002, 23 ss.

[21] Vedi S. Simitis, *Einleitung: Geschichte - Ziele - Prinzipien [Introduction: History - Goals - Principles]*, in *Kommentar Zum Bundesdatenschutzgesetz [Commentary on the Federal Data Protection Law]* 77 ss. (Spiros Simitis ed., 7th ed. 2011). Più in generale, C. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, in *147 U. Pa. L. Rev.* 613 (1999).

impone per i flussi extraeuropei di informazioni[22].

Il sistema dei *Principles* si fonda, pertanto, sulla logica dell'adesione volontaria delle organizzazioni statunitensi ad un sistema disciplinare di tutela della privacy fondato su un nucleo minimo di principi tratti dalla direttiva 95/46/CE, funzionale a garantire ai cittadini europei, i cui dati vengano esportati oltreoceano, un livello di garanzie adeguato[23].

Il *Department of Commerce*, al fine di assicurare la corretta applicazione della decisione 2000/520, compila e rende disponibile al pubblico un elenco delle organizzazioni che abbiano deciso di aderire ai *Safe Harbour*, in modo da rendere riconoscibili le stesse tanto per i privati i cui dati saranno oggetto di trasferimento extraeuropeo, tanto per le autorità di controllo comunitarie[24].

2.1. I principi codificati

Il sistema dei *Safe Harbour Principles* si compone, innanzitutto, di 7 principi generali e 15 *frequently asked questions and answers* (FAQs), da

[22] Cfr. F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in 48 *B.C. L. Rev.* 609, 684 (2007). Nel testo della decisione 2000/520/CE, opportunamente, al fine fi evitare qualsivoglia forma di incertezza interpretativa circa la porta applicativa dei principi, si chiarisce pure che «*because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States*».

[23] Come rivela A. Mantelero, Data protection ed attività di impresa, cit., 458 ss., la *Federal Trade Commission*, nell'ambito della propria competenza in materia di trattamento dati dei consumatori, ha adottato il c.d. «notice-and-choice model», caratterizzato dalla possibilità di un ampio ricorso a forme di consenso implicito. D'altronde, come evidenziato dalla stessa FTC nel documento «*Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*» del marzo 2012 (reperibile alla pagina web: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers) «*the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand*». L'Autore evidenzia ancora come, sempre nell'ottica di un intervento minimo in materia di privacy, la FTC abbia altresì fatto ricorso il c.d. «*harm-based model*», rinunciando ad una tutela di portata generale del consumatore ed optando invece per un intervento di protezione calibrato su peculiari tipologie di danno potenziale («*physical security, economic injury, and unwanted intrusions into their daily lives*»). In tema, vedi anche A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007.

[24] Propone una lettura critica ai *Safe Harbour Privacy Principles*, con diverse proposte di modifica, D.R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, in *41 Case W. Res. J. Int. L.* 193 (2009).

leggere in combinato disposto ed in una logica di interpretazione complessiva che ne favorisca l'applicazione ed il concreto recepimento da parte delle organizzazioni americane.

Nel novero dei principi essenziali, è sancito, innanzitutto, un generale dovere di informazione in favore degli interessati (*notice principle*) assimilabile soltanto in parte a quello di cui agli artt. 10 e 11 della direttiva 95/46/CE. Tale informativa ha ad oggetto le finalità per cui vengono raccolte e utilizzate le informazioni, le modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, la tipologia dei terzi a cui vengono fornite le informazioni e, infine, le opzioni e i mezzi che le organizzazioni interessate pongono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni.

L'importatore di dati statunitense è tenuto a garantire siffatta informativa secondo un linguaggio chiaro e in modo da attirare l'attenzione quando si tratti del primo invito a fornire informazioni personali oppure non appena ciò risulti successivamente possibile, ma comunque prima che l'importatore utilizzi o riveli per la prima volta a terzi siffatte informazioni per finalità diverse da quelle per le quali le stesse erano state originariamente raccolte[25].

Sotto l'enunciazione del principio del consenso (*choice principle*), al meccanismo giuridico dell'*opt-in* è affidato il trattamento dei dati sensibili[26], con la necessità, quindi, del consenso espresso dell'interessato («*affirmative or explicit choice*») in relazione alla rivelazione a terzi delle informazioni o alla utilizzazione delle stesse per finalità differenti rispetto a quelle originarie o successivamente autorizzate.

Per i dati comuni, al contrario, è sufficiente che l'importatore statunitense garantisca all'interessato meccanismi di consenso implicito (secondo il paradigma dell'*opt-out*, anche per la cessione a terzi). In sostanza, l'in-

[25] Tuttavia, «*it is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures*». Sul punto, interessanti sono le riflessioni offerte da P. M. Schwartz, *Feature, Preemption and Privacy*, in 118 *Yale L.J.* 902, 915 (2009).

[26] Per «*informazioni di carattere sensibile*», ai sensi dei *Safe Harbour Privacy Principles*, devono intendersi quelle relative alle condizioni mediche e sanitarie, all'origine etnica o razziale, alle opinioni politiche, alle credenze filosofiche o religiose, all'appartenenza a sindacati ed, infine, alla vita sessuale. Va evidenziato, inoltre, che andrà considerata di carattere delicato anche «*any information received from a third party where the third party treats and identifies it as sensitive*». In tema, di recente, P.M. Schwartz – D.J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, in 86 *N.Y.U. L Rev.* 1814, 1823 (2011)

teressato deve avere la possibilità di esercitare una vera e propria facoltà di rifiuto rispetto alla rivelazione a terzi dei propri dati personali, nonché in ordine all'utilizzazione degli stessi per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati[27].

Analogamente al disposto dell'art. 12 della direttiva 95/46/CE, agli interessati è garantita, inoltre, facoltà di accesso ai dati (*access principle*), con il potere di rettifica, aggiornamento e cancellazione degli stessi, potere che può essere limitato soltanto in ipotesi particolari[28].

I principi di *notice* e *choice*, come codificati nei *Safe Harbour*, si applicano anche ai cd. trasferimenti successivi (*onward transfer principle*), allorché l'ente statunitense intenda trasferire i dati personali a terzi. Quando il terzo destinatario dei dati agisce in qualità di rappresentante, l'importatore, prima del procedere al trasferimento, deve accertarsi che il destinatario aderisca ai *Principles* o, comunque, rientri nel campo d'applicazione delle norme comunitarie in materia o, ancora, di altri modelli che garantiscano idonee tutele per gli interessati. In ultima analisi, l'organizzazione statunitense, al fine di procedere al trasferimento dei dati personali a terzi, può stipulare con questi ultimi un accordo scritto che comporti per gli stessi l'obbligo di offrire almeno «*the same level of privacy protection as is required by the relevant Principles*»[29].

In conformità ai principi cardinali codificati nella direttiva 95/46/CE, poi, all'importatore statunitense viene imposto il rispetto dei principi di sicurezza (*security principle*) ed integrità dei dati personali (*data integrity principle*). In particolare, con formula non lontana dal dettato dell'art. 17

[27] Cfr. K.A. Bamberger – D. Mulligan, *Privacy on the Books and on the Ground*, in 63 *Stan. L. Rev.* 247 (2011). Agli interessati, in ogni caso, dovranno essere forniti mezzi chiari, agevolmente riconoscibili in quanto tali, di rapida fruizione e di costo accettabile per esercitare la propria scelta: «*Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice*».

[28] Nei *Safe Harbour Principles*, difatti, si chiarisce che «Individuals must have access to personal information about them that an organization holds and be able to correct, amend, *or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated*».

[29] In relazione a possibili profili responsabilistici, a chiosa dell'enunciazione dell'*onward transfer principle*, viene specificato che «*if the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing*».

della direttiva privacy, l'importatore statunitense, ove detenga, aggiorni, utilizzi o diffonda informazioni personali deve adottare ragionevoli precauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati. Inoltre, le informazioni personali devono risultare pertinenti ai fini per cui sono state raccolte od a quelli successivamente autorizzati dagli interessati: se ed in quanto necessario per tali fini l'ente statunitense deve assumere *«reasonable steps»* per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati[30].

L'ultimo dei principi enunciati è quello di *enforcement*, inerente la predisposizione di meccanismi volti a garantire, in concreto, il rispetto dei *Principles*, la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi medesimi, e la non impunità degli enti inadempienti[31].

Come è evidente, i sette principi codificati in sede di accordo USA – UE finiscono per imporre all'importatore americano di dati personali di matrice europea gli obblighi essenziali che la direttiva 94/46/CE prescrive in capo ai titolari di trattamento comunitari, con una sostanziale esportazione, unitamente ai dati personali, del modello europeo di disciplina del diritto alla riservatezza.

2.2. Le FAQ

Come osservato, i sette principi che costituiscono il nucleo dei *Safe Harbour Principles* devono essere letti, interpretati ed applicati unitamente alle 15 *Frequently Asked Questions and Answers* (FAQs), anch'esse recepite in sede comunitaria con la decisione 2000/520.

Le FAQ riguardano alcuni aspetti specifici dell'applicazione dei

[30] V. K.A. Bamberger – D. Mulligan, *Privacy on the Books and on the Ground*, cit., 256.
[31] Cfr. J. Reidenberg, *Privacy Wrongs in Search of Remedies*, in 54 *Hastings L.J.* 877 (2003). Nel testo dei *Safe Harbour*, quale soglia minima di *enforcement,* vengono identificati i seguenti meccanismi: *«(a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations».*

Principles ed, in particolare, *Sensitive data*, *Journalistic exceptions*; *Secondary liability*; *Investment banking and audits*; *The role of the data Protection Authorities*; *Self-certification*; *Verification*; *Access*; *Human resources*; *Article 17 contracts*; *Dispute resolution and enforcement*; *Choice - timing of opt-out*; *Travel information*; *Pharmaceutical and medical products* e *Public record and publicly available information*[32].

Nella prospettiva di un'analisi comparatistica, le regole operazionali emergenti dalle FAQ possono essere funzionali vuoi a completare quel processo di 'assimilazione' delle tutele garantite dall'ordinamento statunitense con il sistema di principi e regole desumibile dalla direttiva 95/46/CE, vuoi a marcare le differenze rispetto all'*acquis communautaire* maturato in materia di tutela della riservatezza.

È il caso, ad esempio, della FAQ 1, dedicata ai dati sensibili, che riprende diverse ipotesi codificate dall'art. 8, co. 2, della direttiva comunitaria ai fini dell'esenzione dal sistema dell'*opt-in choice* anche per i *sensitive data* o, ancora, della FAQ 2, che disciplina il delicato equilibrio tra riservatezza e *freedom of the press*, attribuendo comunque prevalenza al *First Amendment* della Costituzione americana. In maniera analoga, l'articolata serie di «questions and answers» che compongono la FAQ 8, in materia di diritto di accesso, contribuisce ad offrire all'interprete una sostanziale sintesi del quadro normativo comunitario consolidatosi sul punto, a partire dalla direttiva 95/46, come interpretata nelle decisioni della Corte di Giustizia e negli interventi delle autorità indipendenti nazionali.

In buona sostanza, dunque, molte delle FAQ che completano il sistema dei *Safe Harbour Principles* non rappresentano soltanto uno strumento interpretativo essenziale dei principi codificati nel 'ponte' UE-USA, ma contengono regole ulteriori e peculiari, funzionali, il più delle volte, ad esplicitare come, di là dalla distanza delle declamazioni astratte, le norme operazionali consolidatesi nelle prassi dei due ordinamenti possano essere estremamente simili[33]. In altri casi, come detto, la logica delle FAQ è inve-

[32] Per approfondimenti circa le FAQ e la portata applicativa delle stesse, Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor*, cit., 196.

[33] Secondo il noto principio euristico della *praesumptio similitudinis*, le soluzioni pratiche adottate da differenti ordinamenti si rivelano spesso assimilabili o sostanzialmente uniformi, anche a fronte di declamazioni di principio e concettualizzazioni generali che si presentano molto lontane le une dalle altre. In dottrina, per tutti, K. Zweigert – H. Kötz, *Introduzione al diritto comparato*, vol. I, Milano, 1998, 44, nonché R. Sacco, *Introduzione al diritto comparato*, Torino, 1992, 47 ss. Ha proposto, al contrario, il principio della *praesumptio dissimilitudinis*, P. Legrand, *The Return of the Repressed: Moving Comparative Legal Studies beyond Pleasure*, in *75 Tul. Law Rev.* 1048 (2001).

ce quella di offrire risalto a specificità sistematiche della regolamentazione della materia proprie degli Stati Uniti, che il *Safe Harbour system* comunque non va ad intaccare: si tratta dell'esplicitazione di un sostanziale argine a potenziali rischi di eccessiva europeizzazione delle prassi d'oltreoceano in materia.

Come detto, il quadro degli *USA-UE Safe Harbour*, oltre ai *Privacy Principles* ed alle FAQ, si completa con le lettere dalla *Federal Trade Commission* e del *Department of Trasportation* relative ai rispettivi poteri di *enforcement*, nonché con lo scambio di missive tra il *Department of Commerce* statunitense e la Commissione europea e, infine, con la decisione 2000/520/CE che – preso atto dell'accordo *Safe Harbour* e dei relativi allegati – certifica l'adeguatezza del livello di tutela garantito dall'ordinamento statunitense in ordine ai *transborder data flows*[34]. Il complesso di questi ulteriori documenti svolge, nella logica complessiva del sistema dei *Safe Harbour* e della demarcazione di confini rispetto all'influenza dell'ordinamento comunitario su quello statunitense in materia di tutela della riservatezza, una funzione interpretativa dei *Principles* assolutamente analoga a quella evidenziata in merito alle FAQ.

2.3. Ambito di applicazione e 'self certification scheme'.

La portata sostanziale dei *Safe Harbour Principles* incontra importanti limiti oggettivi rispetto al proprio ambito di applicazione, dal momento che la possibilità di aderire a questo sistema di principi è limitata esclusivamente alle organizzazioni statunitensi che operino nei settori sottoposti all'autorità della *Federal Trade Commission* o del *Department of Transportation*.

Questo comporta l'esclusione dai *Principles* di importanti operatori economici, che pure possono far ricorso a forme di massiccia importazione di dati personali: si pensi alle istituzioni finanziarie, comprese banche, casse di risparmio e unioni di credito[35]; alle assicurazioni[36]; ai vettori comuni di

[34] Cfr. C. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, in *Privacy & Security L. Rep.* 215 (2012).

[35] Questo specifico ambito è soggetto ai regolamenti emanati dal *Federal Reserve Board, dall'Office of Thrift Supervision e dal National Credit Union Administration Board*

[36] Il *McCarran-Ferguson Act* (15 U.S.C. § 1011 et seq.), infatti, affida la regolamentazione delle attività assicurative ai singoli stati. Tuttavia, le disposizioni del *FTC Act* si applicano all'industria assicurativa «*nella misura in cui tali attività non sono regolate da leggi statali*». La *Federal Trade Commission*, dunque, è competente nel caso di pratiche

telecomunicazione (tra cui gli *Internet Service Providers*)[37] e di trasporti interstatali; ai vettori aerei[38] ed agli operatori del settore zootecnico[39].

Peraltro, visto che l'autorità della *Federal Trade Commission* è limitata alle pratiche sleali o ingannevoli in materia commerciale o collegata al commercio (*«in or affecting commerce»*), non ricadono nell'ambito di applicazione dei *Safe Harbour* tutte le forme di raccolta ed utilizzazione di dati personali a fini non commerciali, quali, ad esempio, la raccolta di fondi per attività caritatevoli.

Ancora, tali principi sono applicabili soltanto alle organizzazioni americane private che ricevono dati personali dall'Unione, mentre le autorità pubbliche non sono tenute al rispetto degli stessi[40].

Il meccanismo di applicazione dei *Safe Harbour Principles* è quello del *«self certification scheme»*, in base al quale l'operatore statunitense gode della presunzione di adeguatezza di tutela e può procedere all'importazione di dati personali dall'Unione Europea dalla data in cui autocertifica al *Department of Commerce* l'adesione ai principi[41].

sleali o ingannevoli poste in essere da società di assicurazione, nel caso in cui tali società non siano impegnate in attività assicurative. Ciò potrebbe comprendere, ad esempio, il caso di assicuratori che vendono informazioni personali sui loro assicurati a imprese di marketing diretto di prodotti non assicurativi.

[37] In questo caso, il *Communications Act* prevede che la disciplina del *«interstate and foreign commerce in communication by wire and radio»* sia rimessa all'autorità della *Federal Communications Commission* (FCC). Cfr. 47 U.S.C. §§ 151 e 152.

[38] In materia trova applicazione il *Federal Aviation Act* del 1958 ed i vettori aerei sono soggetti all'autorità del *Department of Transportation*.

[39] Rispetto a questi ultimi, il riferimento normativo è al *Packers and Stockyards Act* del 1921 (7 U.S.C. § 181 et seq.) ed ai poteri attribuiti al *Secretary of Agriculture*.

[40] Cfr. par. 82 della decisione.

[41] Si rinvia ancora a stesse, D.R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor,* cit., 196. Come chiarito dalla FAQ 6, *«To self-certify for the Safe Harbor, organizations can provide to the Department of Commerce (or its designee) a letter – signed by a corporate officer on behalf of the organization that is joining the Safe Harbor – that contains at least the following information: 1. name of organization, mailing address, email address, telephone and fax numbers; 2. description of the activities of the organization with respect to personal information received from the EU; and 3. description of the organization's privacy policy for such personal information, including: a. where the privacy policy is available for viewing by the public, b. its effective date of implementation, c. a contact office for the handling of complaints, access requests, and any other issues arising under the Safe Harbor, d. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), e. name of any privacy programs in which the organization is a member, f. method of verification (e.g. in-house, third party) and g. the independent recourse mechanism that is available to investigate unresolved complaints».*

L'impegno al rispetto dei *Principles* va ribadito con cadenza almeno annuale ed, anche se non rinnovato, non viene meno per quanto riguarda i dati ricevuti durante il periodo nel quale l'operatore ha goduto dei vantaggi del *Safe Harbour agreement*. Ai fini della dichiarazione di adesione ai *Principles*, l'organizzazione statunitense può attestare il rispetto dei principi tramite procedure di autovalutazione (*«self-assessment approach»*) oppure facendo ricorso a revisioni esterne (*«outside compliance reviews»*)[42].

L'autocertificazione dell'impegno ad adeguarsi ai principi comporta l'obbligo di applicare le relative regole ai dati importati sino a quando l'operatore continuerà a trattarli, anche se successivamente dovesse per qualsiasi motivo abbandonare il sistema dei *Safe Harbour*. Peraltro, l'operatore che accetta i principi non è tenuto ad applicarli indistintamente a tutti i trattamenti di dati personali che pone in essere, bensì esclusivamente a quelli che abbiano ad oggetto informazioni trasferite dall'Unione Europea dopo la volontaria adesione all'accordo[43].

Come sottolineato dalla Corte di Giustizia al paragrafo 81 della decisione *Schrems*, il ricorso, da parte di un Paese terzo, ad un sistema di autocertificazione non è di per sé contrario al requisito previsto dall'art.

[42] La FAQ 7 precisa che *«Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self- assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance". Al contrario, nel caso di revision esterna, «such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of 'decoys' or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance»*.

[43] Per una riflessione sui possibili scenari configurati dalla sentenza Schrems nell'ambito della sovranità digitale v. V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in questo Volume.

25, co. 6, della direttiva 95/46/CE; tuttavia, l'affidabilità di un sistema siffatto finisce per fondarsi essenzialmente sulla contestuale predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali ed, in particolare, del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali[44].

Sino alla pronuncia della sentenza *Schrems*, l'adesione al complesso dei *Safe Harbour Privacy Principles*, attraverso l'omologazione in chiave europea garantita dalla già citata decisione della Commissione, consentiva in pratica alle imprese statunitensi che trattano dati personali importati dall'Europa di evitare il pericolo di veder bloccato il trasferimento su iniziativa di autorità amministrative indipendenti o giurisdizionali degli Stati membri UE, nel momento in cui avessero dovuto fondare il proprio giudizio sulle sole regole vigenti oltreoceano[45].

I *Safe Harbour Principles* hanno in sostanza operato una sorta di *by-pass* tra la tutela dei dati personali di stampo comunitario e il diverso approccio adottato negli Stati Uniti garantendo uno spostamento ininterrotto di dati dal primo al secondo ordinamento, svolto sia per fini commerciali che, come la vicenda *Snowden* insegna, per motivi di sicurezza nazionale. Nel corso dei quindici anni di vigenza dell'accordo, un numero maggiore ai 5000 organismi ha sottoscritto o ancora adesso ottempera all'accordo[46].

[44] Analoghe perplessità sono state formulate anche oltreoceano: vedi, ad esempio, P. Swire, *Why the Federal Government Should Have a Privacy Policy Office*, in *10 J. Telecomm. & High Tech. L.* 41, 46-47 (2012).

[45] Per quanto concerne i costi di adesione al *Safe Harbour framework, «an organization that is self-certifying its compliance with the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework for the first time on or after March 1, 2009 must remit a one-time processing fee of $200.00. An organization that has previously self-certified its compliance with the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework and is due to reaffirm its compliance with the Framework(s) on or after April 1, 2009 must remit an annual processing fee of $100.00 on or before the anniversary of the organization's original self-certification»* (tratto dalla pagina *web*: http://build.export.gov/main/safeharbor/eg_main_020436).

[46] La lista completa è disponibile all'URL: https://safeharbor.export.gov/list.aspx/.Va detto che, nella primissima fase di adozione dei *Safe Harbour Privacy Principles*, pochissime organizzazioni statunitensi decisero di aderireagli stessi e, tra i pochi aderenti, appena una decina appartenevano al settore delle imprese. Questa iniziale diffidenza comportò il legittimo sospetto che vi fosse addirittura carenza di reale sostegno politico nei confronti dei *Principles*. In sostanza, sino ai primi anni dello scorso decennio, la maggior parte delle transazioni di dati personali tra Europa e Stati Uniti era ancora affidata a non poco pressappochismo ed alla 'fuga' dalla disciplina della Direttiva 95/46/CE. Il cambiamento

In sintesi, il 'ponte transatlantico' creato dalla decisione 2000/520/CE (e momentaneamente chiuso dalla Corte di Giustizia) poteva apparentemente contare, sul piano operazionale, di due distinte 'falle' applicative insite nell'accordo stesso: da un lato, esso non si estende a precisi settori quali quello delle telecomunicazioni, dei servizi bancari e finanziari e del 'no-profit'; dall'altro, gli organismi investiti del compito di vigilare in territorio statunitense sulla sua attuazione sono il *Department of Transportation* (solo per ciò che concerne le compagnie aeree e l'emissione di biglietti) e, soprattutto, la *Federal Trade Commission* (FTC) la quale, come è stato ribadito numerose volte nel corpo della sentenza[47], svolge un'attività di controllo limitata a pochi settori del mercato delle informazioni, attività peraltro esclusivamente orientata verso la tutela del consumatore[48].

2.4. La «supremacy clause» in favore del diritto statunitense

Nella decisione *Schrems*, la Corte di Giustizia, nel percorso argomentativo che porterà all'annullamento della decisione 2000/520, evidenzia, in più occasioni[49], come uno dei profili di maggiore criticità dei *Safe Harbour Principles* sia legato alle ipotesi in cui l'applicabilità dei principi possa incontrare delle limitazioni derivanti dalla supremazia del diritto statunitense rispetto all'accordo[50].

---

di prospettiva è legato, senza dubbio, all'affermarsi dei colossi imprenditoriali della Rete, che operando a livello globale e transnazionale hanno ritenuto di adoperare lo strumento giuridico dei *Safe Harbour* per non correre il rischio di vedersi precluso un mercato fondamentale quale quello europeo. Vedi ancora P. Swire, *Elephants and Mice Revisited*, cit., 1990.

[47] V. ad es. CGE Grande sez., 6 ottobre 2015, causa C-362/14, cit., par. 89: *«A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane, dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingerenze nei diritti fondamentali risultanti da misure di origine statale».*

[48] V. Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting of U.S. Privacy Standards*, in *25 Yale J. Int. L.* I, 87 (2000).

[49] Si pensi, a titolo esemplificativo, ai paragrafi 83/89 della decisione. Nella dottrina statunitense, J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, in *38 Hous. L. Rev.* 717 (2001).

[50] Per una riflessione sui possibili scenari configurati dalla sentenza Schrems nell'ambito della sovranità digitale v. V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems:*

Secondo quanto previsto dalle premesse ai *Principles*, infatti, l'adesione a tali principi può essere limitata: *a*) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti; *b*) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure *c*) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili[51].

La Corte di Giustizia, con la sentenza *Schrems*, sottolinea come tutto l'impianto della decisione 2000/520 sia evidentemente assoggettato, in ordine alla sua applicazione concreta, al primato delle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia statunitensi, «primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime»[52].

Di conseguenza, in forza dell'esistenza di questa sorta di «supremacy clause» in favore del diritto statunitense, i *Safe Harbour Principles* finiscono per esporre i dati personali importati negli Stati Uniti a possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, con conseguente compromissione dei diritti fondamentali dei soggetti interessati[53].

Ancor prima della pronuncia della Corte di Giustizia nello *Schrems*

la sovarnità digitale e il governo internazionale nelle reti di telecomunicazioni, retro questo Volume.

[51] Vedi F. Bignami, *European versus American Liberty*, cit., 684, nonché F.H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, in *80 Iowa L. Rev.* 431 (1995).

[52] Così par. 86 della decisione. Cfr. L. Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, in *21 Eur. J. Int. L.* 441 (2010).

[53] Peraltro, in conformità con la propria giurisprudenza precedente, la Corte di Giustizia sottolinea (par. 87) come «*a tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C293/12 e C594/12, EU:C:2014:238, punto 33 e la giurisprudenza ivi citata)*».

case, questo specifico elemento di criticità era stato già ampiamente analizzato dalla Commissione in due comunicazioni al Parlamento ed al Consiglio risalenti al 2013 (rispettivamente nn. 846 e 847), ove si evidenziava come, tenuto conto dei 'punti deboli' individuati, il regime dei *Safe Harbour* non poteva continuare ad essere applicato secondo le attuali modalità e che, nonostante ciò, l'abrogazione dello stesso avrebbe compromesso in maniera rilevante l'attività di imprese operati sia in Europa che negli Stati Uniti[54].

D'altronde, l'incontrollata ed accertata ingerenza di matrice pubblicistica (in particolare ad opera dei servizi di *intelligence* statunitensi) nelle prerogative primarie dei cittadini comunitari si rivela assolutamente incompatibile con il quadro di principi animante la direttiva 95/46/CE, tanto più ove si consideri che la decisione 2000/520 non contiene alcun passaggio specifico dedicato all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale. Analogo silenzio si registra, nei *Principles*, rispetto all'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di matrice pubblicistica[55].

[54] Il riferimento nel testo, presente in diversi passaggi della sentenza Schrems (ad esempio, al paragrafo 90), è a COM(2013) *846 final («Rebuilding Trust in EU-US Data Flows»*, reperibile all'indirizzo http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf), ed a COM(2013) 847 *final («On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU»*, alla pagina *web* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf), ambedue del 27 novembre 2013. Le due comunicazioni trovavano il proprio fondamento nella cooperazione tra Unione Europea e Stati Uniti in seguito alla rivelazione dell'esistenza, negli USA, di diversi programmi di controllo che comprendevano la raccolta e il trattamento su larga scala di dati personali. In particolare, tutte le imprese partecipanti al programma PRISM (un programma di raccolta di informazioni su larga scala), che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultavano certificate nel quadro dei *Safe Harbour* e che siffatto sistema era perciò diventato, in dispregio dei principi di necessità e proporzionalità, una delle principali piattaforme di accesso delle autorità americane di *intelligence* alla raccolta di dati personali inizialmente trattati nell'UE (come evidenzia la Corte di Giustizia discorriamo di veri e propri colossi del mercato della comunicazione, come Google, Facebook, Microsoft, Apple, Yahoo).

[55] In tema, C. Bennett – C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, 2006, 127 ss. e ancora G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE, retro* in questo Volume.

3. I poteri della Federal Trade Commission*, quelli delle* Data Protection Authorities *europee e la responsabilità aquiliana*

La vigilanza sul rispetto dell'accordo, come visto, viene esercitata – almeno in prima battuta - dalla *Federal Trade Commission*, un organismo competente in materia di pratiche commerciali sleali o ingannevoli o, più in generale, che si concentra sull'utente inteso come centro di interesse di attività di tipo consumeristico[56].

In particolare, nel momento in cui un'organizzazione statunitense dichiari di aderire ai *Safe Harbour Principles*, accetta di sottoporsi, anche rispetto a questo specifico profilo, all'autorità della *Federal Trade Commission* ai sensi della *section* 5 del *Federal Trade Commission Act* (15 U.S.C., §§ 41-58).

Ne deriva che il mancato rispetto degli impegni assunti dall'importatore in ordine alla tutela della riservatezza venga equiparato, ai sensi della *section* 5, ad una pratica ingannevole[57]. Difatti, sebbene il sistema dei *Safe Harbour* si fondi su un meccanismo di adesione assolutamente volontario, ciò non esclude come gli operatori che intendano avvalersi della presunzione di garanzia di un livello di tutela adeguato, ai sensi della disciplina comunitaria, siano tenuti a dichiarare esplicitamente la propria volontà di tutelare le informazioni raccolte in conformità ai *Principles*, sicché la violazione di siffatto impegno costituisce *«deceptive practice»* ai sensi del *Federal Trade Commission Act*. Ad esempio, la rappresentazione ingannevole dei motivi per cui le informazioni vengono raccolte dai consumatori o delle modalità di trattamento dei dati personali può essere sanzionata dalla Commissione Federale quale pratica ingannevole in danno dei consumatori[58].

[56] Il *Department of Commerce* cura la tenuta di un elenco di tutti gli operatori che abbiano dichiarato di osservare i *Safe Harbour Principles*, aggiornandolo con cadenza annuale. In tema, W.E. Kovacic, *The Federal Trade Commission as Convenor: Developing Regulatory Policy Norms Without Litigation or Rulemaking*, in *13 J. on Telecomm. & High Tech. L.* 17 (2015) ed *ivi* ampi riferimenti bibliografici; e ancora G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in questo Volume, parr. 2 e ss. ..

[57] Per *«deceptive practice»*, ai sensi della section 5 del *Federal Trade Commission Act*, si intende *«a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion»*. In tema, M. Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, in *Stan. Tech. L. Rev.* 1 (2001).

[58] Rispetto a questo profilo, interessanti spunti di riflessione sono in F.H. Cate, *The Failure of Fair Information Practice Principles, in Consumer Protection in the Age of the «Information Economy»* 341 (Jane K. Winn ed., 2006).

I poteri della *Federal Trade Commission* in materia di violazione dei *Safe Harbour* sono, allora, dettati dalla *section* 5 (ed, in particolare, dal 15 U.S.C. § 45)[59]: l'autorità dichiara l'illiceità di *«unfair or deceptive acts or practices in or affecting commerce»* e può porre in essere idonee misure *«to prevent such acts and practices»*, nonché pronunciare *«cease and desist orders»* al fine di far cessare violazioni già in atto.

Inoltre, per motivi d'interesse pubblico, la Commissione Federale ha facoltà di sollecitare la pronuncia da parte di una *District Court* di un *«temporary restraining order»* oppure di una *«temporary or permanent injunction»*[60] e, qualora vi sia stata ampia diffusione della pratica sleale o ingannevole o la FTC abbia già formulato ordinanze di cessazione e di desistenza in materia, può promulgare *«an administrative rule prescribing the acts or practices involved»*[61].

Ad esempio, con specifico riferimento alle attività di vigilanza sui trattamenti dei dati personali dei consumatori svolte nel corso degli ultimi cinque anni di vigenza dei *Safe Harbour Principles*, la *Federal Trade Commission* ha emanato numerosi ordini nei confronti dei principali *players* del settore della prestazione di servizi del cd. *web* 2.0.

Nell'ordine del marzo 2011 contro *Twitter*[62], la FTC ha rilevato, a seguito di un'articolata attività d'indagine, numerosi comportamenti non consentiti, richiamando espressamente la protezione della privacy dei consumatori. Il provvedimento ordina in primo luogo a *Twitter* di ottemperare in maniera adeguata ai doveri di trasparenza, informazione e sicurezza rispetto al trattamento delle cd. *«non public consumer informations»*, ovvero tutte quelle informazioni non rese pubbliche dall'interessato che ne consentano l'identificazione o ne indichino la provenienza (ad. es. e-mail, indirizzo IP, numero di telefono, informazioni prodotte attraverso canali di comunicazioni privati forniti dal prestatore).

In particolare, la FTC ha rilevato la sussistenza di pratiche atte a falsare la tutela della sicurezza, della privacy, della confidenzialità e dell'integrità

[59] Da sottolineare che chiunque non rispetti le ordinanze della *Federal Trade Commission* è soggetto a *civil penalty* fino a un massimo di $ 10.000, con ciascun giorno in cui l'inottemperanza persista costituente violazione a sé stante [cfr. 15 U.S.C. § 45(1)]. Allo stesso modo, chiunque infranga scientemente una regola dettata dalla Commissione Federale è passibile di *civil penalty* per $ 10.000 per ciascuna violazione [cfr. 15 U.S.C. § 45(m)]. Le azioni volte ad ottenere l'ottemperanza possono essere intraprese dal *Department of Justice* o, in alternativa, dalla stessa FTC (cfr. 15 U.S.C. § 56).

[60] Cfr. 15 U.S.C. § 53(b). Cfr. anche V. D'Antonio, *Il trasferimento dei dati all'estero*, cit., 165.

[61] Cfr. 15 U.S.C. § 57(a).

[62] FTC, In the Matter of Twitter Inc., 2 marzo 2011, docket no. C-4316.

delle informazioni non pubbliche, imponendo altresì al prestatore una serie di obblighi di adeguamento delle proprie prassi ai principi vigenti in materia di tutela della riservatezza.

L'ordine, che ha durata ventennale, dispone infatti il dovere di approntare e rendere effettivo un articolato programma di protezione dei dati non pubblici dei consumatori basato sull'individuazione di un responsabile del trattamento e sulla creazione di un apparato tecnico di tutela e salvaguardia (fondato sulla preventiva analisi dei rischi connessi). Il programma è sottoposto alla vigilanza ed al controllo (iniziale e poi a cadenza biennale) da parte di un organismo terzo e qualificato[63]; sul prestatore gravano altresì precisi doveri di *disclosure* nei confronti della Commissione[64].

Il provvedimento vincolante emesso contro *Twitter* è stato seguito da misure di tenore analogo che hanno interessato nell'ordine *Google*[65], *Facebook*[66] e *Myspace*[67].

In particolare, gli ordini ricalcano con maggiore dovizia di particolari le prescrizioni precedentemente descritte, adattandole agli specifici servizi

[63] I*n the Matter of Twitter Inc*, cit., p. 4: «*It Is Further Ordered that, in connection with its compliance with Paragraph II of this order, respondent shall obtain initial and biennial assessments and reports («Assessments») from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. […]*»

[64] *In the Matter of Twitter Inc*, cit., p. 5: «*It Is Further Ordered that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of: A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely-disseminated statements, including, but not limited to, statements posted on respondent's website that describe the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, with all materials relied upon in making or disseminating such statements, except that respondent shall not be required to provide any such statements that are made using the Twitter microblogging platform; B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that relate to respondent's activities as alleged in the draft complaint and any responses to such complaints; C. for a period of two (2) years from the date received, copies of all subpoenas and other communications with law enforcement entities or personnel, if such communications raise issues that relate to respondent's compliance with the provisions of this order; D. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and E. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment*».

[65] FTC, *In the Matter of Google Inc.*, 13 ottobre 2011, docket no. C-4336.

[66] FTC, *In the Matter of Facebook Inc.*, 27 luglio 2012, docket no. C-4365.

[67] FTC, *In the Matter of My Space LLC.*, 30 agosto 2012, docket no. C-4369.

offerti da ogni prestatore e rafforzando i concetti di trasparenza, consenso e sicurezza delle informazioni trattate con riguardo a tutte le tipologie di dati personali raccolte dai prestatori (cd. *covered information*[68]).

In questo senso, le misure comminate dalla FTC attraverso un approccio *case-by-case* hanno concorso a richiamare l'attenzione sull'efficacia vincolante di alcuni principi-chiave della tutela della riservatezza di stampo comunitario e sulle modalità di corretta ottemperanza agli stessi: a conferma di ciò, gli ultimi tre ordini vietano espressamente ogni forma di violazione e *misrepresentation* concernente accordi o programmi governativi volti a proteggere la privacy dei consumatori, tra i quali appunto viene citato il *Safe Harbour Framework*[69].

Sul versante europeo, la violazione dei *Principles* da parte di quelle organizzazioni statunitensi che hanno aderito agli stessi può comportare, indipendentemente dall'accertamento da parte della *Federal Trade Commission*, una sospensione dei flussi di dati personali.

Nello specifico, l'art. 3 della decisione 2000/520 prevede espressamente che le *Data Protection Authorities* nazionali degli Stati membri possano 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 verso un'organizzazione che abbia autocertificato la propria adesione ai *Safe Harbour Principles* sia quando vi sia stato l'accertamento di una violazione da parte degli organismi di controllo statunitensi, sia

[68] V. per tutti FTC, *In the Matter of Google Inc.*, cit., p. 3: «*'Covered information' shall mean information respondent collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above*».

[69] Si veda per tutti FTC, *In the Matter of My Space LLC*, cit., p. 2: «*It Is Ordered that respondent, and its officers, agents, representatives and employees, acting directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication: A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to: (1) the purposes for which it collects and discloses covered information, and (2) the extent to which it makes or has made covered information accessible to third parties. B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework*».

allorché sia soltanto molto probabile che i principi vengano violati. In quest'ultimo caso, tuttavia, devono sussistere pure *ragionevoli motivi* per ritenere che l'organismo di controllo statunitense non stia adottando o non adotterà misure adeguate e tempestive per risolvere il caso concreto, vi deve essere un rischio imminente di gravi danni per gli interessati in relazione alla continuazione del trasferimento dei dati ed, infine, l'autorità nazionale europea deve aver posto in essere procedure idonee, date le circostanze, ad informare l'organizzazione interessata, dando alla stessa l'opportunità di replicare alle censure.

Chiaramente, la sospensione del trasferimento transfrontaliero di dati personali deve cessare non appena l'ente abbia garantito il rispetto dei *Principles* e ciò sia stato notificato alle competenti autorità europee[70].

A chiosa delle riflessioni intorno alle conseguenze della violazione degli impegni assunti con l'accettazione dei *Safe Harbour Principles*, è necessario rilevare come, accanto ai profili pubblicistici appena evidenziati, possano ingenerarsi, in capo all'operatore 'infedele', anche conseguenze negative in termini risarcitori. In particolare, le organizzazioni aderenti ai principi di approdo sicuro potrebbero essere destinatarie di richieste di risarcimento danni collegate alla violazione della privacy (*breaches of privacy*), nonché essere ritenute responsabili di *misrepresentation* per non essersi attenute ai principi cui pure avevano dichiarato di conformarsi[71].

[70] La decisione 2000/520/CE, sempre all'art. 3, impone agli Stati membri di comunicare immediatamente alla Commissione l'adozione di misure restrittive alla circolazione di dati personali verso organizzazioni aderenti ai *Safe Harbour Principles* e, in ogni caso, gli Stati membri e la Commissione s'informano vicendevolmente in ordine ai casi in cui l'azione degli organismi di controllo statunitensi non garantisca la conformità ai principi negli Stati Uniti. Nell'ipotesi in cui si accerti che uno degli organismi incaricati di garantire la conformità ai *Principles* negli Stati Uniti non svolge la sua funzione in modo efficace, «*la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione*».

[71] V. R.C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, in 77 *Calif. L. Rev.* 957 (1989). Il *Restatement of the Law, Second, Torts* § 525 prevede espressamente che «*One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it, is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation*». Nell'ambito dei sistema dei *Safe Harbour Principles*, la *relevant representation* si identifica con la dichiarazione pubblica con la quale l'operatore statunitense si impegna a conformarsi ai principi in questione. Con l'assunzione di siffatto impegno, l'inosservanza consapevole dei principi potrebbe originare una richiesta risarcitoria per *misrepresentation* promossa da quanti hanno prestato fede alla falsa dichiarazione. Peraltro, poiché l'impegno ad attenersi ai principi è

Conclusioni: dai Safe Harbour Principles *verso il* Privacy Shield*, passando attraverso* Schrems.

In attesa della definizione del *Privacy Shield* (e della conseguente *adequacy decision* della Commissione), ad oggi, all'esito della pronuncia nel caso *Schrems*, la decisione 2000/520/CE inerente il riconoscimento dell'adeguatezza del livello di tutela garantito dall'ordinamento statunitense ai dati personali importati dall'Unione Europea è stata dichiarata invalida.

In particolare, la Corte di Giustizia, nel ribadire la propria esclusiva competenza in ordine al giudizio circa la validità delle *adequacy decisions* adottate ai sensi dell'art. 25, co. 6, della direttiva 95/46/CE[72], ha riconosciuto tuttavia che le *Data Protection Authorities* nazionali conservano il potere di esaminare le istanze di parte *ex* art. 28, co. 4, della direttiva cit., volte a far valere la non conformità dell'ordinamento terzo ai principi comunitari in materia di riservatezza[73].

Per quanto concerne lo specifico del sistema di trasferimento dei dati personali tra Europa e Stati Uniti introdotto dai *Safe Harbour Principles*, la *Schrems ruling* indica che l'opzione generale per un *self certification scheme* affidato all'adesione volontaristica degli operatori di settore non implica di per sé un giudizio di disvalore in termini di adeguatezza del livello di tutela

assunto nei confronti del pubblico in generale, anche i soggetti interessati e i responsabili del trattamento in Europa che trasferiscono dati personali all'importatore statunitense potrebbero intraprendere un'analoga azione legale nei confronti dello stesso. Cfr. anche P. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in 57 *UCLA L. Rev.* 1701 (2010).

[72] Attualmente, le *adequacy decisions* adottate dalla Commissione hanno interessato Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. L'elenco completo è reperibile al seguente indirizzo *web*: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm/. Va detto, tuttavia, che sebbene la decisione *Schrems* sia limitata al vaglio dei *Safe Harbour Principles*, pressoché tutte le *adequacy decisions* di cui sopra presentano delle criticità analoghe a quella dichiarata invalida.

[73] Su questo specifico profilo, v. la *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, COM(2015) 566 final, del 6 novembre 2015, ove viene ulteriormente specificato che «*the Member States have to provide for the possibility to bring the case before a national court, which in turn can trigger the jurisdiction of the Court of Justice by way of a request for a preliminary ruling pursuant to Article 267 of the Treaty on the Functioning of the European Union (TFEU)*». Il testo completo della *Communication* è reperibile all'URL: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf/.

garantito ai flussi informativi, purché l'ordinamento terzo sia dotato di solidi ed efficaci meccanismi di rilevamento e di controllo che consentano, in concreto, di individuare e sanzionare eventuali violazioni.

Ebbene, proprio la carenza sotto questo specifico profilo dell'*enforcement* (soprattutto rispetto a possibili ingerenze di matrice pubblicistica sui dati), registrata dalla Corte di Giustizia, ha condotto alla dichiarazione dell'invalidità della decisione 2000/520/CE, con l'immediata conseguenza, in termini pratici, del venir meno della possibilità, per gli importatori statunitensi di dati personali, di fondare la legittimità del trasferimento di informazioni sulla sola base dei *Safe Harbour Principles*.

Allo stato, dunque, con il venir meno dell'*adequacy decision*, i trasferimenti di dati personali verso l'ordinamento statunitense sono, in linea di principio, vietati ai sensi dell'art. 25, commi 1 e 4, della direttiva 95/46/CE, con la necessità per gli operatori di ricorrere a strumenti alternativi, in particolare di matrice negoziale (*Standard Contractual Clauses* e *Binding Corporate Rules*)[74], sottoposti al vaglio delle *Data Protection Authorities* nazionali[75].

Ciò non toglie, tuttavia, che il paradigma proposto dalla decisione *Schrems* ai fini della valutazione di adeguatezza di tutela dell'ordinamento terzo, destinatario dei dati personali, porrà, nel prossimo futuro, non pochi problemi rispetto alla possibilità per la Commissione di definire un nuovo accordo quadro con gli Stati Uniti, assimilabile ai *Safe Harbour Principles*.

Difatti, nel momento in cui la formula «*adequate level of protection*» di cui all'art. 25 della direttiva 95/46/CE viene interpretata nel senso di esigere dal Paese terzo una soglia di tutela «*essentially equivalent*» a quella comunitaria, difficilmente un ordinamento giuridico, quale quello statunitense, ove la tutela del *right to privacy* non è circondata da quell'apparato generale di principi 'forti' tipico del diritto europeo, potrà introdurre correttivi tali soddisfare il vaglio di adeguatezza[76].

[74] È questa l'indicazione offerta dalla Comunicazione della Commissione COM (2015) 566 *final*, cit.

[75] Con uno specifico *advisory* pubblicato alla pagina http://www.export.gov/safeharbor/index.asp , lo *U.S. Department of Commerce* ha comunque chiarito che, anche dopo la decisione dell'ottobre 2015 della Corte di Giustizia, «*will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework*». Cfr. G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al Safe Harbor agreement?* e ancora A. Mantelero, *Il trattamento dati nelle imprese nel post Safe Harbour. Strategie di breve, medio e lungo periodo*, infra in questo Volume.

[76] Va detto, ad ogni modo, che la Corte di Giustizia, al par. 73 della *Schrems ruling*,

In tal senso, le garanzie ulteriori che sono alla base dell'annunciato *Privacy Shield*, soprattutto se accompagnate, nell'ambito della cooperazione di polizia e giudiziaria in materia penale, da quanto previsto nell'accordo quadro volto a «rafforzare le garanzie di protezione dei dati nell'ambito della cooperazione fra autorità di contrasto», paiono tese a disegnare un insieme completo e armonizzato di garanzie per la protezione dei dati, che si applicheranno a tutti gli scambi transatlantici di informazioni personali.

In consonanza con quanto sancito dalla Corte di Giustizia, il *Privacy Shield*, diversamente da quanto previsto nel sistema *Safe Harbour*, prende le mosse proprio dalla necessità di uniformare il quadro di garanzie non soltanto nel contesto del settore commerciale ma altresì rispetto agli obblighi relativi all'accesso ai dati personali da parte delle pubbliche autorità, anche per esigenze di sicurezza nazionale.

Questo importante ampliamento della sfera di tutela garantita ai cittadini comunitari costituisce certamente un elemento di innovazione fondamentale nei rapporti tra USA e UE, che prende indubbiamente le mosse dal cuore della pronuncia *Schrems* e da uno dei profili maggiormente deficitari dei *Principles*.

Nella medesima direzione di rispetto delle regole enunciate nella decisione *Schrems* si muovono le ulteriori novità annunciate quali elementi caratterizzanti il *Privacy Shield*: rafforzamento dei meccanismi di vigilanza e *deterrence* a fronte di violazioni degli impegni assunti dalle imprese americane importatrici di dati, identificazione di limiti e garanzie chiare per quanto riguarda l'accesso alle informazioni da parte del governo degli Stati Uniti[77] e, soprattutto, la definizione di differenti mezzi di ricorso individuale, accessibili e di costo sostenibile, per i cittadini europei che ritengano i propri dati oggetto di uso improprio nel quadro del nuovo accordo. Accanto alla possilità di accesso gratuito ad organi di risoluzione alternativa delle controversie ed al ruolo di 'collettori dei reclami' individuali assegnato alle *Data Protection Authorities* nazionali, particolarmente

indica pure che, al fine di soddisfare il canone del livello di tutela adeguato, «*anche se gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione*». Vedi anche J. Reidenberg, *The Simplification of International Data Privacy Rules, in 29 Fordham Int. L.J.* 1128 (2006).

[77] Con istituzione, tra l'altro, di di un difensore civico («*Ombudsperson*»), cui i cittadini europei potranno rivolgersi in caso di uso improprio dei propri dati personali da parte delle Autorità di *intelligence* statunitensi.

interessante, rispetto a questo ultimo specifico profilo, si rivela la creazione di un *Privacy Shield Panel*, cioè un *«dispute resolution mechanism»* con il potere di assumere decisioni vincolanti nei confronti delle imprese americane aderenti all'accordo.

Sulla base di queste garanzie proprie del *Privacy Shield*, innovative rispetto al previgente quadro definito nel contesto dei *Safe Harbour Principles*, la Commissione si appresta ad approvare una nuova *adequacy decision*[78], volta ad attestare, in consonanza con quanto deciso dalla Corte di Giustizia in *Shrems*, che il livello di tutela garantito dal nuovo accordo EU-USA è equivalente agli standard europei di protezione dei dati personali.

Nel complesso, se la lettura degli elementi di innovazione contenuti nel *Privacy Shield* indica senza dubbio come vi sia stato un notevole passo in avanti rispetto alle garanzie in origine previste dai *Safe Harbour Principles*, ciò non toglie come la soluzione identificata sembri dettata più dall'esigenza di superare entro tempi ragionevolmente brevi la situazione di *empasse* conseguente alla sentenza *Shrems* che da una reale valutazione dell'adeguatezza dell'ordinamento statunitense, tanto più nell'ottica della soglia di tutela *«essentially equivalent»* richiesta dalla Corte di Giustizia.

Ed allora, anche alla luce delle prassi applicative che andranno a consolidarsi sul novellato quadro di principi definito dall'accordo e delle modalità di implementazione che dello stesso proporranno le autorità europee e quelle statunitensi, non è peregrino chiedersi quale potrà essere l'esito di un'eventuale futura valutazione del *Privacy Shield* da parte della Corte di Lussemburgo.

[78] Di cui, il 29 febbraio 2016, la Commissione ha rilasciato un primo *draft*, consultabile al *link* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf .

Abstract

As provided by article 25 of Directive 95/46/EC, the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection. In order to facilitate the data flows to United States, while ensuring a high level of protection of personal data, the Commission recognized the adequacy of the Safe Harbour Privacy Principles through the adoption of Decision 2000/520/EC. The paper analyzes the Safe Harbour framework, a set of principles, based on EU directive, issued by the U.S. Department of Commerce to provide adequate protection for the purposes of personal data transfers from the EU. Specifically, the Authors focus on genesis, content and criticalities of the Safe Harbour Principles, as well as the grounds for which the Court of Justice, in its judgment dated 6th October 2015, declared the Decision 2000/520/EC invalid.