La Comunità Internazionale

Vol. LXXI 4 2016

Trimestrale della Società Italiana per l'Organizzazione Internazionale

Interventi

Lorenzo Trapassi, La politica estera brasiliana durante la Guerra fredda (1964-1985), fra aspirazioni globali e dimensione regionale

Articoli e saggi

Christian Ponti, Trasferimenti di materiali di armamento e contrasto al traffico illecito delle armi da fuoco nella legislazione italiana

Osservatorio europeo

Marco Mastracci, Evoluzione del diritto alla *privacy* tra Europa e Stati Uniti: dal *Safe Harbor* al *Privacy Shield*

Note e Commenti

Niccolò Lanzoni, Il Tribunale internazionale del diritto del mare tra sviluppo e frammentazione del diritto internazionale

Francesco Emanuele Celentano, Il sistema sanzionatorio delle Nazioni Unite alla prova della questione Nordcoreana

Rassegne delle attività delle Organizzazioni Internazionali. Documenti. Recensioni

Editoriale Scientifica

OSSERVATORIO EUROPEO

EVOLUZIONE DEL DIRITTO ALLA *PRIVACY* TRA EUROPA E STATI UNITI: DAL *SAFE HARBOR* AL *PRIVACY SHIELD*

MARCO MASTRACCI

SOMMARIO: 1. Introduzione. – 2. Due approcci differenti. – 3. La sentenza *Schrems*. 3.1. Il ragionamento della Corte. – 4. La transizione verso il *Privacy shield*. 4.1. Principi dell'Accordo. 4.2. Gestione e vigilanza dello Scudo. 4.3. Le deroghe al regime per le esigenze di sicurezza nazionale. 4.4. Poteri di vigilanza e di ricorso individuale. 4.5. La decisione della Commissione. 4.6. Riesame periodico dell'Accordo. – 5. Conclusioni.

1. Il concetto di *privacy* è nato negli Stati Uniti alla fine del diciannovesimo secolo, per garantire la protezione dei sentimenti e delle emozioni, come estensione del diritto alla proprietà privata, contro la crescente invadenza della carta stampata[1].

Sviluppatasi in seguito negli altri Paesi, il contenuto di tale diritto si è via via esteso fino a ricomprendere al suo interno la tutela dei dati personali contro l'indebito utilizzo da parte di terzi.

La *privacy* è diventata così (anche) il diritto ad esercitare un controllo sulle informazioni che attengono alla propria sfera personale, consentendo di sapere in ogni momento se qualcuno sta raccogliendo informazioni sul proprio conto e, in caso positivo, di decidere se si vuole consentire tale raccolta di dati.

Internet – e in particolar modo lo sviluppo negli ultimi anni dei social network – ha rivoluzionato il concetto di *privacy*, sottoponendola

[1] Il tema fu affrontato per la prima volta, seppure in modo incidentale, nel 1888 in un trattato sui fatti illeciti dal giudice (Thomas) COOLEY, *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, Chicago, 1888, 29, in cui la *privacy* viene definita come *right to be alone*. Due anni più tardi l'argomento fu approfondito nel saggio *The Right of Privacy*, in *HLR*, 1890, degli avvocati (Samuel) WARREN e (Louis) BRANDEIS. Per una ricostruzione dell'evoluzione del concetto di *privacy* negli Stati Uniti, si vedano BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, e RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 19.

LA COMUNITÀ INTERNAZIONALE FASC. 4/2016 pp. 555-579
EDITORIALE SCIENTIFICA SRL

alla probante sfida di un mondo virtuale in cui le informazioni personali sono divenute di dominio pubblico[2].

I dati personali sono, infatti, diventati la principale moneta di scambio della c.d. economia digitale, in cui gli utenti cedono le proprie informazioni personali in cambio di servizi solo all'apparenza gratuiti.

Il principale modello di *business* in Internet si basa proprio sulla raccolta e lo sfruttamento (ad es. attraverso pubblicità sempre più mirate) di masse di dati personali senza precedenti per quantità, livello di dettaglio, ampiezza socio-economica e geografica[3].

Allo stesso tempo, i governi nazionali hanno cominciato a valorizzare, con finalità di controllo, le potenzialità offerte dall'ingente mole di dati personali immessa nella Rete.

Il fenomeno, come hanno dimostrato incontrovertibilmente le rivelazioni di Edward Snowden nel 2013[4], non è limitato ai regimi autoritari, ma si estende anche alle democrazie occidentali, in particolar modo agli Stati Uniti.

Le attenzioni dei legislatori nazionali e sovranazionali, appuntatesi in precedenza soprattutto sull'esigenza di proteggere gli individui contro l'indebito sfruttamento dei dati personali da parte delle organizzazioni private, si sono concentrate sui programmi di sorveglianza adottati dai singoli stati nazionali.

Alla necessità già avvertita di calibrare il delicato equilibrio tra interesse della collettività ad essere correttamente informata e quello de-

[2] Mark Zuckeberg, fondatore di Facebook, nel 2010 preconizzava la fine della *privacy*, avendo le persone perso ogni interesse riguardo alla propria sfera privata, www.theguardian.com.

[3] Il *New York Times*, commentando i risultati ottenuti da Facebook nel primo trimestre del 2016, ha stimato che il *social network*, in Canada e negli Stati Uniti, ha incassato 11,86 dollari di pubblicità per ciascuno dei suoi utenti, www.nytimes.com. Per fornire un altro dato esemplificativo del valore raggiunto dalle informazioni personali, basti pensare che l'acquisizione del servizio di messaggistica Whatsapp da parte di Facebook è costata 19 miliardi di dollari, che corrispondono a circa 30 euro per ognuno dei 450 milioni di utenti dell'applicazione. Secondo il report pubblicato nel marzo 2014 dal Garante Europeo della protezione dei dati, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, il valore complessivo dei dati personali diffusi su Internet era pari a 300 miliardi di euro, destinato a triplicarsi entro il 2020.

[4] Edward Snowden, ex *contractor* della Cia, ha rivelato pubblicamente alla stampa internazionale, nel giugno del 2013, l'esistenza del più grande programma di sorveglianza di massa delle telecomunicazioni messo a punto dal governo statunitense, il PRISM, fino ad allora tenuto segreto. Si veda, a tal riguardo, l'articolo apparso sul *The Guardian*, GREENWALD, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, 6 giugno 2013, disponibile su www.theguardian.com, nonché l'articolo pubblicato sul *The Washington Post*, *NSA Slides Explain the PRISM Datacollection Program*, 6 giugno 2013, disponibile su www.washingtonpost.com.

gli individui a vedere tutelata la propria *privacy*, si è aggiunta l'esigenza di evitare che i governi nazionali utilizzino gli odierni strumenti tecnologici e l'enorme mole di dati personali che transitano in Rete per esercitare un controllo di massa sull'intera popolazione.

Sotto tale profilo, le rivelazioni in merito al programma di sorveglianza globale adottato dagli Stati Uniti all'indomani dell'11 settembre 2001 hanno inevitabilmente sottoposto all'attenzione delle istituzioni comunitarie il delicato tema relativo al rischio che i dati personali dei cittadini dell'Unione Europea fossero oggetto di indiscriminato utilizzo da parte del governo americano.

Tali considerazioni hanno condotto la Commissione Europea ad avviare i negoziati per la modifica dell'Accordo, denominato *Safe Harbor* (Approdo sicuro) che, dal 2000, regolamentava il trasferimento da parte delle imprese statunitensi dei dati personali dei cittadini comunitari dall'Europa agli Stati Uniti.

Ad imprimere un'evidente accelerata ai negoziati è stata la Corte di Giustizia Europea che, con la sentenza *Schrems* (causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*), intervenuta in data 6 ottobre 2015, ha dichiarato l'invalidità dell'Accordo *Safe Harbor*.

Il 2 febbraio 2016 la Commissione Europea e il Governo degli Stati Uniti d'America hanno raggiunto l'accordo su un nuovo regime per gli scambi transatlantici di dati personali a fini commerciali: lo Scudo UE-USA per la *privacy* (o *Privacy Shield*).

Appare utile, nell'ottica di una migliore comprensione dei tratti caratteristici dello Scudo, ricostruire il processo che ha condotto alla sottoscrizione del nuovo Accordo.

2. Unione Europea e Stati Uniti d'America scontano tradizionalmente un approccio profondamente differente in merito al regime di tutela del trattamento dei dati personali[5].

Secondo la normativa di stampo europeo, il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo, ricavabile, in via interpretativa, dall'art. 8 della Convenzione Europea dei Diritti dell'Uomo, in ragione del quale ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

Il merito della consacrazione formale del diritto alla protezione dei dati personali, all'interno dei principi fondamentali del diritto comuni-

[5] Sulle diversità di approccio alla materia da parte dei due continenti, si veda BENNET, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, 1992, e WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in *Yale LJ*, 2004, 1151 ss.

tario, va alla Carta dei diritti fondamentali dell'Unione Europea[6], adottata nel 2000, nella quale trova tutela non solo il più generico diritto al rispetto della vita privata, ma anche il più specifico diritto alla protezione dei dati personali.

A livello più di dettaglio, già la direttiva comunitaria 95/46/CE, si era preoccupata di rendere operativo tale principio, prescrivendo una serie dettagliata di regole e criteri ai quali informare la raccolta e l'utilizzo dei dati personali[7]. La direttiva non si limita a tutelare i dati personali dei cittadini europei all'interno dei confini comunitari, ma, consapevole della facilità con cui questi, in ragione della loro immaterialità, possono essere trasferiti al di fuori dei detti confini, consentendo in tal modo una facile elusione della protezione garantita dalla direttiva, prescrive (art. 25, co. 6) che il «trasferimento verso un Paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il Paese terzo di cui trattasi garantisce un livello di protezione adeguato».

In sostanza, pur affermando la legittimità del trasferimento di dati fuori dal territorio comunitario, la direttiva subordina tale possibilità al fatto che il Paese terzo verso il quale sono trasferiti garantisca un livello di protezione sostanzialmente coincidente con quello offerto dall'*acquis communautaire*.

Al contrario, la disciplina statunitense in tema di tutela dei dati personali presenta senza dubbio un quadro normativo più frammentato. A livello costituzionale, la *privacy* – e indirettamente i dati personali – trovano protezione nel Quarto emendamento alla Costituzione[8], che sancisce il diritto di ogni cittadino a non veder violata la propria persona e il proprio domicilio, attraverso perquisizioni o sequestri, se non vi siano

[6] La Carta è diventata giuridicamente vincolante nell'UE con l'entrata in vigore del Trattato di Lisbona, a dicembre 2009, ed ora ha lo stesso valore giuridico dei Trattati dell'Unione. Per un commento della Carta, si veda BARBERA, *La Carta europea dei diritti e la costituzione italiana,* in *Le libertà e i diritti nella prospettiva europea: studi in memoria di Paolo Barile*, Padova, 2002, 108 ss., e AA.VV., *Carta dei diritti fondamentali dell'Unione europea*, in POCAR, BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, 2ª ed., Padova, 2014, 1651 ss.

[7] Come noto, la direttiva 95/46/CE è stata sostituita dal regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che si applicherà a decorrere dal 25 maggio 2018. In dottrina, si veda sulla direttiva 95/46/CE DASSI, *La direttiva del 24 ottobre 1995 sulla protezione dei dati e la direttiva 96/9/CE dell'11 marzo 1996 sulle banche dati*, in *Resp. civ. prev.*, 1997, 600 ss.; si v., anche, DELFINO, *La direttiva comunitaria 46/95 "Sulla protezione dei dati personali e sulla libera circolazione di tali dati"*, in *Contr. imp./Europa*, 1996, 888.

[8] ATKINSON, *The Fourth Amendment's National Security Exception: Its History and Limits*, in *Vanderbilt L. Rev.*, 2013, 1343, 1381.

probabili motivi che tale attività possa contribuire a ottenere prove relative alla commissione di un reato[9].

L'ombrello di protezione offerto dal Quarto emendamento soffre, tuttavia, di numerose limitazioni, che ne condizionano fortemente l'estensione. *In primis*, le garanzie in esso contenute operano esclusivamente a favore della popolazione americana, non estendendosi alla tutela dei cittadini stranieri. Inoltre, l'ambito di tutela del disposto costituzionale è ulteriormente limitato dall'applicazione del principio della c.d. *third party doctrine*, in forza del quale gli individui non possono vantare una legittima aspettativa di *privacy* riguardo alle informazioni che essi stessi trasferiscono a terzi in maniera volontaria[10]. Ciò implica che, una volta prestato il consenso all'utilizzo dei propri dati personali a favore (ad esempio) del fornitore del servizio di telefonia, non si possa lamentare che tali dati siano poi trasferiti – anche a propria insaputa – a soggetti terzi.

A ciò si aggiunga che il diritto alla *privacy* è tutelato da una normativa federale, settoriale e frammentaria, composta da una serie di leggi non armonizzate tra loro – l'*US Privacy Act* del 1974, che si applica unicamente ai cittadini americani e agli stranieri ammessi con lo *status* di residente permanente, il *Freedom of Information Act* (FOIA), l'*E-Government Act* del 2002 – che non garantiscono una omogenea protezione della sfera privata degli individui.

Anche questa scarna disamina del regime di tutela della *privacy* operante nei due continenti evidenzia una difformità di approccio difficilmente conciliabile, se non in considerazione di opportunità politiche legate alla necessità di non ostacolare i traffici commerciali tra Europa e Stati Uniti.

Fino alle rivelazioni di Snowden nel 2013, il potenziale conflitto tra i due assetti regolatori[11] era contenuto dall'adozione di una serie di regole generali che consentivano al singolo esportatore di dati personali dall'Europa verso gli Stati Uniti di superare la soglia di adeguatezza di tutela imposta dalla direttiva 95/46/CE.

[9] La Corte Suprema degli Stati Uniti d'America ha fornito nel corso degli anni un'interpretazione evolutiva della disposizione in esame. Mentre, nel caso *Olmstead v. United States*, *277 U.S. 438*, del 1928, l'applicabilità del Quarto Emendamento è stata limitata alle sole intrusioni fisiche, nel caso *Katz v. United States*, *389 U.S. 347*, del 1967 il campo applicativo di tale disposizione è stato esteso alle intercettazioni telefoniche e ai metodi di sorveglianza elettronica, sulla base del rilievo che la stessa è intesa a proteggere «people not places».

[10] Sulla *third party doctrine*, si veda KERR, *The Case for the Third-Party Doctrine*, in *Michigan LR*, 2009, 561.

[11] Sul tema si veda BIGNAMI, RESTA, *Transatlantic Privacy Regulation: Conflict and Cooperation*, in *LCP*, 2015, 101.

Tali principi, contenuti nell'Accordo denominato Approdo Sicuro (*Safe Harbor*)[12] –, sostanzialmente riconducibili ai criteri cui è informato il trattamento dei dati personali secondo la direttiva 95/46 e ravvisabili nei principi di notifica, scelta, sicurezza, integrità dei dati, accesso e garanzia d'applicazione – vennero poi cristallizzati con la decisione della Commissione Europea 2000/520/CE, creando così una presunzione di adeguatezza di tutela in favore di quelle organizzazioni statunitensi che si fossero impegnate al rispetto degli stessi.

Tale Accordo, stipulato prima degli eventi tragici dell'11 settembre 2001, rispecchiava l'approccio dell'epoca, nel quale le preoccupazioni principali delle istituzioni comunitarie, relative all'utilizzo indebito dei dati personali dei cittadini europei, si concentravano prevalentemente sulle organizzazioni private.

Ciò era evidente nel testo della stessa decisione, nel quale la Commissione si concentrava sulla normativa civilistica statunitense in materia di trattamento dei dati personali e dei rimedi risarcitori approntati a favore del singolo, senza fare alcun riferimento alle deroghe ai principi di tutela dei dati personali concesse a favore dell'amministrazione pubblica e delle sue autorità di *intelligence*.

Come noto, a seguito dell'attacco alle Torri Gemelle, gli Stati Uniti adottarono una serie di provvedimenti che restrinsero profondamente le libertà dei cittadini, al fine di garantire un maggior controllo da parte del governo.

In particolare, attraverso il *Patriot Act* del 26 ottobre 2001[13], che ha modificato il Titolo V del *Foreign Intelligence Surveillance Act* del 1978 (FISA), sono state adottate alcune misure volte ad ampliare notevolmente i poteri di indagine delle autorità di *intelligence* nella lotta al terrorismo, autorizzando le stesse ad avere libero accesso a varie banche dati pubbliche e private, con evidente compressione della sfera privata dei cittadini americani.

I documenti diffusi da Snowden – che hanno svelato i lineamenti essenziali dei programmi di sorveglianza di massa posti in essere dalle agenzie di *intelligence* statunitensi – hanno evidenziato limpidamente

[12] Il sistema dei *Safe Harbor Principles* si componeva di 7 principi generali e 15 *frequently asked questions* (FAQs), che imponevano all'importatore americano dei dati personali provenienti dall'UE gli obblighi essenziali che la direttiva 94/46/CE prescrive in capo ai titolari di trattamento comunitari, con una sostanziale esportazione del modello europeo di disciplina del diritto alla riservatezza. Il meccanismo dei *Safe Harbor Principles* era basato su un sistema di autocertificazione che consentiva all'impresa statunitense di procedere all'importazione di dati personali dall'Unione Europea, autocertificando al Department of Commerce l'adesione ai principi del *Safe Harbor*.

[13] 50 USC 1861 – *Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations.*

come gli interventi normativi, succedutisi a seguito degli attacchi terroristici dell'11 settembre 2001, avessero ampliato, oltre il limite legittimo, i poteri di indagine delle agenzie di *intelligence* statunitensi.

Ci si è accorti che il sistema approntato dal *Safe Harbor* rappresentava il volano attraverso il quale le autorità pubbliche americane potevano acquisire in blocco i dati legittimamente trasferiti in territorio statunitense, conformemente alle procedure di *Safe Harbor*.

Più precisamente, come ben evidenziato dalla Commissione Europea nella sua comunicazione COM(2013)847 def., dal momento che «tutte le imprese partecipanti al programma PRISM [programma di raccolta di informazioni su larga scala], che consente alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultano certificate nel quadro di Approdo sicuro», tale sistema «è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'[Unione]».

Il divario tra le tutele previste dall'ordinamento comunitario e la pervasiva ingerenza delle autorità governative degli Stati Uniti nella sfera privata delle persone aveva superato il punto di equilibrio, garantito fino a quel momento dall'Accordo di Approdo Sicuro.

Il mutato contesto, rispetto al tempo di stipula di questo Accordo, rappresenta il substrato giuridico e fattuale nel quale sono maturate dapprima le comunicazioni COM(2013)846 e 847, con cui la Commissione sollecitava una sua revisione, e successivamente la pronuncia della Corte di Giustizia Europea (causa C-362/14, *Schrems*) che ha dichiarato invalida la ricordata decisione 2000/520/CE, che aveva dichiarato la conformità dei principi del *Safe Harbor* agli *standard* comunitari.

3. La decisione della Corte di Giustizia nel caso *Schrems* sviluppa il filone giurisprudenziale inaugurato dalla Corte con la sentenza *Digital Rights*[14] dell'8 aprile 2014, con cui ha dichiarato l'invalidità della direttiva 2006/24/CE, riguardante la conservazione dei dati personali da parte degli operatori di telecomunicazione.

Le motivazioni della sentenza *Digital Rights* affondano le loro radici nell'eccessiva compressione del diritto alla riservatezza e alla tutela dei dati personali, in considerazione dell'assenza di limiti nella fase della raccolta dei dati e di idonee garanzie in merito al loro utilizzo da parte dei terzi, nonché dell'eccessiva durata (da sei mesi a due anni) del periodo di conservazione degli stessi.

[14] Per un commento a tale pronuncia, si veda: IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *ELR*, 2014, 835.

Analoghi profili di illegittimità sono rivenuti dalla Corte nel sistema di Approdo Sicuro, in considerazione dei vasti poteri di indagine concessi alle autorità di *intelligence* USA – rispetto ai dati provenienti dalla UE – dalla clausola dell'Accordo che consentiva di derogare ai principi ivi contenuti per ragioni di sicurezza nazionale.

La vicenda giudiziaria ha origine dal ricorso presentato dal cittadino austriaco, Maximillian Schrems, innanzi all'Autorità per la protezione dei dati personali irlandese, con il quale, a seguito delle rivelazioni di Snowden, chiedeva di vietare il trasferimento dei propri dati personali dalla consociata irlandese del *social network* Facebook – cui egli era iscritto – agli Stati Uniti, stante l'inadeguatezza dell'ordinamento statunitense ad impedire il controllo indiscriminato sui dati personali da parte dell'*intelligence* americana.

L'Autorità respingeva il ricorso, sia per mancanza di prove in merito alla circostanza asserita dal ricorrente che i suoi dati personali fossero stati oggetto di accesso da parte delle autorità pubbliche statunitensi, sia perché l'adeguatezza del trasferimento dei dati verso gli Stati Uniti era stata già determinata sulla base della decisione2000/520/CE della Commissione.

Schrems proponeva di conseguenza ricorso alla Corte di Appello irlandese, la quale, rilevava come un effettivo accesso massiccio ed indifferenziato ai dati personali sarebbe stato «manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese» e come la decisione 2000/520/CE non fosse più adeguata al soddisfacimento dei requisiti previsti dagli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea.

Rimetteva, pertanto, la questione alla Corte di Giustizia, chiedendo a questa di valutare se una decisione adottata in forza dell'art. 25 della direttiva 95/46/CE – come appunto la decisione della Commissione sul *Safe Harbor* – possa precludere ad un'autorità nazionale di controllo di pronunciarsi su un ricorso concernente l'inadeguatezza del livello di protezione assicurato da un Paese terzo e di bloccare il trasferimento dei dati verso tale Paese.

3.1. La Corte, come vedremo di seguito, ha trasceso i confini della questione sottopostale dalla Corte di appello irlandese, arrivando a dichiarare l'invalidità totale della decisione 2000/520/CE. Il ragionamento della Corte parte dalla considerazione preliminare secondo cui l'esistenza di una decisione della Commissione Europea – che dichiari l'adeguatezza del livello di protezione dei dati personali offerto da un Paese terzo – non preclude la possibilità per le autorità nazionali di esercitare i poteri di

controllo previsti dalla Carta dei diritti fondamentali e dalla direttiva 95/46/CE.

Pertanto, anche qualora la Commissione abbia adottato una decisione di adeguatezza ai sensi dell'art. 25 della direttiva, le autorità nazionali, investite di un ricorso, devono poter esaminare in piena indipendenza se il trasferimento di dati personali verso un Paese terzo rispetti i requisiti sanciti dalla direttiva. Tali poteri tuttavia non si estendono fino alla possibilità di dichiarare invalida una decisione della Commissione, essendo riservata tale facoltà esclusivamente alla Corte di Giustizia, a cui dovranno rivolgersi in via pregiudiziale i giudici nazionali qualora nutrano dubbi sulla validità di una decisione della Commissione.

Passando poi ad analizzare la validità della decisione della Commissione europea sul *Safe Harbor*, la Corte ricorda che la Commissione avrebbe dovuto verificare l'adeguatezza del livello di protezione offerto dal Paese terzo, nel caso specifico gli Stati Uniti. Tale parametro, precisa la Corte, deve ravvisarsi in un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46/CE.

In particolar modo, la Commissione avrebbe dovuto valutare il contenuto delle norme applicabili in tale Paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, la prassi intesa ad assicurare il rispetto di tali norme, nonché verificare periodicamente, attraverso una valutazione in fatto e diritto, che l'adeguatezza del livello di protezione assicurato dal Paese terzo permanesse nel tempo.

Al contrario, la Commissione si è limitata a valutare l'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi dell'Approdo Sicuro, senza tuttavia soffermarsi sul livello di protezione complessivo offerto dalla legislazione nazionale americana. Tale mancata valutazione ha assunto un rilievo particolare nel determinare il giudizio di invalidità da parte della Corte, in ragione della possibilità prevista dall'allegato I della decisione 2000/520/CE, che consentiva di limitare l'applicabilità dei principi del *Safe Harbor* per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia da parte di disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti.

In tal modo, la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti» sui principi dell'Approdo sicuro, in forza del quale le imprese americane che ricevono dati personali dall'Unione sono tenute a disapplicare tali principi nel momento in cui questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

Peraltro, continua la Corte, non esiste nel sistema di *Safe Harbor* un meccanismo di tutela nei confronti delle ingerenze da parte delle autorità pubbliche americane, in quanto i rimedi previsti (arbitrato privato e procedimenti dinanzi alla Commissione federale per il commercio) sono limitati alle controversie in materia commerciale, scaturenti dal mancato rispetto, da parte delle imprese americane, dei principi dell'Approdo Sicuro, e non sono applicabili nell'ambito delle controversie concernenti la legittimità dell'azione delle agenzie di *intelligence*.

Tali considerazioni hanno costituito la base del ragionamento, che ha condotto la Corte a dichiarare l'invalidità della decisione 2000/520/CE e, di conseguenza, del regime di Approdo Sicuro.

4. L'esigenza di rivedere i termini di questo Accordo era già stata manifestata dalla Commissione nella citata comunicazione del 27 novembre 2013, in considerazione di una serie di elementi – quali l'aumento esponenziale dei flussi di dati, la rapida crescita del numero di imprese statunitensi aderenti al regime dell'Approdo Sicuro e le informazioni disponibili sull'estensione dei programmi di *intelligence* statunitensi – che sollevavano forti dubbi circa il livello di tutela che il regime era in grado di garantire.

Sulla base delle informazioni emerse dai lavori del gruppo di contatto UE-Stati Uniti sulla vita privata[15] e di quello sui programmi di *intelligence* statunitensi[16], la Commissione ha formulato 13 raccomandazioni per una revisione del regime dell'Approdo Sicuro. Esse sollecitavano il rafforzamento dei principi sostanziali in materia di *privacy*, attraverso una maggiore trasparenza delle politiche di *privacy* da parte delle imprese statunitensi aderenti al regime, un'azione più incisiva delle autorità statunitensi in termini di verifica, vigilanza e controllo dell'osservanza di tali principi, la presenza di meccanismi di risoluzione delle controversie a costo accessibile e la necessità di limitare allo stretto necessario il ricorso all'eccezione per motivi di sicurezza nazionale.

Nel 2014 la Commissione ha avviato un dialogo con le autorità statunitensi al fine di discutere di un rafforzamento del regime dell'Approdo Sicuro, in linea con le 13 raccomandazioni formulate nella sua comunicazione. Come anticipato, i colloqui hanno subito una notevole accelerazione a seguito della sentenza *Schrems*, finalizzati ad adottare

[15] Consiglio dell'Unione europea, *Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, documento 9831/08 del 28 maggio 2008, consultabile all'indirizzo: www.europarl.europa.eu.

[16] *Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection*, del 27 novembre 2013. consultabile all'indirizzo: ec.europa.eu.

una nuova decisione sull'adeguatezza rispondente ai requisiti dell'art. 25 della direttiva 95/46/CE.

La Commissione ha presentato il progetto di testo della decisione il 29 febbraio 2016. A seguito del parere del Gruppo di lavoro *ex* art. 29[17] e della risoluzione del Parlamento europeo del 26 maggio, la Commissione, il 12 luglio 2016, ha completato la procedura di adozione del nuovo Accordo, denominato Scudo UE-USA per la *privacy*.

Analizziamo, di seguito – attraverso la lettura della decisione di esecuzione 2016/1250, con cui la Commissione ha dichiarato l'adeguatezza del livello di protezione dei dati personali trasferiti dall'Unione Europea agli Stati Uniti d'America in base allo Scudo – i tratti salienti della nuova intesa.

4.1. In linea di continuità con il precedente Accordo di Approdo Sicuro, il *Privacy Shield* non ha modificato il sistema di accreditamento delle aziende che intendono aderirvi, mantenendo il precedente regime di autocertificazione – non censurato dalla sentenza *Schrems* – in base al quale l'organizzazione statunitense potrà aderire allo Scudo, impegnandosi a rispettare l'insieme di principi costituenti il nuovo regime.

I profili di continuità non si esauriscono nel sistema di accreditamento, dal momento che i principi del *Privacy Shield* presentano altresì notevoli somiglianze rispetto ai criteri che informavano il precedente regime dell'Approdo Sicuro.

Del resto, i profili di criticità che hanno determinato la decisione di invalidare il regime di *Safe Harbor* non concernevano il contenuto dei principi, quanto la facilità con cui questi potevano essere elusi dalle organizzazioni aderenti al regime, nonché dalle autorità di *intelligence* americane.

Nel dettaglio, l'organizzazione che vuole aderire allo Scudo deve rispettare i seguenti principi:

1. principio dell'informativa, in base al quale è tenuta a informare l'interessato di una serie di informazioni circa le modalità con cui avverrà il trattamento dei suoi dati personali (ad esempio, tipo di dati raccolti,

[17] Il Gruppo per la tutela della persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 della direttiva 95/46/CE, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Tra i suoi compiti più rilevanti, vi è quello previsto dall'art. 30, lett. *c*) della direttiva di «consigliare la Commissione in merito a ogni progetto di modifica della presente direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà».

finalità del trattamento, diritto di accesso e di scelta, condizioni applicabili all'ulteriore trasferimento, responsabilità);

2. principio dell'integrità dei dati e della limitazione della finalità, secondo il quale deve raccogliere e utilizzare i dati esclusivamente per le finalità evidenziate nell'informativa trasmessa all'interessato, avendo cura di conservarne l'integrità;

3. principio della sicurezza, per il quale deve adottare misure di sicurezza "ragionevoli e adeguate", tenuto conto dei rischi insiti nel trattamento dei dati e nella loro natura;

4. principio dell'accesso, che attribuisce all'interessato il diritto di sapere dall'organizzazione se questa tratti dati personali che lo riguardano;

5. principio del ricorso, controllo e responsabilità, in forza del quale l'organizzazione aderente allo Scudo deve mettere a disposizione meccanismi solidi volti a garantire il rispetto dei principi e la possibilità di ricorso per l'interessato dell'UE, i cui dati personali siano stati trattati in modo non conforme;

6. principio della responsabilità in caso di ulteriore trasferimento a soggetti terzi, che può avvenire solo per finalità determinate e limitate, in base a un contratto che preveda lo stesso livello di protezione garantito dai principi, compresa la condizione che permette di limitare l'applicazione dei principi soltanto per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico.

Vi è tuttavia da rilevare che, sebbene il complesso dei principi dello Scudo ricalchi sostanzialmente il novero delle regole previste dalla direttiva 95/46/CE, in ottica futura problemi di compatibilità potrebbero sorgere dalla mancanza nel *Privacy Shield* dei principi previsti dal nuovo regolamento per la protezione dei dati personali.

Il regolamento introduce, infatti, una serie di principi innovativi, che ampliano l'ambito di protezione accordato dalla direttiva 95/46/CE, con lo scopo di garantire una tutela effettiva – e non più meramente formale – ai dati personali.

A tal fine, esso riconosce espressamente il diritto all'oblio, ovvero la possibilità per l'interessato, a determinate condizioni, di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali; stabilisce il diritto alla portabilità dei dati, in virtù del quale l'interessato ha il diritto di trasferire i dati personali da un titolare ad un altro, a condizione che il trattamento si basi sul consenso o su un contratto e che non vengano lesi diritti e libertà altrui; sancisce il principio di *accountability*, per cui il titolare dovrà dimostrare l'adozione di politiche *privacy* e misure adeguate in conformità al regolamento; introduce il principio della *privacy by design*, dal quale discende l'attuazione di

adeguate misure tecniche e organizzative, sia all'atto della progettazione che dell'esecuzione del trattamento.

La mancata inclusione di tali principi – al momento in cui il regolamento troverà piena attuazione nel maggio 2018 – determinerà inevitabilmente il venir meno del requisito di sostanziale equivalenza tra il livello di protezione garantito dall'Unione Europea e il quadro giuridico di tutele approntato dagli Stati Uniti.

4.2. Lo Scudo prevede meccanismi di vigilanza e di controllo sull'attuazione dell'Accordo, tesi a verificare che le imprese autocertificatesi come aderenti al regime rispettino i principi e a provvedere in caso di mancata osservanza degli stessi.

L'autorità preposta a vigilare sul corretto adempimento dell'Accordo da parte delle organizzazioni aderenti allo Scudo è il Dipartimento del Commercio degli Stati Uniti, con l'assistenza della Commissione Federale del Commercio (*Federal Trade Commission*) e del Dipartimento dei Trasporti[18]. A tal fine il Dipartimento del Commercio: predispone un elenco delle organizzazioni che si sono autocertificate come aderenti allo Scudo, consultabile su internet; verifica periodicamente l'effettivo assolvimento degli obblighi assunti dalle imprese aderenti allo Scudo, depennando dall'elenco le organizzazioni che abbiano ripetutamente violato le prescrizioni dell'Accordo; controlla le organizzazioni che, essendosi ritirate volontariamente o non avendo rinnovato la certificazione, non sono più membri dello Scudo, per verificare se intendano restituire, cancellare o conservare i dati personali ricevuti nell'ambito del regime; controlla i casi di millantata adesione allo Scudo e di uso improprio del relativo marchio di certificazione.

Lo Scudo offre diversi meccanismi di reclamo al soggetto privato che ritenga di aver subito un danno ad esito della violazione dell'Accordo da parte di un'organizzazione aderente al regime.

In primis, ogni azienda aderente allo Scudo è obbligata ad approntare un meccanismo di risoluzione interna dei reclami, che assicuri una tutela effettiva alle ragioni del ricorrente.

L'interessato può sporgere reclamo direttamente all'organizzazione – che a tal fine è obbligata ad approntare un meccanismo di risoluzione interna dei reclami, che assicuri una tutela effettiva alle ragioni del ricorrente –, a un organo indipendente di risoluzione delle controversie da questa designato, all'autorità nazionale di protezione dei dati oppure alla *Federal Trade Commission*.

[18] Gli impegni della Commissione Federale del Commercio e del Dipartimento dei Trasporti sono contenuti, rispettivamente, nell'Allegato IV e V del *Privacy Shield*.

In ultima istanza, dopo avere esaurito tutti i mezzi di ricorso anzidetti, il soggetto leso ha il diritto di chiedere un arbitrato vincolante ad un collegio arbitrale, costituito da arbitri scelti all'interno di un elenco di almeno 20 arbitri predisposto dal Dipartimento del Commercio e dalla Commissione Europea sulla base dell'indipendenza, dell'integrità e delle competenze in materia di diritto della *privacy* statunitense e di normativa dell'UE sulla protezione dei dati.

Ad eccezione del collegio arbitrale, cui potrà rivolgersi solo dopo aver esperito i mezzi di contestazione suddetti, l'interessato è libero di scegliere il meccanismo di ricorso che preferisce, senza alcun obbligo di rivolgersi a uno piuttosto che a un altro o di seguire una determinata sequenza.

4.3. Le preoccupazioni delle istituzioni UE concernenti gli eccessivi poteri investigativi delle autorità di *intelligence* americane si riflettono sul testo del nuovo Accordo, che contiene una descrizione puntuale delle principali disposizioni legislative che consentono alle autorità governative l'accesso alle informazioni personali dei cittadini statunitensi e stranieri.

Tale maggiore trasparenza riguardo il funzionamento del meccanismo di sorveglianza adottato *dall'intelligence* USA potrà consentire alle istituzioni comunitarie un maggiore controllo sui potenziali abusi nei confronti dei dati personali provenienti dall'Europa.

Resta ferma, comunque, la clausola di salvaguardia a favore delle autorità di *intelligence*, già affermata nel regime del *Safe Harbor*, per il quale il rispetto dei principi fissati nel *Privacy Shield* «trova il suo limite se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia».

Il mantenimento di tale principio espone i dati personali dei cittadini comunitari agli ampi poteri di indagine che la legislazione statunitense accorda alle agenzie governative, oltre ad aprire la porta ad eventuali mutamenti *in peius* della disciplina in materia, suscettibili di ripercuotersi, attraverso la clausola anzidetta, sulla libertà dei cittadini comunitari.

Ciò nonostante, la Commissione ha ritenuto che il quadro normativo statunitense, in ragione delle modifiche intervenute negli ultimi anni, fornisca garanzie sufficienti in merito alle limitazioni all'accesso e all'uso dei dati personali da parte delle autorità pubbliche statunitensi.

Precisando i contorni di tale giudizio, la Commissione ha esaminato i due strumenti giuridici centrali attraverso il quale il Presidente, nella sua qualità di capo del governo, attua tale principio: il decreto presidenziale

12333 (*Executive Order* 12333[19]) e la direttiva presidenziale 28 (PPD-28).

Soffermandosi in particolare su quest'ultima, la Commissione segnala il grosso passo avanti – nell'ambito delle disposizioni legislative suscettibili di limitare l'accesso indiscriminato da parte delle autorità pubbliche – determinato dall'approvazione di tale provvedimento.

La direttiva presidenziale 28, emanata il 17 gennaio 2014 dal Presidente Obama, stabilisce, infatti, una serie di principi generali, che disciplinano la raccolta dati nell'ambito dell'*intelligence* dei segnali[20] e ne limitano l'utilizzo indiscriminato.

Sotto il profilo soggettivo, la direttiva assicura equità di trattamento tra cittadini americani e stranieri, prevedendo per questi ultimi che le attività di *intelligence* rispettino, relativamente alla conservazione e divulgazione delle informazioni personali rilevate nell'ambito dell'*intelligence* dei segnali, i limiti fissati espressamente per i cittadini statunitensi o residenti negli USA.

Inoltre, stabilisce il principio secondo il quale la raccolta dati deve essere autorizzata per legge o per disposizione presidenziale, nel rispetto della Costituzione e della legge.

La raccolta deve altresì avvenire esclusivamente per finalità di *intelligence* esterna o di controspionaggio e deve essere sempre condotta in modo mirato, evitando, quando possibile, la raccolta in blocco.

Anche in tale ultimo caso, la PPD-28 limita l'uso delle informazioni così rilevate a sei finalità di sicurezza nazionale[21], al fine di tutelare la vita privata e le libertà civili di chiunque, a prescindere dalla cittadinanza e dal luogo in cui la persona vive.

I dati raccolti in violazione delle citate prescrizioni non possono essere conservati per oltre cinque anni, a meno che il Direttore dell'*intelligence* nazionale stabilisca espressamente che il prolungamento della

---

[19] *EO 12333: United States Intelligence Activities*, Registro federale, vol. 40, n. 235 (8 dicembre 1981). Il decreto definisce le finalità, gli indirizzi, i compiti e le responsabilità delle attività d'*intelligence* degli USA (compreso il ruolo dei diversi servizi della comunità dell'*intelligence*) e fissa i parametri generali per la condotta di tali attività (in particolare la necessità di adottare regole procedurali specifiche).

[20] Per *intelligence* dei segnali o SIGINT, abbreviazione delle parole inglesi *SIGnals INTelligence*, si intende l'attività di raccolta di informazioni mediante l'intercettazione e analisi di segnali, sia emessi tra persone sia tra macchine, oppure una combinazione delle due. Secondo la National Security Agency statunitense «SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems», www.nsa.gov.

[21] Le finalità di sicurezza ricomprendono le misure finalizzate ad individuare e contrastare le minacce derivanti da attività di spionaggio, terrorismo, armi di distruzione di massa, le minacce alla sicurezza informatica, le minacce alle forze armate o al personale militare e le minacce criminali transnazionali inerenti alle altre cinque finalità.

conservazione è nell'interesse della sicurezza nazionale degli Stati Uniti d'America.

Ad esito di tale analisi, la Commissione, nel considerando n. 76 della decisione, giunge alla conclusione che, sebbene non formulati nei medesimi termini giuridici, nell'essenza detti principi rispecchiano i principi di necessità e di proporzionalità.

Passando poi ad analizzare i singoli istituti giuridici che autorizzano le autorità pubbliche ad accedere e raccogliere i dati personali dei cittadini europei, una volta che questi siano trasferiti negli Stati Uniti, la Commissione evidenzia che gli enti statunitensi di *intelligence* possono ottenerli soltanto se la richiesta è conforme alla FISA o se è presentata dal Federal Bureau of Investigation (FBI) in base a una *National Security Letter* (NSL[22]).

La FISA, in particolare, è lo strumento giuridico attraverso il quale le autorità americane possono avere accesso a tali dati: oltre all'art. 104, che contempla la sorveglianza elettronica tradizionale personalizzata, e all'art. 402, relativo all'installazione di dispositivi di intercettazione dei dati informativi della comunicazione in entrata e in uscita, i due strumenti centrali sono l'art. 501 (ex art. 215 della legge *U.s. Patriot*) e l'art. 702.

Sul punto, la Commissione rileva come l'introduzione della legge *USA Freedom*, adottata il 2 giugno 2015, vieti la raccolta in blocco di dati in base all'art. 402 della FISA (potere di intercettazione dei dati informativi della comunicazione in entrata e in uscita) e all'art. 501 della FISA e mediante le National Security Letter, imponendo invece l'impiego di selettori specifici.

Anche i programmi di sorveglianza denominati PRISM e Upstream, autorizzati ai sensi dell'art. 702 della FISA[23] e la cui esistenza, rivelata nel giugno 2013 da Edward Snowden, aveva destato sconcerto tra le istituzioni comunitarie, passano il vaglio della Commissione alla luce delle modifiche legislative intervenute *medio tempore*, che ne hanno

[22] Attraverso le *National Security Letters*, il Federal Bureau of Service può richiedere a un fornitore di servizi di telecomunicazione la trasmissione dei dati riguardanti le comunicazioni di una persona, senza la preventiva autorizzazione da parte di un'autorità giurisdizionale. Sull'abuso dell'FBI di tale strumento di indagine, si veda l'articolo pubblicato il 14 marzo 2008 dal *Washington Post*, *FBI Found to Misuse Security Letters*, disponibile all'indirizzo: www.washingtonpost.com.

[23] L'art. 702 della FISA permette ai servizi di *intelligence* statunitense di chiedere l'accesso a informazioni, compresi i contenuti delle comunicazioni via Internet, che, seppur raccolte all'interno degli USA, riguardano determinati cittadini stranieri che si trovano al di fuori degli Stati Uniti. Per un'analisi dettagliata del suo funzionamento si veda il rapporto dell'Autorità per la tutela della vita privata e delle libertà civili, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 luglio 2014, consultabile all'indirizzo www.pclob.gov.

limitato fortemente – almeno secondo il giudizio della Commissione – la pervasività.

La raccolta di dati effettuata in base a tale strumento trova adesso una notevole limitazione in base ai principi fissati nella disposizione presidenziale PPD-28: la ricerca è resa mirata mediante l'impiego di singoli selettori che identificano dispositivi di comunicazione specifici, come l'indirizzo di posta elettronica o il numero di telefono dell'obiettivo, ma non parole chiave e neppure il nome degli obiettivi.

I dati raccolti, inoltre sono soggetti ad un limite temporale di archiviazione che, in linea di principio, è fissato in cinque anni, salvo la conservazione per un periodo più lungo sia ritenuta nell'interesse della sicurezza nazionale in virtù di una disposizione di legge o di una decisione del Direttore dell'*intelligence* nazionale.

Alla luce delle considerazioni relative al sistema complessivo di tutele approntate in merito alle modalità di raccolta e conservazione dei dati personali da parte delle autorità di *intelligence* americane, la Commissione giunge alla conclusione che negli Stati Uniti vigono regole intese a limitare, alla misura strettamente necessaria per conseguire l'obiettivo, qualsiasi ingerenza per motivi di sicurezza nazionale nei diritti fondamentali della persona.

Sulla base di tali considerazioni, la Commissione precisa dunque che gli Stati Uniti operano in modo conforme ai criteri stabiliti dalla Corte di Giustizia nella sentenza *Schrems*, in base ai quali la normativa che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere «regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati».

4.4. La Commissione prosegue l'analisi della nuova intesa, valutando i meccanismi di vigilanza approntati dalla normativa statunitense al fine di verificare che l'attività di *intelligence* avvenga nel rispetto dei limiti sanciti dalla legge, nonché i rimedi individuali di cui dispone un cittadino UE che assuma la violazione della sua *privacy* da parte delle autorità pubbliche americane.

Sotto il primo profilo, la Commissione ha rilevato che la comunità dell'*intelligence* statunitense è sottoposta a vari meccanismi di controllo e di vigilanza dipendenti dai tre poteri dello Stato: organi interni e esterni dell'esecutivo, varie commissioni del Congresso e, per le attività contemplate dalla FISA, vigilanza del potere giudiziario.

In primo luogo, l'esecutivo esercita una consistente vigilanza sulle attività di *intelligence* condotte dalle autorità statunitensi. A norma della PPD-28, le politiche e procedure dei servizi della comunità dell'*intelligence* devono prevedere misure adeguate per facilitare la vigilanza sull'attuazione delle garanzie a protezione delle informazioni personali, tra cui misure che dispongono verifiche periodiche.

A tal fine, sono stati predisposti vari livelli di vigilanza: ispettori generali, l'Ufficio per la tutela della vita privata e le libertà civili dell'Ufficio del Direttore nazionale dell'*intelligence*, l'Autorità per la tutela della vita privata e delle libertà civili e l'Autorità presidenziale di vigilanza sull'*intelligence*.

Per facilitare l'esercizio della vigilanza, i servizi della comunità dell'*intelligence* sviluppano sistemi informatici che permettono il monitoraggio, la registrazione e la verifica delle interrogazioni o altre ricerche di informazioni personali.

Gli organi di vigilanza e di controllo della conformità controllano periodicamente le pratiche seguite dai servizi di *intelligence* per proteggere le informazioni personali contenute nell'*intelligence* dei segnali e il rispetto delle relative procedure.

In secondo luogo, oltre ai citati meccanismi di vigilanza inquadrati nell'esecutivo, il Congresso degli Stati Uniti d'America, e più precisamente le commissioni Giustizia e Intelligence della Camera dei rappresentanti e del Senato, ha competenze di vigilanza sulle attività d'*intelligence* esterna condotte dagli USA, *intelligence* dei segnali compresa.

Inoltre, il Presidente provvede affinché le commissioni del Congresso che si occupano di *intelligence* siano tenute perfettamente informate e aggiornate sulle attività d'*intelligence* condotte dagli USA.

La Commissione passa poi a verificare uno dei punti deboli del precedente regime di Approdo Sicuro – rivelatosi decisivo nel determinare la scelta della Corte di Giustizia di dichiararne l'invalidità –, ossia l'assenza di un rimedio giuridico che consenta al cittadino comunitario di accedere ai dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati.

Sotto tale profilo, la Commissione rileva che la normativa americana offre diversi mezzi al cittadino comunitario per sapere se i servizi della comunità dell'*intelligence* statunitense abbiano trattato dati personali che lo riguardano e, in caso affermativo, se siano state rispettate le limitazioni applicabili a norma della legge statunitense.

La FISA, nonché le leggi regolatrici di specifici settori – nel dettaglio, la legge sulle frodi e gli abusi informatici, la legge sulla *privacy* nelle comunicazioni elettroniche, la legge sul diritto alla *privacy* finanziaria – prevedono la possibilità di promuovere un procedimento civile contro

gli USA o nei confronti degli agenti del governo statunitense per ottenere un risarcimento pecuniario quando le informazioni che riguardano la persona interessata sono state usate o divulgate illecitamente e con dolo.

Nonostante, almeno in linea di principio, l'ordinamento statunitense offra una serie di possibilità di ricorso, i motivi per cui si possono adire le vie legali sono limitati e l'istanza presentata da una persona è dichiarata irricevibile se questa non è in grado di dimostrare la propria legittimazione ad agire, il che limita di fatto l'accesso al giudice ordinario.

Per rispondere alle legittime obiezioni delle istituzioni comunitarie circa l'effettività della tutela giurisdizionale avverso il trattamento illegittimo dei dati personali, il governo statunitense ha creato un nuovo meccanismo di mediazione, al fine di «assicurare che ogni reclamo riceva un esame e un trattamento adeguati e che una fonte indipendente confermi alla persona che le leggi degli Stati Uniti sono state rispettate o, se sono state violate, che l'inosservanza è stata nel frattempo sanata».

In realtà, tale organismo non è stato istituito *ad hoc* per rispondere specificamente alle istanze connesse all'applicazione del *Privacy Shield*, ma rientra nell'ambito degli strumenti previsti dalla direttiva presidenziale PPD-28, per svolgere la funzione di interlocutore per i governi stranieri in merito alle attività di *intelligence* dei segnali condotte dagli Stati Uniti d'America.

Le sue funzioni sono state dunque estese all'ambito di applicazione del *Privacy Shield*, per offrire un rimedio alternativo alla giustizia ordinaria (presumibilmente più efficiente ed economico) avverso le lesioni dei propri dati personali da parte delle agenzie governative statunitensi.

L'organismo di mediazione, denominato nell'Accordo Mediatore dello Scudo (o Ombudsperson), è composto da un Primo coordinatore, nominato direttamente dal Segretario di Stato, e da altri organi di vigilanza competenti a controllare i vari servizi della comunità dell'*intelligence*, sulla cui collaborazione il Mediatore dello scudo fa affidamento per il trattamento dei reclami.

In particolare, se il reclamo della persona verte sulla compatibilità della sorveglianza con la legge statunitense, il Mediatore può contare su organi di vigilanza indipendenti dotati di poteri di indagine (quali gli ispettori generali o l'Autorità per la tutela della vita privata e delle libertà civili).

In ogni caso il Segretario di Stato provvede a che il Mediatore disponga dei mezzi per garantire che la risposta apportata alla richiesta prenda in considerazione tutte le informazioni necessarie.

Questa struttura composita permette al meccanismo di mediazione di garantire una vigilanza indipendente e la possibilità di ricorso individuale.

Il reclamo può essere sporto presso l'autorità di vigilanza, competente nello Stato membro per la vigilanza sui servizi di sicurezza nazionali e/o del trattamento dei dati personali da parte delle autorità pubbliche, la quale lo sottopone a un organo centralizzato dell'UE, da cui viene poi inoltrato al Mediatore dello Scudo.

Il meccanismo di mediazione estende l'ambito di tutela accordata dall'autorità giudiziaria ordinaria, in quanto consente al soggetto leso di sporgere reclamo senza dovere dimostrare che il governo degli USA abbia effettivamente avuto accesso, nell'ambito delle attività di *intelligence* dei segnali, ai dati personali che lo riguardano.

Il reclamo si conclude in ogni caso con una risposta da parte del Mediatore, con cui conferma che il reclamo è stato esaminato adeguatamente e che è stata rispettata la legge statunitense applicabile oppure, in caso contrario, che l'inosservanza è stata nel frattempo sanata.

Nel complesso, la Commissione ritiene che il meccanismo assicuri che ciascun caso di reclamo sia esaminato a fondo e risolto e che, almeno relativamente alla sorveglianza, siano coinvolti autorità di vigilanza indipendenti dotate delle competenze tecniche e dei poteri d'indagine necessari e un Mediatore in grado di svolgere le proprie funzioni senza indebite ingerenze, in particolare di ordine politico.

Nonostante le rassicurazioni degli Stati Uniti, secondo cui il Mediatore è indipendente dalla comunità dell'*intelligence* statunitense e riferisce direttamente al Segretario di Stato, sono legittime – a nostro parere – le perplessità espresse dal Gruppo *ex* art. 29 in merito alla mancanza di indipendenza della figura del Mediatore[24], selezionato tra i ranghi governativi e facilmente removibile dall'incarico in ragione della nomina di origine politica.

4.5. Dopo aver passato in rassegna i principi del nuovo Scudo per la *privacy* e, in particolar modo, il meccanismo di funzionamento dell'*intelligence* statunitense, nell'intento di verificare se le deroghe

[24] Nel citato parere del 13 aprile 2016, il Gruppo esprime dubbi, oltre che sulla mancanza di indipendenza del Mediatore, anche sui suoi poteri di controllo, limitati dalla difficoltà ad avere accesso a tutte le informazioni rilevanti per esprimere la propria valutazione e dalla mancanza di un effettivo potere impositivo nei confronti delle autorità di *intelligence*: «First of all, concerns exist as to whether the Ombudsperson can be considered (formally and fully) independent, especially due to the relative ease with which political appointees can be dismissed. Secondly, concerns remain regarding the powers of the Ombudsperson to exercise effective and continuous control. Based on the available information in Annex III, the WP29 cannot come to the conclusion that the Ombudsperson will at all times have direct access to all information, files and IT systems required to make his own assessment nor that he can really compel the intelligence agencies in charge to end any non-compliant data processing, certainly in case of disagreement over the question if the data processing is in compliance with the law or not».

previste per le finalità di pubblica sicurezza siano suscettibili di minare il corretto funzionamento del sistema, la Commissione giunge alla conclusione (considerando n. 136) che gli Stati Uniti d'America assicurano «un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo dall'Unione alle organizzazioni statunitensi che si sono autocertificate come aderenti al regime».

Precisando il concetto nei considerando successivi, la Commissione evidenzia come il nuovo regime abbia rimediato ai principali vizi che avevano determinato la cassazione da parte della Corte di Giustizia del precedente Accordo *Safe Harbor*.

Sono stati, infatti, approntati meccanismi di vigilanza e di ricorso che permettono di individuare e punire le violazioni dei principi commesse dalle organizzazioni aderenti al regime e offrono all'interessato mezzi di ricorso che gli consentono di accedere ai dati personali che lo riguardano e di ottenerne la rettifica o cancellazione.

D'altra parte, l'ingerenza nei diritti fondamentali della persona, compiuta dall'autorità pubblica statunitense per esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico, si limita a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato.

In definitiva (considerando n. 141), «la Commissione giunge alla conclusione che sono soddisfatti i criteri dell'art. 25 della direttiva 95/46/CE, interpretati alla luce della Carta dei diritti fondamentali dell'Unione europea sulla scorta delle delucidazioni apportate dalla Corte di giustizia, in particolare nella sentenza *Schrems*».

4.6. Al fine di evitare che mutamenti nella legislazione statunitense in materia di tutela dei dati personali possano compromettere la coerenza complessiva dell'Accordo di Scudo, la Commissione verificherà periodicamente, anche attraverso le informazioni che il governo degli Stati Uniti si è impegnato a trasmettere in caso di cambiamenti rilevanti, che la normativa americana assicuri un livello di protezione sostanzialmente equivalente a quello offerto dalla legislazione comunitaria, anche alla luce della prossima definitiva applicazione del nuovo regolamento 2016/679.

Tale previsione dà così contenuto alle indicazioni di cui al punto 76 della sentenza *Schrems*, in cui la Corte, dopo aver precisato che il livello di protezione assicurato da un Paese terzo può evolversi, ha affermato che «incombe alla Commissione, successivamente all'adozione di una decisione in forza dell'art. 25, par. 6, della direttiva 95/46, verificare periodicamente se la constatazione relativa al livello di protezione

adeguato assicurato dal Paese terzo in questione continui ad essere giustificata in fatto e in diritto».

In tale ottica, l'Accordo sarà oggetto di un'analisi congiunta annuale da parte della Commissione con il Dipartimento del Commercio USA e la Federal Trade Commission, vertente su tutti gli aspetti del funzionamento dello Scudo, comprese le eccezioni ai principi per motivi di sicurezza nazionale e di amministrazione della giustizia.

Se, in base a tali verifiche, la Commissione dovesse constatare che il livello di protezione offerto dallo Scudo non può più essere considerato sostanzialmente equivalente a quello dell'Unione Europea, potrà chiedere l'adozione di misure adeguate per risolvere rapidamente i potenziali casi di inosservanza dei principi.

Qualora le autorità statunitensi non dovessero dimostrare che lo Scudo continua a garantire il rispetto effettivo dei principi e un livello di protezione adeguato, la Commissione avvierà la procedura per la sospensione o abrogazione totale o parziale dell'Accordo.

5. Il giudizio sul *Privacy Shield* non può prescindere dall'analisi del contesto emergenziale in cui è maturata la conclusione dell'Accordo. La sentenza *Schrems* rischiava di determinare uno stallo nel sistema che aveva consentito per circa quindici anni il trasferimento dei dati personali dei cittadini comunitari verso gli Stati Uniti[25]. Nel corso degli anni, infatti, oltre 5000 aziende, tra cui le maggiori *web companies* mondiali (ad es. Facebook, Google, Microsoft), avevano aderito al *Safe Harbor*, potendo, in tal modo, trasferire agevolmente i dati degli utenti europei presso i propri server negli Stati Uniti.

L'improvviso arresto di tale meccanismo imponeva la necessità di concludere in breve tempo una nuova intesa che ripristinasse tale flusso, correggendo al contempo i vizi del precedente Accordo *Safe Harbor*. Il *Privacy Shield* raggiunge parzialmente tale scopo. Le critiche principali non sono riconducibili all'elenco di principi, cui dovranno conformarsi le organizzazioni private nell'eseguire il trattamento dei dati personali: l'Accordo (come già in precedenza il *Safe Harbor*) richiama sostanzialmente i principi codificati dalla direttiva 95/46/CE. L'urgenza nel concludere l'Accordo non ha consentito, tuttavia, di includere le novità introdotte dal nuovo regolamento per la protezione dei dati personali, da cui consegue l'inevitabile necessità di procedere alla

[25] Secondo lo studio del marzo 2013 del Centro europeo per la politica economica internazionale per la Camera di Commercio statunitense *The Economic Importance of Getting Data Protection Right* l'impatto negativo sul Pil dell'UE derivante dalla soppressione del regime di Approdo Sicuro sarebbe stato ricompreso tra -0,8% e -1,3%, e le esportazioni di servizi dall'UE agli USA sarebbero calate del 6,7% a causa della perdita di competitività.

revisione del *Privacy Shield* prima della definitiva applicazione del regolamento, prevista per il maggio 2018.

Sotto il profilo formale, sono poche, dunque, le censure addebitabili al complesso di tutele disegnato dalla nuova intesa. Maggiori sono le perplessità circa l'effettività della tutela garantita dallo Scudo, in ragione dell'ampia possibilità per le autorità di *intelligence* statunitensi di derogare ai principi fissati nell'intesa. La Commissione Europea non è riuscita ad ottenere dagli Stati Uniti l'impegno a predisporre una disciplina *ad hoc* per il trattamento dei dati dei cittadini comunitari, affinché questi non ricadessero nella normativa generale prevista dall'ordinamento americano.

Il mantenimento, anche nel nuovo Accordo, della clausola che consente agli Stati Uniti di derogare ai principi fissati nel *Privacy Shield* per esigenze di sicurezza nazionale assoggetta i dati personali provenienti dall'Europa agli ampi poteri di indagine che la legislazione statunitense accorda alle agenzie governative. La maggiore trasparenza circa il meccanismo di funzionamento del sistema di *intelligence* statunitense – il precedente Accordo non faceva menzione alcuna delle leggi che consentivano alle autorità di *intelligence* di derogare ai principi fissati nell'intesa – non vale ad escludere il forte rischio che i dati dei cittadini comunitari siano sottoposti a raccolta indiscriminata da parte delle agenzie governative americane.

Nonostante le rassicurazioni in merito ampiamente espresse dalle autorità americane, l'analisi del quadro normativo statunitense evidenzia ampi margini discrezionali circa l'estensione dei controlli sui dati personali dei cittadini stranieri. La direttiva presidenziale PPD-28, su cui si fonda molto del ragionamento della Commissione nell'affermare la presenza di limiti più stringenti ai poteri dell'*intelligence* statunitense, è atto fortemente collegato alla figura del Presidente che lo ha emanato e, in quanto tale, pur non decadendo automaticamente alla cessazione del suo mandato, è revocabile dal Presidente entrante, qualora questi intenda estendere i poteri delle agenzie di *intelligence*[26].

[26] Sulla natura giuridica delle direttive presidenziali, si veda United States. Department of Justice. Office of Legal Counsel, MOSS, *Legal effectiveness of a presidential directive, as compared to an executive order* (2000), che sancisce il seguente principio: «A presidential directive has the same substantive legal effect as an executive order. It is the substance of the presidential action that is determinative, not the form of the document conveying that action. Both an executive order and a presidential directive remain effective upon a change in administration, unless otherwise specified in the document, and both continue to be effective until subsequent presidential action is taken».

Tra l'altro, come sottolineato anche dal Gruppo di lavoro *ex* art. 29[27], la direttiva presidenziale non è in grado di creare diritti a favore degli individui, essendo tale facoltà riservata esclusivamente alla legge; ragion per cui, un soggetto non potrà invocare in giudizio la mancata applicazione delle garanzie fornite dalla direttiva[28].

Su un piano strettamente giuridico, la profonda diversità di disciplina, circa i limiti che l'attività di *intelligence* deve incontrare nei riguardi della sfera privata dei cittadini non consente di concordare con la valutazione della Commissione, secondo la quale la normativa statunitense assicura un livello di protezione sostanzialmente equivalente a quello garantito dalla legislazione comunitaria.

Sotto tale profilo, l'attuale strutturazione dell'Accordo rischia di ricevere le medesime censure che la Corte di Giustizia ha riservato al precedente Accordo *Safe Harbor*. Sul punto, basti ricordare che la Corte di Giustizia ha dichiarato l'illegittimità della direttiva 2006/24/CE, considerando eccessivo il periodo di conservazione dei dati, da sei mesi a due anni, previsto nel provvedimento, mentre la normativa statunitense consente al Governo americano la conservazione dei dati personali per cinque anni, peraltro prorogabili con decisione del Direttore dell'*intelligence* nazionale.

Considerazioni di natura extragiuridica – i.e. di natura commerciale e politica, legate all'esigenza di non intralciare il traffico di informazioni personali tra Europa e USA, fondamentale per lo sviluppo dell'economia digitale – potrebbero, tuttavia, indurre la Corte di Giustizia – qualora fosse chiamata ad esprimersi sulla legittimità del *Privacy Shield* – ad esprimere un giudizio di compatibilità con l'art. 25 della direttiva 95/46/CE, eventualmente sollecitando la Commissione Europea a rivedere gli aspetti più critici dell'Accordo.

[27] Il Gruppo di lavoro, nel parere già citato del 13 aprile 2016, evidenzia: «The WP29 notes that PPD-28 is only a directive and therefore cannot create any rights for individuals. This can only be done through legislation. Therefore, individuals cannot go to court based on an alleged violation of the PPD-28 safeguards».

[28] In merito alla scarsa efficacia della direttiva nel contenere i poteri dell'*intelligence* americana, si veda SEVERSON, *American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Changes*, in *HILJ*, 2015, 465, 481-492.

ABSTRACT

The Evolution of the Right to Privacy Between Europe and United States: From Safe Harbor to Privacy Shield

This article analyses the way that led to the drawing up of the Privacy Shield Agreement that regulates the personal dataflow from the European Union to the United States.

The analysis begins with a description of the different approaches to personal data protection by both the US and the EU.

Starting from the principles that constituted the previous agreement in matter, the so-called Safe Harbor Agreement, this article considers the reasons that have brought the European Court of Justice to declare its invalidity by means of the Schrems decision. It also analyses the main characteristics of the new agreement with the purpose of highlighting the differences with the preceding regime and the compliance with the principles stated in the Directive 95/46/EC of the European Parliament.