OSSERVATORIO EUROPEO

L'ACCORDO QUADRO TRA USA E UE SUL TRASFERIMENTO DEI DATI PERSONALI PER IL CONTRASTO DELLA CRIMINALITÀ

MARCO MASTRACCI

1. Le opportunità offerte dall'evoluzione tecnologica e dallo sviluppo di Internet hanno posto il diritto alla protezione dei dati personali di fronte a nuove sfide. La raccolta e lo sfruttamento massivo degli stessi hanno reso, infatti, molto più difficile il bilanciamento tra esigenze di protezione della *privacy* ed esigenze di prevenzione e repressione della criminalità[1].

Gli odierni sistemi informatici – con una molteplicità di strumenti sempre più sofisticati e interconnessi – hanno determinato un continuo processo di raccolta delle informazioni personali, agevolmente archiviati a costi contenuti, ampliando a dismisura lo spettro delle attività che possono essere svolte attraverso l'analisi delle informazioni ottenute.

È forte la tendenza da parte delle forze di polizia, nell'ambito delle strategie nella lotta contro la criminalità interna ed internazionale, a fronteggiare tali minacce avvalendosi dei suddetti strumenti, con il rischio di delegare totalmente l'attività di indagine e di contrasto della criminalità ad algoritmi in grado di predire la futura commissione di crimini[2].

[1] Per una completa ricostruzione del rapporto tra *privacy* e sfruttamento dei dati personali per finalità di contrasto della criminalità si veda NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012, 147-350; RUBECHI, *Sicurezza, tutela dei diritti fondamentali: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 2016, n. 23; SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento*, in S. TORRE (a cura di), *Costituzioni e sicurezza dello Stato,* Maggioli, Bologna, 2013.

[2] Sul tema, si veda il contributo di VAN BRAKEL, DE HERT, *Policing, Surveillance and Law in a Pre-crime Society: Understanding the Consequences for Technology based Strategies*, in *Cahiers Politiestudies Jargaang*, 2011-3, n. 20.

L'estensione territoriale assunta da fenomeni criminali quali il terrorismo, il traffico illecito di stupefacenti, il riciclaggio di capitali, la corruzione, denotano come la criminalità organizzata abbia assunto dimensioni che esorbitano lo spazio territoriale dei singoli Stati, per divenire vero e proprio fenomeno transnazionale. Diventa, quindi, indispensabile unificare la raccolta delle informazioni personali, permettere una tempestiva condivisione delle stesse, coordinarne l'impiego e sviluppare sistemi di elaborazione e di analisi che aggreghino tali dati per estrarre nuova conoscenza dagli stessi.

In tale ottica, si rivela fondamentale la sottoscrizione di accordi internazionali per condividere tale mole di dati ed evitare che la frammentazione delle informazioni a livello dei singoli paesi impedisca un'efficiente repressione dei crimini di rilevanza sovranazionale. Al contempo, è necessario che le esigenze investigative e repressive non diano luogo alla creazione di un sistema generalizzato di controllo delle comunicazioni personali, in cui la *privacy* delle persone sia fortemente compromessa. Tale rischio è particolarmente avvertito negli ultimi tempi, in cui diversi Stati nazionali – i più toccati da eventi legati al terrorismo internazionale – hanno adottato misure emergenziali che limitano fortemente la libertà dei cittadini.

All'indomani degli attentati alla sede del giornale *Charlie Hebdo* del 7 gennaio 2015, il Parlamento francese ha varato una legge[3] che autorizza numerose tecniche di sorveglianza mirata: intercettazioni ambientali, telefoniche e delle comunicazioni *internet*, intrusione informatica nei *computer*, geolocalizzazione. La legge autorizza inoltre l'installazione, sulle reti e sui *server*, delle c.d. *boîtes noires* (scatole nere), ossia dispositivi per scannerizzare i traffici telefonici e via internet al fine di individuare, con l'ausilio di algoritmi tenuti segreti, le comunicazioni sospette in rapporto con una minaccia terroristica.

Oltre alle numerose critiche per le gravi ingerenze nella vita privata delle persone[4], tali misure hanno sollevato forti dubbi anche in merito alla loro efficacia, considerato che non hanno evitato il ripetersi di

[3] Legge n. 2015-912 del 24 luglio 2015. Il *Conseil constitutionnel*, con la *décision* n. 2015-713 DC del 23 luglio 2106, ha dichiarato la conformità della legge alla Costituzione, ad eccezione di alcune disposizioni in tema di geolocalizzazione e delle misure di "sorveglianza internazionale"; in un secondo tempo, con la *décision* n. 2016-590 QPC del 21 ottobre 2016, ha esteso l'incostituzionalità della norma alla parte in cui consentiva «la surveillance et le control de transmissions empruntant la voie hertzienne» senza particolari autorizzazioni giudiziarie e amministrative.

[4] I giornali francesi hanno espresso ripetutamente il loro dissenso nei confronti della legge: si veda, per tutti, l'articolo di *Le Monde* del 15 aprile 2015, *Pourquoi la loi sur le renseignement cristallise les critiques*, disponibile al sito www.lemonde.fr.

ulteriori attacchi terroristici, come dimostrano i fatti tragici di Parigi nel novembre del 2015 e di Nizza nel luglio 2016.

Spostando l'attenzione fuori dai confini europei, il caso più noto in cui le esigenze di sicurezza interna hanno prevalso nettamente sulla tutela dei dati personali dei cittadini è sicuramente rappresentato dagli Stati Uniti d'America. Dopo gli attacchi terroristici dell'11 settembre 2001, gli USA hanno adottato il famigerato *Patriot Act*[5], che ha consentito alla National Security Agency (NSA) di raccogliere indistintamente i dati telefonici di milioni di americani e conservarli nei suoi database. Le rivelazioni nel 2013 dell'ex *contractor* della CIA, Edward Snowden[6], hanno evidenziato come gli Stati Uniti avessero creato un sistema di sorveglianza globale che prevedeva l'intercettazione diretta del flusso di comunicazioni telefoniche e telematiche veicolato attraverso le reti statunitensi e l'accesso sistematico ai dati di traffico degli utenti, conservati nelle banche dati tenute dai maggiori fornitori di servizi di telecomunicazione e contenuti multimediali.

A differenza degli esempi appena citati, l'Unione Europea ha accresciuto negli ultimi anni l'ambito di tutela dei dati personali trattati per finalità di contrasto della criminalità. Tale diversità di impostazione[7], rimasta sopita per anni, è emersa prepotentemente a seguito delle rivelazioni di Snowden, che hanno convinto le istituzioni UE circa la necessità di rivedere gli accordi che disciplinavano il trasferimento dei

---

[5] 50 USC 1861 − *Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations.* Nel corso degli anni la legge è stata oggetto di ripetute modifiche, che ne hanno limitato il raggio d'azione. Nel 2015, con l'approvazione dello Usa Freedom Act (*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*), sono state modificate le disposizioni del Patriot Act che avevano consentito alla National Security Agency di raccogliere enormi quantità di metadati telefonici.

[6] Snowden 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 vedano, a tal riguardo, gli articoli apparsi il 6 giugno 2013 sul *The Guardian*, GREENWALD, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, disponibile su www.theguardian.com, e sul *The Washington Post*, *NSA Slides Explain the PRISM Datacollection Program*, disponibile su www.washingtonpost.com.

[7] Per un'ampia disamina delle differenze tra UE e USA in materia di trattamento dei dati per finalità di contrasto della criminalità, si veda BOHEM, *A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes*, Study for the LIBE Committee, PE 2015; SCHWARTZ, SOLOVE, *Reconciling Personal Information in the United States and European Union*, in *California L Rev.*, 2014, 877; BIGNAMI, RESTA, *Transatlantic Privacy Regulation: Conflict and Cooperation*, in *LCP*, 2015, 101. Sul sistema statunitense si veda anche BIGNAMI, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the LIBE Committee, PE 519.215, maggio 2015.

dati tra i due continenti[8]. Per quanto attiene al flusso dei dati personali trasferiti oltreoceano per finalità commerciali, è stato quindi sottoscritto il nuovo Accordo denominato *Privacy Shield*, che, nel 2016, ha preso il posto della precedente intesa *Safe Harbor*, in vigore dal 2000, dichiarata invalida dalla Corte di Giustizia UE con la nota sentenza *Schrems* del 6 ottobre 2015[9].

Il trasferimento dei dati personali per finalità di contrasto della criminalità, regolato in passato solo da accordi parziali, è stato disciplinato dal recente Accordo quadro noto come *Umbrella Agreement*, entrato in vigore l'1 febbraio 2017, che predispone un *set* di principi cui le parti contraenti dovranno informare il trasferimento dei dati personali per le finalità anzidette. Prima di addentrarci nei dettagli dell'Accordo – oggetto del presente contributo – appare opportuno fornire un breve quadro di insieme sul modo in cui i due continenti traducono in atti normativi le differenti impostazioni sul trattamento dei dati personali per finalità di contrasto della criminalità, in quanto tali (differenti) approcci sono destinati a ripercuotersi inevitabilmente in fase di esecuzione dell'Accordo.

2. *L'acquis* di diritto UE offre un livello di protezione dei dati personali difficilmente rinvenibile in altri ordinamenti giuridici nazionali. Il Trattato di Lisbona ha conferito rango di fonte primaria dell'Unione Europea alla Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000[10]. L'art. 8 della Carta precisa che ogni persona ha diritto alla protezione dei dati personali che la riguardano, i quali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso delle persona interessata o a un altro fondamento legittimo previsto dalla legge. Se naturalmente si può prescindere dal consenso della persona interessata per garantire l'efficacia dell'attività investigativa, il trattamento dei dati deve comunque essere eseguito in conformità ai principi stabiliti dall'art. 8 della Carta.

Passando dai principi alla normativa di dettaglio, va ricordato che per molto tempo la legislazione comunitaria non prevedeva uno strumento generale a livello europeo che disciplinasse il trattamento dei

[8] Cfr. la comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM(2013) 846 def. del 27 novembre 2013.

[9] Causa C-362/14.

[10] 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 POCAR, *Commento alla Carta dei diritti fondamentali dell'Unione europea,* in ID. (a cura di), *Commentario breve ai Trattati della Comunità e dell'Unione europea,* Cedam, Padova, 2014, 1179 ss.

dati nel settore della cooperazione giudiziaria e di polizia in materia penale. La fondamentale direttiva 95/46/CE si applica, infatti, a qualsiasi trattamento di dati personali negli Stati membri sia nel settore pubblico che in quello privato, ma non ai trattamenti di dati personali effettuati per le finalità di contrasto della criminalità.

Fino alla decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008, la tutela dei dati personali in tale settore era disciplinata da norme *ad hoc*, che, in relazione a ciascun organo (ad esempio Europol, Eurojust) incaricato di trattare determinati dati personali, ne stabiliva la relativa disciplina, con conseguente creazione di un quadro incoerente e frammentario della protezione dei dati personali in materia penale. Va peraltro rilevato che il perimetro applicativo della decisione quadro era espressamente circoscritto al trattamento di dati personali trasmessi o resi disponibili tra Stati membri. Ne restavano, quindi, esclusi i trattamenti che uno Stato membro effettuava su dati personali trattati soltanto dai propri organi interni.

Al fine di equiparare la tutela dei dati personali per le finalità di contrasto della criminalità a quella predisposta in ambito generale dalla direttiva 95/46/CE[11], nel 2016 il Parlamento Europeo e il Consiglio hanno approvato la direttiva (UE) 2016/681[12], relativa al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che ha abrogato la citata decisione quadro. La direttiva ha esteso i principi che già ispiravano la disciplina generale prevista dalla direttiva 95/46/CE al trattamento dei dati per finalità di contrasto della criminalità, al cui rispetto pertanto neanche le autorità di polizia potranno sottrarsi. A tal riprova, l'art. 4 della direttiva riproduce quasi alla lettera la formulazione dell'art. 6 della direttiva 95/46/CE, che stabilisce i principi cardine in materia di trattamento dei dati personali.

In tale ambito, va altresì menzionata la fondamentale attività propulsiva della Corte di Giustizia[13] che, negli ultimi anni, ha rafforzato

[11] Come noto, la direttiva n. 95/46/CE è stata sostituita dal Regolamento 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.

[12] Per un commento della direttiva v. DI FRANCESCO MAESA, *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*, 24 maggio 2016, disponibile su http:// rivista.eurojus.it.

[13] Sulla giurisprudenza della Corte di Giustizia, si veda FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems,* in RESTA,

il contenuto garantista dei precetti normativi che salvaguardano la tutela dei dati personali. Fondamentale, al riguardo, è stato il *decisum* nella ormai celebre sentenza *Digital Rights*[14], che ha dichiarato l'illegittimità della direttiva 2006/24/CE, per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza. La direttiva imponeva l'obbligo, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, di conservare i dati personali relativi al traffico e all'ubicazione dei soggetti fruitori di tali servizi, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi. Come ha rilevato la Corte, tali dati, pur non riproducendo il contenuto della conversazione, forniscono comunque indicazioni importanti sulle comunicazioni intrattenute da ciascuno, sui loro destinatari e sulla loro frequenza.

L'accesso da parte dell'autorità pubblica a queste informazioni comporta una forte ingerenza nella vita privata dei cittadini, convincendoli di essere esposti a una costante sorveglianza, in quanto la conservazione e il successivo utilizzo dei dati stessi avviene a insaputa dell'interessato. Pur essendo tale accesso giustificato dalla necessità di combattere gravi forme di criminalità, la direttiva avrebbe, secondo la Corte, ecceduto i limiti imposti dal principio di stretta proporzionalità, che ammette deroghe o limitazioni alla protezione dei dati personali soltanto nella misura in cui le stesse siano strettamente necessarie.

L'analisi congiunta dell'operato degli organi legislativi e giurisdizionali evidenzia la volontà delle istituzioni europee di non cedere il passo alle tentazioni provenienti da singoli Stati membri di accentuare il controllo sui cittadini europei, compromettendo i loro diritti di libertà. In tal senso, la recente emanazione del Regolamento 2016/679 sottolinea la volontà di innalzare il livello di tutela dei dati personali e renderlo realmente uniforme all'interno del territorio comunitario.

In tale contesto, emerge anche la difficoltà per l'Unione Europea di garantire che lo stesso livello di protezione ai dati personali venga garantito anche nel momento in cui i dati raccolti nel territorio dei suoi Stati membri siano trasferiti ad uno Stato terzo. Tale preoccupazione

---

ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbor Principles" al "Privacy Shield"*, Roma, 2016.

[14] Corte di giustizia, sentenza 8 aprile 2014, cause riunite C-293/12 e C-594/12. Per un commento della sentenza si v. SCAGLIARINI, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra*, in *Dir. Inf.*, 2014, 851, e CASCIONE, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della Corte di giustizia e gli echi del Datagate*, in *Nuova giur. civ. comm.*, 2014, I, 1044.

accompagna le istituzioni UE fin dall'approvazione della direttiva 95/46/CE, che, all'art. 25, prevedeva la possibilità di trasferire i dati personali verso un paese terzo «soltanto se il Paese terzo di cui trattasi garantisce un livello di protezione adeguato». Come accennato, con la sentenza *Schrems* la Corte di Giustizia ha dichiarato invalidi gli accordi noti come *Safe Harbor*, che disciplinavano il trasferimento dei dati personali in ambito commerciale dall'Europa agli USA, considerato che l'ordinamento giuridico americano non garantiva un livello di protezione sostanzialmente conforme agli *standard* UE.

Anche in materia di cooperazione giudiziaria e di polizia in materia penale, la decisione quadro 2008/977/GAI aveva ribadito tale principio, subordinando il trasferimento dei dati personali a favore di uno stato terzo alla circostanza che questo garantisse un livello di protezione adeguato. In linea di continuità con tale orientamento, la già citata direttiva 2016/681 conferma, precisandone i contenuti, la portata di tale disposto. In particolare, la direttiva prevede una serie di procedure che legittimano il trasferimento dei dati personali a paesi terzi. L'art. 36 prevede il trasferimento sulla base di una decisione della Commissione, che abbia accertato l'adeguatezza del livello di protezione del Paese terzo. In tal caso il trasferimento non necessita di autorizzazioni specifiche. Ai fini del nostro contributo rileva la previsione della lett. *a*) dell'art. 37, par. 1, di tale direttiva, che prevede che gli Stati membri dispongono il trasferimento di dati personali verso un Paese terzo se sono fornite garanzie adeguate per la protezione dei dati personali in uno strumento giuridicamente vincolante.

L'*Umbrella Agreement* è l'atto giuridico, che garantisce l'adeguatezza del livello di protezione offerto dagli Stati Uniti. Come espressamente previsto dall'art. 1, l'Accordo quadro non costituisce una base giuridica per il trasferimento di dati personali tra UE e USA, essendo a tal fine necessaria una distinta base giuridica. Inoltre, a differenza della decisione di adeguatezza contemplata dall'art. 36 della direttiva 2016/681, l'Accordo non prevede un'autorizzazione generale per i trasferimenti, sebbene l'art. 5 disponga che l'effettiva implementazione dell'Accordo da parte dei contraenti non richieda un'ulteriore autorizzazione per i trasferimenti di dati successivi.

3. Nonostante gli Stati Uniti vantino una lunga tradizione in materia di tutela della *privacy* – la prima enunciazione di tale principio è solitamente riconducibile al saggio *The Right of Privacy* degli avvocati Samuel Warren e Louis Brandeis nel 1890[15] – e di tutela dei dati

[15] WARREN, BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, 5.

personali[16], le esigenze di sicurezza interna hanno spesso prevalso sulla necessità di salvaguardare il diritto alla protezione dei dati personali degli individui.

A livello costituzionale, il Quarto emendamento alla Costituzione USA 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 probabili motivi che tale attività possa contribuire a ottenere prove relative alla commissione di un reato[17]. Per estensione, tale precetto vale a garantire tutela costituzionale al diritto alla *privacy* e, di riflesso, alla tutela dei dati personali. La protezione offerta dal Quarto emendamento soffre di un'importante limitazione, dal momento che non si estende alla tutela dei cittadini stranieri, ma opera esclusivamente a favore della popolazione americana. L'ambito di tutela è ulteriormente limitato dall'applicazione del principio della c.d. *third party doctrine*[18], in ragione del quale le persone non possono vantare una legittima aspettativa di *privacy* riguardo alle informazioni che esse stesse trasferiscono a terzi in maniera volontaria. In altri termini, una volta comunicate tale informazioni ad un soggetto terzo, ad esempio un *provider* di servizi Internet, il titolare di tali dati perde ogni diritto su di essi e non può dolersi che tali informazioni siano, in un momento successivo, comunicate alle agenzie governative.

A livello di normativa federale, l'*US Privacy Act* del 1974[19] – una tra le prime leggi al mondo a regolare la tutela della *privacy* in ambito pubblico – disciplina, in via generale, il trattamento dei dati personali da parte delle agenzie federali per finalità di contrasto della criminalità. [20]

Il *Privacy Act* conferisce agli individui il diritto di accesso ai loro dati personali e quello di rettifica e di cancellazione, qualora tali dati non siano corretti, rilevanti o completi; inoltre, consente al soggetto il quale

---

[16] Sul punto si veda GROSS, *The Concept of Privacy*, in *New York Univ. LR*, 1967, 34 ss.; WESTIN, *Privacy and Freedom*, New York, 1967; Thomson, *The Right to Privacy*, in *Philosophy & Public Affairs dimensions of Privacy*, 1975, 295 ss.; BENNETT, *Regulating Privacy: Data protection and public policy in Europe and the United States*, Cornell University Press, 1992, 14 ss.

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

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

[19] *Privacy Act of 1974, 5 U.S.C. § 552.*

[20] Le origini della sua emanazione sono direttamente riconducibili al timore creato dallo scandalo del Watergate circa la possibilità che le agenzie federali potessero compiere attività illegale di investigazione e sorveglianza nei confronti degli individui. In linea generale, il *Privacy Act* condivide molti dei principi UE in materia di tutela dei dati personali. Il trattamento dei dati personali deve essere informato a trasparenza, accuratezza, pertinenza e proporzionalità.

ritenga lesi i propri diritti a seguito di una violazione del *Privacy Act* da parte delle autorità di polizia di adire l'autorità giurisdizionale al fine di ottenere il risarcimento dei danni subiti. Al contempo, esso prevede così tante eccezioni da frustrare inevitabilmente la tenuta complessiva del sistema di tutele approntate[21].

Tra le più rilevanti vi è quella prevista dalla *subsection 5 U.S.C. § 552a(j)* che consente ad ogni agenzia federale «which performs as its principal functions any activity pertaining to the enforcement of criminal laws» di essere esentata dalla maggior parte degli obblighi previsti dal *Privacy Act*, tra cui quelli fondamentali di rilevanza, di accuratezza, di completezza, privando allo stesso tempo il cittadino dalla facoltà di accesso e di rettifica, nonché di azionare in via giudiziale la lesione del suo diritto.

Per far comprendere l'estensione di tali esenzioni, basti pensare che rientrano nella suddetta definizione il *Federal Bureau of Investigation (FBI),* la *Drug Enforcement Administration (DEA),* agenzia federale antidroga, e il *Bureau of Alcohol, Tobacco, Firearms and Explosives,* agenzia preposta a indagare sui reati federali relativi all'uso, alla fabbricazione e al possesso di armi da fuoco ed esplosivi, nonché su incendi dolosi, attentati dinamitardi, e sul traffico illegale di alcolici e tabacchi[22]. Di rilievo è anche l'esenzione prevista dal *Privacy Act* dalla *subsection 5 U.S.C. § 552a(k)* con riferimento a «matters that are [...] (A) specifically authorized under criteria established by Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order». La previsione in oggetto, che ricomprende le agenzie che operano nell'interesse della sicurezza nazionale, è valsa ad esimere la National Security Agency – responsabile del programma di sorveglianza globale adottato dagli Stati Uniti – dagli obblighi imposti dal *Privacy Act*.

Di fatto, l'ampiezza di tali deroghe pregiudica inevitabilmente l'effettività delle garanzie offerte dal complesso di diritti predisposto dal *Privacy Act*. A ciò si aggiunga che, al pari del Quarto Emendamento della Costituzione, le tutele fornite dal *Privacy Act* si applicano esclusivamente ai cittadini americani e ai soggetti residenti in via permanente negli

[21] Per una esemplare panoramica delle disposizioni del *Privacy Act* v. il rapporto *Overview of the Privacy Act of 1974,* redatto dall'*Office of Privacy and Civil Liberties* (OPCL) del Dipartimento di Giustizia Americano, reperibile al sito: www.justice.gov.

[22] La portata di tali deroghe è così ampia, da aver fatto pronunciare alla Corte distrettuale della Virginia le seguenti parole: «Put in the simplest terms, what Congress gave Congress can take away, which it did here by conferring on agencies the power to exempt certain records from the Privacy Act» (*Williams v. Farrior*, 334 F. Supp. 2d 898, 905; E.D. Va. 2004). La Corte prosegue il ragionamento, spiegando che «Congress, at most, granted" an "inchoate right" to individuals"».

USA[23]. Sotto tale profilo, almeno per quanto attiene ai cittadini UE, va peraltro sottolineato che il *Judicial Redress Act* (JRA), firmato dal Presidente Obama il 24 febbraio 2016, ha migliorato parzialmente tale limitazione, estendendo ai cittadini delle *designated countries*[24] (tra cui sono ricompresi i Paesi UE) i motivi di ricorso giurisdizionale previsti dal *Privacy Act*.

Come vedremo più diffusamente in seguito, la tutela prevista dal JRA è parziale, in considerazione delle già limitate garanzie fornite dal *Privacy Act* e delle ulteriori deroghe a quest'ultime, fissate dal JRA.

4. Il 1° febbraio 2017 è entrato in vigore l'Accordo quadro denominato *Umbrella Agreement* tra gli Stati Uniti d'America e l'Unione Europea sulla protezione delle informazioni personali a fini di prevenzione, indagine, accertamento e perseguimento di reati[25].

L'Accordo ha avuto un lungo periodo di gestazione: nel 2006 è stato istituito un gruppo di contatto ad alto livello, composto da funzionari UE ed USA, al fine di individuare le soluzioni più opportune per rendere più stretta ed efficace la collaborazione nello scambio di informazioni in materia di contrasto della criminalità.

Nella relazione finale dell'ottobre 2009, il gruppo suggeriva l'adozione di un Accordo internazionale che vincolasse l'UE e gli USA ad applicare principi comuni in materia di protezione dei dati per i trasferimenti transatlantici di dati nel settore dell'attività di contrasto alla criminalità. Sulla base di tali conclusioni, nel dicembre 2010 il Consiglio autorizzava la Commissione ad avviare i negoziati con gli Usa per raggiungere un'intesa in tal senso.

I negoziati, avviati il 28 marzo 2011, si sono conclusi l'8 settembre 2015 con la sigla del testo finale, cui è seguita in data 2 giugno 2016 l'effettiva sottoscrizione dell'Accordo da parte delle rispettive delegazioni diplomatiche. Ai sensi della procedura stabilita dall'art. 218 TFUE, l'approvazione definitiva dell'Accordo ha necessitato del voto

[23] Sul punto v. BIGNAMI, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Study for the LIBE Committee*, 2015; GWU Law School Public Law Research Paper No. 2015-54; GWU Legal Studies Research Paper No. 2015-54.

[24] Una *designated country* ai sensi del JRA è un Paese: i) che ha concluso con gli USA un Accordo che prevede adeguate tutele della vita privata per le informazioni condivise a fini di contrasto della criminalità (è questo il caso dell'UE); ii) che permette il trasferimento di dati personali a fini commerciali mediante un Accordo con gli USA o in altro modo; iii) le cui politiche in materia di trasferimento di dati personali a fini commerciali non compromettono gli interessi di sicurezza nazionali degli Stati Uniti. L'Attorney General degli Stati Uniti provvede a individuare le *designated countries.*

[25] *GUUE* L 25, 31 gennaio 2017.

positivo del Parlamento Europeo, intervenuto in data 1 dicembre 2016, e dell'approvazione del Consiglio[26], avvenuta il giorno successivo. Come già detto, l'Accordo è entrato in vigore il 1° febbraio 2017, a seguito delle notifiche di avvenuto completamento delle rispettive procedure interne di approvazione. Esso si propone di istituire una cornice di principi e garanzie in materia di protezione dei dati per il trasferimento di informazioni personali a fini di contrasto penale tra gli Stati Uniti, da un lato, e l'UE o i suoi Stati membri, dall'altro. Il duplice obiettivo è garantire un livello elevato di protezione dei dati e rafforzare così la cooperazione tra le parti.

Nel preambolo – e successivamente all'art. 1 – è precisato che l'Accordo non costituisce di per sé la base giuridica del trasferimento delle informazioni personali, ma il suo compito è quello di fissare principi e garanzie che informino i futuri accordi di trasferimento, integrando, al contempo, ove necessario, le disposizioni degli accordi vigenti. A tal fine, appare utile ricordare che sono già vigenti accordi fra UE e USA per attività di contrasto del crimine: ricordiamo l'Accordo sulla mutua assistenza giudiziaria, quello sull'uso e trasferimento delle registrazioni dei nominativi dei passeggeri (PNR)[27] e quello sul trattamento e trasferimento di dati di messaggistica finanziaria ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP)[28]. Il preambolo precisa che le disposizioni dell'art. 19, relative all'adozione di un rimedio giurisdizionale a favore degli individui che subiscano una lesione dei propri dati personali, si applicheranno anche a questi.

L'*Umbrella Agreement* costituisce il naturale completamento della recente intesa denominata *Privacy Shield*, attraverso la quale USA e UE hanno disciplinato il flusso di dati personali in ambito commerciale dal continente europeo agli Stati Uniti[29]. L'Accordo quadro copre tutte le informazioni personali (nomi, indirizzi, dati del casellario penale)

[26] Decisione n. 2016/2220.

[27] «Accordo tra gli USA e l'UE sull'uso e sul trasferimento del codice di prenotazione (Passenger Name Record — PNR) al Dipartimento per la sicurezza interna degli Stati Uniti» in GUUE L215 dell'11.8.2012. I *passenger name record* consistono in un insieme di informazioni che vengono raccolte dalle compagnie aeree in sede di prenotazione di un biglietto; tra le informazioni raccolte rientrano anche quei dati non strettamente necessari alla transazione, ma il cui trattamento è comunque finalizzato a fornire un migliore servizio alla clientela.

[28] «Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi», in GUUE L8 del 13.1.2010.

[29] In materia sia consentito rinviare a MASTRACCI, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield,* in questa *Rivista,* 2016, 555.

condivise tra le autorità di polizia degli Stati UE e degli USA, e stabilisce norme comuni per la protezione della *privacy*.

5. L'*Umbrella Agreement* si compone di 29 articoli, sommariamente suddivisibili in cinque categorie: i) scopo e ambito di applicazione dell'Accordo; ii) principi e garanzie in materia di protezione dei dati; iii) diritti delle persone fisiche; iv) aspetti relativi all'applicazione dell'Accordo e alla supervisione; v) disposizioni finali.

Nell'Accordo ritroviamo concetti e termini che affondano le proprie radici non solo nella consolidata tradizione UE, ma che appartengono anche all'esperienza giuridica statunitense che, come detto, ebbe il merito di introdurre una delle prime normative in materia di trattamento dei dati personali per finalità di polizia al fine di scongiurare il ripetersi dello scandalo *Watergate*, che aveva portato alle dimissioni del presidente Nixon.

Scendendo nel dettaglio del trattato, l'art. 1 ne enuncia lo scopo, che è quello di assicurare un elevato livello di protezione dei dati personali e di migliorare la cooperazione tra gli Stati Uniti e l'Unione Europea in relazione alla prevenzione, investigazione, perseguimento di reati, incluso il terrorismo. Esso precisa inoltre che l'intesa non costituisce di per sé la base giuridica del trasferimento delle informazioni personali verso gli Stati Uniti: il suo compito è quindi quello di integrare, ove necessario, le garanzie di protezione dei dati contemplate negli accordi vigenti o futuri per il trasferimento di dati o nelle disposizioni nazionali che autorizzano tali trasferimenti.

L'art. 3 dell'Accordo quadro definisce il campo di applicazione dello stesso, precisando che le tutele e le garanzie in esso previste si applichino a tutti gli scambi di dati effettuati nell'ambito della cooperazione transatlantica nell'attività di contrasto in materia penale. Sono quindi ricompresi i trasferimenti effettuati sulla base di legislazioni nazionali, accordi UE-Stati Uniti (ad esempio il Trattato UE-USA di mutua assistenza giudiziaria), accordi tra Stati membri e Stati Uniti (ad esempio, per il rafforzamento della cooperazione nella prevenzione e lotta delle forme gravi di criminalità e accordi sulle informazioni relative ai terroristi) e accordi specifici per il trasferimento di dati personali da parte di organizzazioni private per le finalità di contrasto della criminalità (ad esempio, PNR e TFTP).

L'art. 4 sancisce il principio secondo il quale ciascuna parte attuerà l'Accordo senza alcuna discriminazione arbitraria o ingiustificata tra i propri cittadini e quelli dell'altra parte. Come vedremo in seguito, tale principio è destinato a restare disatteso (almeno sul fronte statunitense),

dal momento che, solo per citare un esempio, le garanzie giurisdizionali fornite dal *Privacy Act* si applicheranno solo in parte ai cittadini europei.

L'art. 5 precisa il concetto – già implicito nell'art. 1 – per il quale il trattato ha lo scopo di integrare, ma non di sostituire, le previsioni concernenti la protezione dei dati personali contenute negli accordi internazionali stipulati tra le parti, aventi ad oggetto lo scambio di dati per finalità di contrasto della criminalità. Dispone, inoltre, che le parti adottino tutte le misure necessarie per implementare nella propria legislazione domestica le disposizioni dell'Accordo, con riferimento particolare alle previsioni concernenti i diritti delle persone fisiche. Tale sottolineatura si è resa necessaria, in quanto all'epoca della sua sottoscrizione (settembre 2015), gli Stati Uniti ancora non avevano adottato il *Judicial Redress Act*, che, come detto, estende alle *designated countries* le tutele giurisdizionali, di cui godono i cittadini americani rispetto agli abusi commessi da parte delle agenzie federali nell'ambito delle materie oggetto dell'Accordo.

Le Parti si danno reciproco atto che l'effettiva attuazione dell'Accordo quadro determinerà una presunzione di compatibilità con le norme applicabili in materia di trasferimenti internazionali di dati, ragion per cui non sarà più necessaria alcuna autorizzazione in futuro per il trasferimento dei dati da un continente all'altro. In realtà, come già evidenziato, esso non è uno strumento autonomo per il traferimento dei dati; pertanto, la presunzione di compatibilità opererà di volta in volta, in base alla valutazione del fatto che l'Accordo quadro e la base giuridica specifica del trasferimento, in combinato disposto, offrano un livello di protezione in linea con le norme UE sulla protezione dei dati. Resta, inoltre, fermo, in base al principio fissato dalla Corte di Giustizia nella sentenza *Schrems*, il potere dell'autorità di vigilanza del Paese membro di esercitare il controllo previsto dalla normativa UE e sollecitare la Corte di Giustizia alla verifica dell'effettivo livello di tutela offerto dal Paese terzo.

L'art. 6 fissa uno dei principi cardine in tema di trattamento dei dati personali, quello della limitazione delle finalità, in forza del quale il trattamento può avvenire solo per finalità esplicite e legittime nell'ambito del campo di applicazione dell'Accordo quadro. Tale principio si applica a tutti i trasferimenti di dati rientranti nel campo di applicazione del trattato: tanto a quelli in relazione a casi specifici, quanto a quelli eseguiti in base ad un'intesa che autorizza il trasferimento di dati personali in blocco concluso tra gli Stati Uniti e l'UE. Inoltre, l'ulteriore trattamento dei dati personali ad opera di un'autorità (di contrasto, regolamentare o amministrativa) diversa dalla prima autorità ricevente di una parte è ammesso a condizione che non sia incompatibile con le finalità per le

quali i dati sono stati originariamente trasferiti e che tale altra autorità rispetti tutte le altre disposizioni dell'Accordo quadro. Infine, le informazioni personali possono essere trattate solo in modo «direttamente pertinente e non eccessivo rispetto alle finalità del trattamento». L'articolo in oggetto garantisce che l'ambito di tutele, cui è soggetto il trasferimento dei dati tra i due continenti, non perda efficacia nei trasferimenti interni da un'autorità all'altra delle rispettive parti contraenti.

Preoccupazione analoga informa anche il successivo art. 7, in forza del quale l'ulteriore trasferimento ad un Paese terzo dei dati ricevuti in base all'Accordo deve essere subordinato al consenso dell'autorità che ha autorizzato il trasferimento originario. Tale principio – che si ritrova identico anche nel menzionato *Privacy Shield*, sul trasferimento dei dati personali in ambito commerciale – è statuito in modo che le garanzie previste dal trattato non vengano frustrate dal trasferimento ad un Paese terzo, che non vanti lo stesso livello di protezione dei dati personali fissato nell'intesa. In effetti, tra i fattori che l'autorità che ha effettuato il trasferimento originario dovrà tenere in conto al fine di autorizzare il trasferimento, oltre alla gravità dell'offesa e allo scopo per il quale i dati personali sono stati originariamente trasferiti, vi è il fatto che lo Stato terzo o l'organismo internazionale garantisca o meno un livello adeguato di protezione delle informazioni personali.

Gli articoli 9 e 10 affrontano il tema della sicurezza dei dati, prescrivendo che le parti adottino adeguate misure tecniche, organizzative e di sicurezza per proteggere le informazioni personali da distruzione accidentale o illecita, perdita accidentale e comunicazione, alterazione, accesso o altro trattamento non autorizzati. In caso si realizzi una di queste fattispecie, da cui derivi un rischio significativo di danni, devono essere prontamente adottati i provvedimenti opportuni per attenuare i danni, compresa la notificazione all'autorità competente del trasferimento e, ove opportuno in considerazione delle circostanze dell'incidente, alla persona in questione.

L'art. 12 disciplina la durata del periodo di conservazione dei dati personali, non determinando *a priori* un termine massimo di conservazione, ma lasciando alle parti la facoltà di specificare nelle rispettive legislazioni tale durata, al fine di non conservare i dati più a lungo di quanto necessario, secondo una valutazione effettuata in base ad alcuni elementi, quali, in particolare, la finalità del trattamento o dell'uso, la natura dei dati e l'impatto sui diritti e sugli interessi delle persone interessate. Tale previsione è destinata a produrre profonde divergenze di disciplina tra le parti, attesa la notevole difformità di approccio che contraddistingue le due sponde dell'Atlantico in merito alla congruità del

periodo di conservazione dei dati personali. In linea generale, le *policies* delle agenzie governative statunitensi prevedono un periodo massimo di conservazione dei dati di 5 anni[30]. Per altro verso, l'Accordo PNR tra Stati Uniti e UE per finalità di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi prevede – con un'evidente misura di compromesso – che i dati personali siano conservati per cinque anni in una banca dati attiva e per ulteriori dieci anni in una banca dati inattiva. Al contrario, la menzionata nuova direttiva 2016/681, che regola l'utilizzo dei dati del codice di prenotazione per finalità analoghe, prevede un periodo massimo di conservazione di cinque anni e la spersonalizzazione dei dati dopo sei mesi.

Come già ricordato, la Corte di Lussemburgo ha censurato la direttiva 2006/24/CE, in quanto in contrasto con il principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza. Uno dei punti sui quali si è soffermata la Corte nell'emettere il giudizio di non compatibilità della direttiva con i principi fondamentali UE riguardava proprio la durata di conservazione dei dati personali da parte delle società di telecomunicazione – da sei mesi a due anni – ritenuta eccessiva dalla Corte e non rispondente ad alcun criterio oggettivo ai fini della sua determinazione, tale da garantire la conservazione dei dati per il periodo strettamente necessario agli scopi perseguiti. Pertanto, considerata anche la stretta imposta dalla Corte di Giustizia, vi sono pochi dubbi che l'applicazione di tale articolo condurrà a risultati molto diversi.

L'art. 13 si preoccupa di definire le tutele da riservare ai dati sensibili, prescrivendo la possibilità di effettuare il trattamento di tali dati solo in presenza di garanzie adeguate ai sensi di legge (ad esempio il mascheramento dei dati dopo il conseguimento delle finalità per le quali sono stati trattati o l'obbligo di ottenere l'approvazione dell'autorità di controllo per accedere alle informazioni). Tuttavia, non pone il divieto per il trasferimento massivo dei dati sensibili, ma si limita a precisare che gli accordi che autorizzano tali trasferimenti dovranno specificare ulteriormente le norme e le condizioni per il trattamento di tali dati. La disposizione in esame si è discostata pertanto dal parere reso, in sede di valutazione preliminare dell'Accordo, dal Garante europeo della

[30] Si veda al riguardo il *report* dell'American Civil Liberties Union presentato al Parlamento tedesco il 5 settembre 2016, reperibile on line al sito https://www.bundestag.de/blob/439632/6c7f2de50e2016c9b8249ec351764e84/mat-a-sv-15-2-data.pdf

protezione dei dati[31] (GEPD), che aveva raccomandato che il trasferimento in blocco dei dati sensibili fosse escluso dal contenuto dell'intesa.

L'art. 15 dispone che il trattamento dei dati che può portare a decisioni aventi effetti negativi su una persona fisica (ad esempio nel contesto della profilazione) non può basarsi unicamente su un trattamento automatizzato delle informazioni personali, a meno che ciò non sia autorizzato da disposizioni di legge nazionali e purché sussistano garanzie adeguate, compresa la possibilità di ottenere l'intervento umano.

Gli articoli 16 e 17 prescrivono due facoltà a favore degli individui, che rientrano ormai da tempo nel novero dei diritti connessi alla piena esplicazione della tutela dei dati personali: il diritto all'accesso, consistente nella facoltà di chiedere e ottenere l'accesso ai propri dati personali e il diritto di rettifica, che autorizza ogni persona fisica a chiedere la correzione o la rettifica dei propri dati personali qualora siano inesatti o siano stati trattati impropriamente. Il diritto di accesso dell'interessato non è assoluto, in quanto l'autorità interrogata ha la possibilità di limitare tale accesso per salvaguardare la sicurezza pubblica e privata e per impedire l'ostruzione di indagini od investigazioni. L'Accordo prevede anche una modalità indiretta di accesso o di rettifica, consentendo all'interessato di rivolgere la propria richiesta non direttamente all'autorità interessata, ma ad un'autorità di supervisione (nel caso di un cittadino UE, all'autorità nazionale di protezione dei dati), agevolando in tal modo (almeno in teoria) la possibilità di avvalersi delle facoltà in questione. Se l'accesso o la rettifica sono negati o limitati, l'autorità interrogata fornirà una risposta illustrante i motivi del diniego o della limitazione dell'accesso o della rettifica, per consentire all'interessato il conseguente esercizio del diritto di proporre ricorso amministrativo o giurisdizionale.

A tal riguardo, gli articoli 18 e 19 definiscono i rimedi di natura amministrativa e giurisdizionale a disposizione del soggetto che non concordi con l'esito della propria domanda di accesso o di rettifica dei dati personali. L'art. 18 prevede pertanto che il soggetto abbia la possibilità di proporre ricorso amministrativo, anche per il tramite di un'autorità di supervisione, all'autorità competente secondo la legge dello Stato nel quale il ricorso è proposto, la quale dovrà inviare all'interessato una risposta scritta indicando, se del caso, le azioni

[31] Cfr. The European Data Protection Supervisor, *Opinion 1/2016 Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences,* in*: https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf*

migliorative o correttive adottate. L'art. 19 prevede che i cittadini di ogni parte abbiano il diritto di proporre ricorso giurisdizionale avverso il diniego dell'accesso, il diniego della rettifica o la diffusione illecita dei dati personali ad opera delle autorità dell'altra parte.

Al riguardo va sottolineato che, fino all'approvazione del *Judicial Redress Act*, un cittadino UE che subiva una lesione dei propri dati personali in territorio americano non aveva a disposizione gli stessi strumenti di tutela giurisdizionale di cui poteva avvalersi un cittadino statunitense, dal momento che il *Privacy Act* accordava le garanzie in esso previste esclusivamente ai cittadini americani e ai residenti permanenti.

L'introduzione di un rimedio giurisidizionale anche a favore dei cittadini europei rappresentava un requisito, alla cui adozione l'Unione Europea aveva espressamente subordinato la conclusione sia del *Privacy Shield* che dell'*Umbrella Agreement*[32]. Sembra, pertanto, opportuno precisare i contorni del JRA nell'ottica di comprendere se l'adozione di tale provvedimento risponda effettivamente alle aspettative dell'Unione Europea. Esso consente ad un cittadino di una *designated country* di proporre un'azione giudiziaria civile (sono esclusi, quindi, i rimedi di natura penale) «in the same manner, to the same extent, and subject to the same limitations» dei cittadini americani. Tuttavia, limita esplicitamente tale possibilità ai casi di divulgazione volontaria o intenzionale delle informazioni e ai casi in cui l'agenzia rifiuti di soddisfare la richiesta dell'individuo, ma non alle ipotesi di incompletezza, di mancata pertinenza dei dati conservati e di eccessiva durata di conservazione degli stessi. Tale esclusione deriva plausibilmente dalla volontà di non offrire un rimedio giurisdizionale avverso l'utilizzo da parte del governo americano di dati inesatti, incompleti o irrilevanti provenienti da soggetti esterni all'amministrazione pubblica, come ad esempio banche dati commerciali o *web companies*, in possesso di una mole smisurata di dati personali dei loro utenti [33].

Inoltre, il provvedimento non prevede la possibilità generalizzata di citare in giudizio qualsiasi agenzia federale, ma solo quelle oggetto di designazione da parte dell'*Attorney General*. Per le considerazioni appena esposte, non sembra dubitabile che il JRA rispecchi solo formal-

[32] Si vedano i punti 57 e BJ della risoluzione del Parlamento Europeo del 12 marzo 2014 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni [2013/2188(INI)], consultabile all'indirizzo: www.europarl.europa.eu.

[33] In tal senso si veda HASBROUCK, *Why the Judicial Redress Act is worthless,* in *Privacy Laws & Business International Report,* April 2016.

mente le richieste dell'Unione Europea, in quanto riduce ulteriormente la già minima tutela che il *Privacy Act* garantisce ai cittadini americani[34]. Il par. 3 dell'art. 19 precisa che l'estensione dei tre suddetti motivi di ricorso giurisdizionale non fa venir meno le altre vie di ricorso giurisdizionale altrimenti disponibili per quanto riguarda il trattamento dei dati (ad esempio ai sensi dell'*Administrative Procedure Act*, dell'*Electronics Communication Privacy Act* o del *Freedom of Information Act*), le quali, a differenza del JRA che si applica esclusivamente ai cittadini UE, sono a disposizione di tutte le persone interessate dal trasferimento dei dati a fini di contrasto, a prescindere dalla loro cittadinanza o luogo di residenza[35].

Gli articoli 21 e 22 prevedono una serie di disposizioni che disciplinano l'attività di supervisione da parte di organi indipendenti, a cui è attribuito il compito di verificare circa la corretta applicazione dell'Accordo quadro da parte delle autorità governative. Esse hanno il potere di ricevere e dar seguito ai reclami presentati da persone fisiche in merito alle misure di attuazione dell'Accordo quadro e di segnalare le violazioni di legge connesse a tale Accordo ai fini di un'azione giudiziaria o disciplinare. Mentre per l'UE tale attività di supervisione sarà esercitata dalle autorità di protezione dei dati, per gli USA l'attività stessa sarà attribuita ad un insieme di autorità di supervisione (tra cui i responsabili della protezione della vita privata, gli ispettori generali, le autorità per la tutela della vita privata e delle libertà civili), sulla cui effettiva indipendenza è lecito nutrire qualche dubbio, considerata la loro appartenenza all'esecutivo [36]. È inoltre previsto che le autorità di supervisione cooperino al fine di garantire l'attuazione efficace dell'Accordo quadro, in particolare per quanto riguarda il sistema di esercizio indiretto dei diritti delle persone fisiche relativi all'accesso, alla rettifica e al ricorso amministrativo.

L'art. 23 prevede un meccanismo di revisione congiunta dell'Accordo, con particolare riferimento all'esecuzione degli articoli riguardanti i diritti delle persone fisiche (accesso, rettifica, ricorsi amministrativo e giurisdizionale) e alla questione dei trasferimenti a enti territoriali non rientranti nel campo di applicazione dell'Accordo (ad esempio Stati federati degli USA). La prima verifica congiunta è

---

[34] Per una visione nettamente critica del provvedimento, cfr. BENDER, *The Judicial Redress Act: A Path to Nowhere,* in *Privacy Advisor*, 17 dicembre 2015.

[35] Sul punto v. BIGNAMI, *op.cit.,* la quale sottolinea la limitata tutela giurisdizionale offerta in tale ambito (anche agli stessi cittadini americani) dalla frammentaria normativa statunitense.

[36] SCHLANGER, *Offices of Goodness: Influence Without Authority in Federal Agencies*, in *Cardozo LR*, 2014, 52, 64.

effettuata entro tre anni dalla data di entrata in vigore dell'Accordo e quelle successive a scadenze regolari.

Completano l'Accordo le disposizioni dagli articoli 24 al 29, che prevedono, tra l'altro, la possibilità di ciascuna parte di sospendere l'Accordo in caso di violazione sostanziale dello stesso ad opera dell'altra parte (art. 26) e di denunciare l'Accordo mediante notificazione all'altra parte, fermo restando che le informazioni personali trasferite prima della denuncia continueranno ad essere trattate conformemente alle norme dell'Accordo quadro. L'art. 29 prevede l'entrata in vigore dell'Accordo il primo giorno del mese successivo alla data in cui le parti si sono scambiate le notificazioni di avvenuto espletamento delle rispettive procedure interne di approvazione. Al riguardo, con una dichiarazione congiunta[37], il 5 dicembre gli Stati Uniti e l'Unione Europea hanno confermato di avere completato le rispettive procedure interne di approvazione; con provvedimento del 17 gennaio 2017, *l'Attorney General* degli Stati Uniti ha designato gli Stati membri dell'Unione Europea e l'Unione Europea nella sua interezza, quali *designated countries* ai sensi del *Judicial Redress Act*, consentendo, di fatto, l'entrata in vigore dell'Accordo quadro il 1° febbraio 2017.

Va sottolineato che l'Attorney General ha proveduto altresì alla designazione delle agenzie federali, nei cui confronti potrà attuarsi la tutela giurisdizionale fornita ai cittadini comunitari dal JRA[38]. Si sono rivelati fondati i timori di chi ipotizzava una ristretta applicabilità della norma, dal momento che l'Attorney General ha indicato solo 4 agenzie federali (United States Department of Justice, United States Department of Homeland Security, United States Securities and Exchange Commission, United States Commodity Futures Trading Commission).

6. Unione Europea e Stati Uniti d'America hanno imboccato negli ultimi anni due strade sostanzialmente antitetiche circa i limiti cui sottoporre l'utilizzo della crescente quantità di dati personali a disposizione delle autorità pubbliche a seguito dell'incessante sviluppo delle comunicazioni elettroniche e dei *social network*. Il Governo americano ha adottato un approccio rivolto a consentire la prevalenza in ogni caso delle esigenze di sicurezza sui diritti di libertà dei cittadini – soprattutto non americani – approntando misure che consentono alle autorità di polizia l'accesso indiscriminato a tali dati. Al contrario, le istituzioni UE, intravedendo nella possibilità di fornire accesso alle autorità di polizia a tale quantità di informazioni il rischio di un'eccessiva

[37] Il testo della dichiarazione è disponibile su: europa.eu.
[38] Il provvedimento è reperibile su www.federalregister.gov.

ingerenza da parte dei governi nella vita dei cittadini, hanno subordinato tale potere ad una serie di limiti sempre più estesi e dettagliati.

L'Accordo quadro rappresenta un timido tentativo di riavvicinare le due posizioni, provando a creare uno spazio giuridico comune in cui i dati personali ricevano la stessa protezione, a prescindere dal territorio – Stati Uniti o Unione Europea – nel quale siano trattati.

L'Accordo ha il pregio di costruire uno *standard* minimo di garanzie, non derogabile *in peius* nella stipula dei futuri accordi tra le parti. Con alcune eccezioni, esso ricomprende i tradizionali principi che informano il corretto trattamento dei dati personali – pertinenza, necessità, finalità, lealtà, correttezza – dai quali non si può prescindere neanche in presenza di esigenze investigative o di repressione della criminalità. Esso istituisce inoltre un meccanismo di ricorso giurisdizionale a favore dei cittadini comunitari, applicabile anche agli accordi già stipulati in ambito di contrasto della criminalità, quali gli accordi PNR e TFTP.

Tuttavia, la delega eccessiva conferita alle rispettive legislazioni interne di tradurre in pratica i principi sanciti nell'intesa rappresenta il vero *vulnus* alla tenuta del sistema di garanzie approntate, consentendo di fatto una sostanziale elusione degli impegni assunti. A titolo esemplificativo, l'art. 19 precisa l'impegno delle parti a predisporre nel proprio ordinamento un complesso di tutele giurisdizionali avverso il diniego di accesso e di rettifica e contro le lesioni della privacy da parte delle agenzie governative. Gli Stati Uniti hanno tradotto in pratica tale impegno, emanando il *Judicial Redress Act*, di cui sono già stati evidenziati i notevoli limiti.

In tale ottica, assume ancora più rilievo l'atteggiamento che assumerà la nuova Presidenza degli Stati Uniti nei confronti del tema della *privacy* e dei diritti ad essa connessi. A giudicare dalle prime mosse, i segnali non sono incoraggianti. A differenza del suo predecessore Obama, che aveva indirizzato l'azione del governo una maggiore tutela dei dati personali, Donald Trump ha lasciato subito intravedere la volontà di ridurre le tutele connesse alla *privacy* dei cittadini (almeno dei non americani), stabilendo, con uno dei suoi primi ordini esecutivi[39], che le agenzie federali si assicurino che le loro privacy *policy* escludano tutti i soggetti che non siano cittadini USA o residenti permanenti dalla protezione del *Privacy Act.* Pur essendo privo di riflessi

[39] L'art. 14 dell'*Executive Order* n. 13768, *Enhancing Public Safety in the Interior of the United States*", emesso il 25 gennaio 2017, così dispone: «Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information».

diretti sull'*Umbrella Agreement* – in quanto l'estensione delle garanzie del *Privacy Act* ai cittadini comunitari è garantita dal JRA – tale provvedimento sottintende l'intenzione dell'Amministrazione americana di subordinare i diritti di libertà dei cittadini non americani alle esigenze di sicurezza nazionale.

In definitiva, l'*Umbrella Agreement*, troppo esposto alle volubili inclinazioni del potere politico, non appare in grado di assicurare un livello di protezione uniforme ed elevato dei dati personali, in considerazione del carattere piuttosto lasco delle sue disposizioni che legittima interpretazioni difformi dell'Accordo in fase applicativa.

È appena il caso di aggiungere che le considerazioni appena esposte inducono forti timori circa la resistenza dell'Accordo ad un eventuale vaglio da parte della Corte di Giustizia UE.

Come già evidenziato, l'articolo 37 della direttiva 2016/681 prevede che gli Stati membri dispongono il trasferimento di dati personali verso un Paese terzo se sono fornite garanzie adeguate per la protezione dei dati personali in uno strumento giuridicamente vincolante. Qualora in sede di esecuzione dell'intesa le divergenze normative tra le parti dovessero ampliarsi, la Corte di Giustizia UE, in caso fosse chiamata a pronunciarsi sulla conformità del trattato *all'acquis* comunitario, potrebbe adottare una decisione analoga a quella resa nella sentenza *Schrems*, dichiarando l'annullamento dell'Accordo per incompatibilità con la predetta norma.

ABSTRACT

The US-EU Umbrella Agreement on Data Protection Rights in Law Enforcement Cooperation

This contribution focuses on the recent framework agreement called "Umbrella Agreement" between the European Union and the United States, dealing with the personal data transfer with the aim of fighting crime.

After briefly summarizing the law system of the relevant contracting parties concerning the purpose of the agreement, this paper describes its main provisions, aiming at verifying if its purpose has been actually achieved, that is, to enact a high and uniform protection level of personal data and to enhance cooperation between the United States and the European Union in matter of prevention, investigation and prosecution of criminal offence.