Giorgio Resta

La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE

Sommario: Introduzione. – 1. Le rivelazioni di Snowden e lo scandalo *NSA*. – 2. L'infrastruttura giuridica dei programmi di sorveglianza elettronica: il quadro costituzionale. – 3. (*Segue*): le regole di dettaglio. – 4. Il conflitto regolatorio USA/EU nella materia dei dati personali. – 5. La prospettiva della Corte di Giustizia: da *Digital Rights* a *Schrems*. – Conclusioni.

Introduzione

La decisione della Corte di Giustizia nel caso *Schrems c. Data Protection Commissioner* può essere considerata, se non un *leading case,* certamente uno dei precedenti più rilevanti nell'ambito della recente giurisprudenza europea in tema di diritti fondamentali. Per apprezzarne compiutamente il significato e le implicazioni, è necessario ricostruire, sia pure per grandi linee, il contesto politico e giuridico nel quale essa si inserisce. Su un piano 'micro' essa rappresenta l'ultimo tassello di un mosaico di pronunzie particolarmente innovative, tutte concernenti la tutela della riservatezza e dei dati personali, composto (per limitarsi alle principali)[1] dalle decisioni *Google Spain*[2]*, Digital Rights*[3] e per l'appunto *Schrems*[4]. Pur affrontando

[1] Ma per una disamina più dettagliata e completa si rinvia al contributo di G. Finocchiaro*, La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, *infra* in questo Volume.

[2] Corte di giustizia, *infra* 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12; la decisione è pubblicata in *Dir. Inf.* 2014, 535, con molteplici commenti; v. anche G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

[3] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources*, cause riunite C-293/12 e C-594/12, in *Dir. Inf.* 2014, 851, con nota di S. Scagliarini, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni* pro *e alcuni* contra; e in *Nuova giur. civ. comm.,* 2014, I, 1044, con nota di C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di giustizia e gli echi del Datagate*.

[4] Corte di giustizia, Grande Sezione, 6 ottobre 2015, causa C-362/14, *Maximilian*

questioni diverse, ciascuna di esse offre un significativo contributo alla ridefinizione dello statuto dei dati personali nell'epoca dei *big data* e della 'sorveglianza liquida'[5]. Su un piano 'macro' essa costituisce uno specifico sviluppo del conflitto regolatorio, che ha diviso l'Unione Europea e gli Stati Uniti sin dall'entrata in vigore della direttiva 95/46/CE; conflitto che è deflagrato nel periodo 2013-2015, a seguito delle rivelazioni di Edward Snowden circa i programmi di sorveglianza di massa posti in atto dalle agenzie di informazione e sicurezza statunitensi (spesso in cooperazione con le omologhe agenzie europee)[6]. Offrire una lettura puramente 'interna' della pronunzia *Schrems*, che prescinda dalla considerazione di questi dati di contesto, rischierebbe di falsare i risultati dell'interpretazione. Queste pagine vorrebbero quindi soffermarsi piuttosto sulle premesse che non sulle implicazioni della decisione, guardando alla controversia *Schrems* come il prevedibile punto di sbocco di due principali situazioni di conflitto: da un lato quello, esogeno, tra il modello europeo e il modello statunitense di tutela della riservatezza; dall'altro quello, endogeno, tra le politiche della sicurezza e le garanzie costituzionali dei diritti di libertà.

1. Le rivelazioni di Snowden e lo scandalo NSA

Com'è noto, i documenti diffusi da Snowden e pubblicati dal *Guardian* e dal *Washington Post* nel giugno 2013 hanno disvelato i lineamenti essenziali dei programmi di sorveglianza di massa posti in essere dalle agenzie di *intelligence* statunitensi a seguito degli attacchi terroristici dell'11 settembre[7]. Si tratta di programmi che prevedono la raccolta su ampia scala

Schrems c. Data Protection Commissioner [Ireland], supra in questo Volume.

[5] Secondo la suggestiva formula di Z. Bauman – D. Lyon, *Liquid Surveillance,* Cambridge, 2012.

[6] In tema sia consentito rinviare a F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* 78 *Law & Cont. Prob's* 101 (2015); cfr. inoltre G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU,* in *Dir. Inf.* 2014, 657.

[7] Per un quadro di sintesi v. C. Bowden, *The U.S. Surveillance Programmes And Their Impact On EU Citizens' Fundamental Rights* (2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf [ultimo accesso 12.7.2016]; sul problema dei rapporti con i programmi di sorveglianza europei v. D. Bigo et al., *National Programs for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law,* (2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

di informazioni e dati personali degli utenti di servizi di telecomunicazione statunitensi e stranieri. Tale raccolta e il successivo trattamento non avvengono in maniera mirata, secondo il modello tradizionale di «small data», ma rispondono in prevalenza alla logica dei *big data*: acquisizione su larga scala e in maniera automatica dei dati, conservazione per un lungo periodo di tempo, integrazione con altre banche dati e analisi attraverso potenti elaboratori elettronici dell'intero compendio informativo, con l'obiettivo di ricavarne inferenze statisticamente rilevanti per fini di «foreign intelligence»[8].

In particolare, le modalità principali di acquisizione di tali informazioni – secondo la configurazione originaria dei programmi in oggetto – sono due: *a*) l'intercettazione diretta del flusso di comunicazioni telefoniche e telematiche veicolato attraverso le reti statunitensi (programma UPSTREAM); *b*) l'accesso sistematico ai dati di traffico degli utenti, conservati nelle banche dati tenute dai maggiori fornitori di servizi di telecomunicazione e contenuti multimediali (quali Facebook, Google, Twitter, etc.) operanti negli USA (programma PRISM). Una volta acquisite, tali informazioni sono immesse in uno o più *database*, conservate per un ampio lasso temporale (generalmente 5 anni) e rese disponibili per ricerche mirate tramite appositi 'puntatori'[9]. Elementi connotativi di tali programmi sono: la segretezza (atteso che anche i provvedimenti giurisdizionali che autorizzano l'acquisizione presso terzi di dati e informazioni sono coperti dal vincolo di segreto)[10]; il carattere sistematico ed indiscriminato della raccolta (oggetto di raccolta e conservazione sono dati e metadati relativi a qualsiasi cittadino, indipendentemente dall'esistenza di indizi di reato)[11]; il raggio transfrontaliero delle operazioni di sorveglianza (interessati non sono soltanto i cittadini e i residenti sul territorio USA,

[ultimo accesso 12.7.2016].

[8] La differenza tra le tecniche di *small data* e *big data surveillance* è sintetizzata in maniera particolarmente nitida da M. Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, in 42 *Pepp. L. Rev.* 773 (2015).

[9] Per i dettagli tecnici v. D.S. Kris, *On the Bulk Collection of Tangible Things*, in 7 *J. Nat'l Security L. & Pol'y* 209 (2014); nonché C. Comella, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza «Safe Harbor» della Corte di giustizia dell'Unione Europea, infra* in questo Volume.

[10] IIn tema v. S. Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, in 51 *Stan. J Int'l L.* 69 (2015).

[11] M. Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, cit.; L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 *Harv. J.L. & Pub. Pol'y* 757 (2014).

ma anche gli stranieri)[12].

All'indomani della rivelazione dell'esistenza dei programmi di sorveglianza elettronica di massa, si è sviluppato negli Stati Uniti un ampio e articolato dibattito circa i limiti di legittimità e compatibilità democratica delle suddette attività. Rapporti di studio sono stati elaborati ad opera di diversi *think tank*, tra i quali su posizioni particolarmente critiche quello del *Brennan Center*[13], nonché di commissioni governative e parlamentari, tra le quali il *President's Review Group on Information and Communication Technologies*[14] e il *Privacy and Civil Liberties Oversight Board*[15]. Progetti di riforma sono stati presentati in Congresso e uno dei più importanti di essi, il US Freedom Act (*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015*), approvato nel giugno 2015[16]. Lo stesso Presidente degli Stati Uniti ha disposto il mutamento delle procedure di *signal intelligence,* attraverso la *Presidential Policy Directive - PPD28* del Gennaio 2014[17]. Tuttavia, il tema al centro della discussione pubblica è stato, almeno sino a pochi mesi fa, quello della compatibilità dei sistemi di *bulk collection* dei dati personali con il quadro delle *American liberties,* ove il termine «American» sta ad indicare

[12] V. ad es. P. Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism,* 82 *Fordham L. Rev.* 2137 (2014).

[13] *What Went Wrong with the FISA Court*, Brennan Center for Justice at New York University School of Law (2015).

[14] President's Review Group on Information and Communication Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Recommendation*, Recommendation 13, 12 dicembre 2013.

[15] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 luglio 2014.

[16] In base alla suddetta normativa, il programma di raccolta di massa di metadati telefonici da parte dell'NSA è d'ora in avanti abolito e sostituito da un meccanismo di *data retention* da parte dei providers di telecomunicazioni, ai quali le autorità competenti potranno rivolgersi per ottenere selettivamente l'accesso ai dati necessari per finalità di tutela della sicurezza nazionale; inoltre, si prevede che i destinatari di un ordine di esibizione dei metadati non siano vincolati ad un obbligo assoluto di non divulgazione e che i provvedimenti della FISC court siano soggetti, previo apposito filtro governativo, a un regime di pubblicità (per un'analisi dettagliata v. P. Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013,* Georgia Tech. Scheller College of Business Research Paper n. 36, December 18 2015, in http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2709619 [ultimo accesso 12.7.2016].

[17] Presidential Policy Directive - Signals Intelligence Activities, Jan. 17, 2014, accessibile all'indirizzo http:// www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [ultimo accesso 12.7.2016].

non soltanto il contenuto sostanziale delle libertà in oggetto[18], quanto soprattutto la nazionalità dei loro titolari. Infatti, l'attenzione dei cittadini, dei commentatori e dei giuristi, si è appuntata in maniera pressoché esclusiva sul problema della tutela dei diritti fondamentali dei cittadini statunitensi rispetto alle suddette pratiche di controllo di massa. Per contro, la questione della sfera privata degli stranieri è rimasta sullo sfondo, essendo destinata a riemergere soltanto quando le esigenze di 'normalizzazione' dei rapporti politici e soprattutto commerciali (in vista della finalizzazione delle negoziazioni per il TTIP) con l'Unione Europea hanno spinto all'approvazione del *Judicial Redress Act,* del quale si dirà meglio in seguito. Ciò, sia chiaro, era del tutto prevedibile, data la natura della posta in gioco e la delicatezza del tema del contrasto al terrorismo internazionale[19], oltre che la visione particolarmente 'insulare' che gli USA hanno sempre mantenuto sul tema del rispetto dei diritti umani. Una serie di interrogativi meritano però di essere sollevati, quanto meno per comprendere la natura e le implicazioni del conflitto sotteso alla decisione *Schrems*.

In base a quali presupposti le autorità federali hanno avuto accesso quotidianamente, per diversi anni, ad una mole immensa di dati relativi al traffico telefonico e Internet di cittadini (statunitensi e) stranieri? È ciò avvenuto in conformità o in violazione del quadro normativo interno o sovranazionale? Come affrontare nel futuro casi simili, indipendentemente dalle risposte che possano derivare dal quadro degli eventuali accordi bilaterali?

2. L'infrastruttura giuridica dei programmi di sorveglianza elettronica: il quadro costituzionale

Sembra si possa affermare, sulla scorta dei risultati ai quali sono pervenute diverse commissioni d'indagine, che il meccanismo di sorveglianza elettronica posto in essere dalle agenzie di sicurezza statunitensi non ha operato al di fuori dei circuiti della legalità, ma ha sfruttato alcune falle, o meglio alcune caratteristiche distintive, del regime statunitense di tutela

[18] Secondo l'accezione del sintagma fatta propria, ad esempio, da F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* in 48 *Bost. Coll. L. Rev.* 609 (2007).

[19] Cfr. F. Resta, *11 Settembre: attentato alle libertà? I diritti umani dopo le Torri Gemelle,* Roma, 2011.

della riservatezza[20]. Ferme restando alcune zone grigie di dubbia qualificazione, rispetto alle quali è tuttora aperto il contenzioso[21], il livello capillare di interferenza con la sfera privata non appare imputabile ad un abuso dei poteri pubblici (che potrebbe far pensare ad un nuovo *Watergate*), quanto piuttosto alle caratteristiche intrinseche del sistema normativo. L'architettura giuridica del sistema della sorveglianza elettronica post-11 settembre risulta, infatti, connotata da una notevole porosità e, specie là dove oggetto delle operazioni di intelligence siano le comunicazioni che coinvolgano almeno uno straniero, preordinata a una netta prevalenza del polo del controllo su quello della riservatezza. Ciò si evince non soltanto da un'analisi delle principali fonti in materia – il *Foreign Intelligence Surveillance Act*, il *Patriot Act* e l'*Executive Order* n. 12333 – ma anche del quadro delle regole costituzionali che di tali fonti rappresentano la griglia ordinante.

Prendendo le mosse proprio dal livello delle garanzie costituzionali, vi sono almeno tre elementi che meritano di essere segnalati, i quali riducono ad ambiti piuttosto ristretti il perimetro della tutela riconosciuta ai destinatari, e segnatamente agli stranieri, dei programmi di controllo.

In primo luogo sussiste una netta diversificazione del regime applicabile – ai sensi del Quarto Emendamento della Costituzione USA – alle interferenze con la sfera privata dettate, rispettivamente, da esigenze di contrasto della criminalità ordinaria e di protezione della sicurezza nazionale[22]. L'esistenza di un doppio binario è affermata dalla Corte Suprema sin dal celebre caso *United States v. United States District Court* (noto come Keith case)[23], nel quale si dibatteva dell'utilizzabilità di intercettazioni telefoniche disposte, senza previa autorizzazione dell'autorità giudiziaria,

[20] V. ad es. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* 21 *Mich. Telecomm. Tech. L. Rev.* 317, 358 (2015)

[21] Si veda in particolare la questione relativa alla compatibilità del programma di *bulk data collection* adottato ai sensi della Sect. 215 Patriot Act con il Quarto Emendamento: i casi più rilevanti in materia, i quali pervengono a conclusioni difformi, sono costituiti da *Obama v. Klayman,* 14-5004, U.S. Court of Appeals, District of Columbia Cir. (Aug. 2015); *Klayman v. Obama*, 957 F. Supp. 2d 1, 29 (D.D.C. 2013); *ACLU v. Clapper,* 14-42-cv, U.S. Court of Appeals, 2nd Cir. (May 2015); *ACLU v. Clapper*, F. Supp. 2d 724 (S.D.N.Y. 2013).

[22] F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* Bruxelles, 2015, 20; Id., *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* cit., 620-621.

[23] *United States v. United States District Court*, 407 U.S. 297 (1972).

nei confronti di alcuni membri del gruppo estremistico «White Panters», accusati di un attacco alla sede della CIA. La Corte ha tracciato una netta distinzione tra le intercettazioni disposte, da un lato, per finalità di prevenzione e repressione dei reati 'ordinari' e, dall'altro, per finalità di tutela della «sicurezza nazionale» [24]. Queste ultime troverebbero la loro legittimazione nella prerogativa costituzionale del Presidente di «preservare, proteggere e difendere la Costituzione degli Stati Uniti» e dovrebbero ritenersi preordinate a «proteggere il sistema costituito contro l'azione di coloro, i quali vorrebbero sovvertirlo o rimuoverlo attraverso mezzi illeciti». Tuttavia, 'sicurezza nazionale' è un concetto che la Corte circoscrive distinguendo due diverse ipotesi: *a*) la sicurezza nazionale nei suoi aspetti 'domestici' (protetta cioè nei confronti delle azioni eversive di gruppi interni); *b*) la sicurezza nazionale 'esterna' (rilevante nei confronti delle minacce provenienti da potenze straniere o da loro agenti). Le fattispecie rilevanti *sub a*), tra le quali il caso di specie, rientrerebbero nell'ambito oggettivo di applicazione del Quarto Emendamento, con la conseguente necessità del previo mandato giudiziario, assistito dal ragionevole sospetto della commissione di un reato. Le ipotesi rilevanti *sub b)* ne resterebbero fuori, non suscitando particolari preoccupazioni in termini di possibili abusi del potere esecutivo, a danno della libertà dell'espressione e del corretto funzionamento dei circuiti democratici[25]. Dunque, benché la Corte abbia lasciato aperto l'interrogativo concernente le eventuali salvaguardie da adottare nell'ambito delle operazioni di *foreign intelligence*, si è eliminato qualsiasi dubbio circa la duplicità del regime giuridico di riferimento, più garantistico nei casi di rischi per la *domestic security*; meno garantistico, invece, nei casi di minacce alla sicurezza nazionale provenienti dall'esterno.

In secondo luogo, l'ambito soggettivo di operatività del Quarto Emendamento risulta strutturalmente limitato per effetto della distinzione tra cittadini (ivi compresi i residenti permanenti) e stranieri. In particolare, sin dal caso *United States v. Verdugo-Urquidez*[26], recentemente richiamato in maniera adesiva in *Clapper v. Amnesty International USA*[27], la Corte Suprema ha affermato l'applicabilità del Quarto Emendamento a tutte le fattispecie di perquisizione e sequestro all'interno del territorio nazionale, indipendentemente dalla nazionalità dei soggetti coinvolti.

[24] L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits,* 66 *Vand. L. Rev.* 1343, 1381 (2013).
[25] F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 20.
[26] *United States v. Verdugo-Urquidez*, 494 U.S. 1092 (1990).
[27] *Clapper v. Amnesty International USA*, 133 Sup. Ct. 1138, 1154 (2013).

Pertanto, si tratti di cittadini statunitensi, o di stranieri presenti a qualsiasi titolo sul suolo americano, le garanzie sancite dal Quarto Emendamento devono ritenersi comunque operanti. Per contro, qualora le ingerenze con la sfera privata si realizzino al di fuori del territorio nazionale, il Quarto Emendamento potrà essere invocato unicamente da quella «classe di persone che siano parte della comunità nazionale o che abbiano altrimenti sviluppato legami sufficienti con questo paese, tali da farle considerare parte integrante di tale comunità» [28]. Innestandosi all'interno del dibattito se la «costituzione segua la bandiera»[29], la questione dell'applicabilità extraterritoriale del diritto alla *privacy* (nei limiti della tutela offerta dal Quarto Emendamento) è stata dunque risolta dalla Corte nel senso più restrittivo[30]. Di conseguenza, mentre la cittadinanza è un criterio irrilevante ai fini del giudizio sulla legittimità di perquisizioni e sequestri condotti sul territorio USA, essendo tali atti comunque soggetti al rispetto dei vincoli costituzionali, essa opera come parametro identificativo della disciplina applicabile in tutte le ipotesi di azione extraterritoriale. Ne deriva che le intercettazioni condotte «al di fuori del territorio nazionale» ricadono nell'area di operatività del Quarto Emendamento unicamente nel caso in cui i soggetti coinvolti siano cittadini USA o a questi equiparabili. Per contro, qualora si tratti di stranieri, il Quarto Emendamento non sarebbe applicabile, in quanto norma strutturalmente preordinata alla tutela del popolo americano [31]. Ovviamente va chiarito, e sul punto si tornerà in seguito, in che modo si debba esattamente declinare la nozione di 'territorio' rispetto ad atti e rapporti condotti nella virtualità delle reti telematiche, e pertanto connotati da una specifica attitudine a-territoriale[32]. Resta fermo, comunque, che, pur soggetta a notevoli incertezze di ordine applicativo, tale diversificazione tra i regimi di tutela possiede un rilevante valore simbolico e di orientamento ermeneutico.

[28] *United States v. Verdugo-Urquidez*, cit., 265-268.

[29] K. Raustiala, *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law*, Oxford, 2009.

[30] Per un'analisi approfondita di questi aspetti v. M. Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,* in corso di pubblicazione in *Harv. Int. L.J.,* (2014) accessibile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485 [ultimo accesso 12.7.2016].

[31] Tale regola di esclusione è rimarcata e difesa con argomenti non incontroversi da J. Yoo, *The Legality of National Security Agency's Bulk Data Surveillance Programs*, 37 *Harv. J. L. & Pub. Pol'y* 901, 919 (2014).

[32] Cfr. in tema J. Daskal, *The Un-Territoriality of Data*, di prossima pubblicazione in *Yale L.J.* (2015/16) e accessibile all'indirizzo http://insct.syr.edu/wp-content/uploads/2015/06/Daskal_Un-Territoriality_of_Data.pdf [ultimo accesso 12.7.2016].

In terzo luogo, il raggio applicativo del Quarto Emendamento si rivela alquanto ridotto anche sul piano oggettivo. Ciò è la conseguenza della ben nota *third-party doctrine*, fatta propria (e non ancora formalmente abbandonata) dalla Corte Suprema USA sin dai casi *United States v. Miller*[33] e *Smith v. Maryland*[34]. Essa verte sull'interpretazione della «reasonable expectation of privacy» quale coelemento della fattispecie di tutela della riservatezza ai sensi del Quarto Emendamento. Non vi sarebbe «reasonable expectation of privacy», ad avviso della Corte, qualora le informazioni in oggetto siano nella disponibilità di un terzo, che le ha originate o conservate in maniera strumentale al perseguimento di propri interessi, come nel caso della banca rispetto ai dati bancari e del fornitore di servizi di telecomunicazioni rispetto ai dati di traffico[35]. Ciò è coerente con il fondamentale asse «inside-outside», che struttura la logica statunitense tradizionale di tutela della riservatezza[36] e che induce alla conclusione che l'accesso da parte dei poteri pubblici alle informazioni volontariamente condivise con terzi non è subordinato agli stringenti requisiti posti dal Quarto Emendamento. Le ricadute di tale modello in ordine al problema della sorveglianza elettronica sono di immediata evidenza: l'acquisizione da parte delle autorità governative dei dati di traffico (ma non dei contenuti) in possesso dei fornitori dei servizi di telecomunicazione sarebbe sottratta al rispetto dei vincoli del mandato giudiziario e della *probable cause*[37].

3. (Segue): Le regole di dettaglio

Le premesse costituzionali appena illustrate appaiono oggi molto più controverse e meno univoche di quanto non fosse in passato. In particolare, la de-materializzazione dei rapporti indotta dalla sinergia tra digitalizzazione e interconnessione attraverso le reti telematiche ha revocato in dubbio molti dei presupposti fattuali sui quali si reggeva la lettura

[33] *United States v. Miller,* 425 U.S. 435, 443 (1976).
[34] *Smith v. Maryland*, 442 U.S. 735, 744–46 (1979).
[35] J.T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?,* in 74 *Fordham L. Rev.* 1731, 1743-1745 (2006).
[36] O.S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach,* in 62 *Stanford L. Rev.* 1005, 1009-1011 (2010).
[37] M. Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply,* in 54 *B.C.L. Rev.* 1, 12-17 (2013); F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 10.

tradizionale del Quarto Emendamento. Tra questi le dicotomie interno/esterno (sfera domestica di *privacy* / dati pubblici) e territorialità/extraterritorialità[38]. La recente controversia che ha contrapposto il governo USA e la società Microsoft, a proposito dell'ordine di esibizione di dati personali relativi a un soggetto privato e fisicamente archiviati in un server ubicato in Irlanda, ha evidenziato quanto siano labili i confini tra la nozione di accesso territoriale e accesso extraterritoriale nello spazio virtuale definito dalle reti telematiche[39]. Di qui le varie proposte di riforma avanzate in dottrina, tra cui quella, molto radicale, formulata da Orin Kerr e consistente nella sostituzione del criterio della nazionalità a quello della territorialità, come presupposto per l'applicazione del Quarto Emendamento[40]. Inoltre, la *third party doctrine* è stata fatta oggetto di numerose critiche, poiché inidonea a governare i nuovi fenomeni comunicativi dell'era digitale[41]. Alcune di queste critiche hanno peraltro trovato uno sbocco giudiziario, inducendo alcune corti ad affermare l'incompatibilità dei programmi di raccolta di massa dei dati di traffico con i principi costituzionali, e segnatamente con il Quarto Emendamento, interpretato in maniera più liberale rispetto alla risalente giurisprudenza della Corte Suprema[42]. Nonostante tali crepe siano profonde e verosimilmente destinate a espandersi, sta di fatto che gli equilibri definiti a livello costituzionale si sono fedelmente riprodotti anche sul piano delle regole di settore adottate negli anni '70 e profondamente rimaneggiate nel periodo successivo agli attacchi terroristici dell'11 settembre 2001[43].

Innanzitutto la disciplina dei programmi di sorveglianza per finalità di tutela della sicurezza nazionale segue fedelmente il doppio binario tracciato dalla Corte Suprema tra *law enforcement* e *foreign intelligence*.

[38] Sui due aspetti v. rispettivamente O.S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach,* cit.; O. S. Kerr, *The Fourth Amendment and the Global Internet,* 67 *Stan. L. Rev.* 285 (2015).

[39] *In re Microsoft*, 15 F. Supp. 3rd 466 (S.D.N.Y 2014).

[40] O. S. Kerr, *The Fourth Amendment and the Global Internet,* cit., 303-304.

[41] Tra i tanti v. M. Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply,* cit., spec. 50 ss.

[42] V. ad es. la decisione di primo grado nel caso *Klayman v. Obama*, 957 F. Supp. 2d 1, 29 (D.D.C. 2013); e, seppur fondata su argomenti diversi da quelli relativi alla costituzionalità del programma di intelligence, *ACLU v. Clapper,* 14-42-cv, U.S. Court of Appeals, 2nd Cir. (May 2015) (su cui M. Catanzariti, *ACLU v. Clapper: una nuova stagione per il right to privacy?,* in *Costituzionalismo.it,* n. 2/2015, http://www.costituzionalismo.it/articoli/526 [ultimo accesso 12.7.2016].

[43] Per un quadro di sintesi v. M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* in *Dir. umani e dir. int.*, 2013, 727, 733 ss.

Le due principali fonti normative in materia, ossia il *Foreign Intelligence Surveillance Act* (promulgato nel 1978, a seguito degli scandali emersi durante la presidenza Nixon)[44] e l'*Executive Order* 12333[45] (adottato dal Presidente Reagan nel 1981) si occupano esclusivamente della *foreign surveillance,* dettando un sistema di controllo che prescinde dalle garanzie iscritte nel Quarto Emendamento e dalle altre regole poste per la sorveglianza per finalità di *law enforcement* contenute nell'*Electronic Communications Privacy Act*[46]. Mette conto chiarire che la nozione di 'foreign' si articola diversamente nelle due ipotesi normative: la prima ha una connotazione soggettiva, in quanto copre prevalentemente le attività di sorveglianza mirate a soggetti stranieri, benché effettuate sul suolo americano; la seconda una connotazione oggettiva, in quanto pertiene alle attività di *intelligence* condotte all'estero[47].

In secondo luogo, la disciplina in esame riproduce e accentua il divario di tutela tra cittadini e stranieri fatto proprio dalla giurisprudenza costituzionale[48]. Le garanzie previste nel FISA appaiono essenzialmente preordinate, da un lato, a evitare che le attività di sorveglianza siano disposte per contrastare minacce puramente domestiche, rispetto alle quali rimane applicabile il sistema ordinario e, dall'altro, a far sì che la *privacy* e gli altri diritti fondamentali dei cittadini statunitensi accidentalmente caduti nella rete della sorveglianza siano adeguatamente tutelati. Ciò si ricava testualmente dal § 702 FISA[49], nella sua versione modificata a seguito del *Patriot Act*, ove si prevede che l'*Attorney General* e il *Director of National Intelligence* possono autorizzare la sorveglianza di persone «ragionevolmente ritenute al di fuori del territorio degli Stati Uniti al fine di acquisire *foreign intelligence information*». Tra le limitazioni espressamente previste si

[44] Per la ricostruzione storica v. L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 *Harv. J.L. & Pub. Pol'y* 757, 766-782 (2014).

[45] Per approfondimenti v. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* cit., 321 ss.

[46] In tema F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* cit., 626; A.K. Chhabra, *Fisa Surveillance and Aliens,* 82 *Fordham L. Rev. Res Gestae* 17, 23 (2014); M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* cit., 734.

[47] A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* cit., 329-335.

[48] Sul punto v. A.K. Chhabra, *Fisa Surveillance and Aliens,* cit., 20; K. Lachmayer – N. Witzleb, *The Challenge to Privacy From Ever-Increasing State Surveillance: A Comparative Perspective,* 37 U.N.S.W. L.J. 748, 764 (2014).

[49] 50 U.S.C. § 1881a..

annoverano il divieto di sottoporre intenzionalmente a sorveglianza individui presenti al momento dell'acquisizione all'interno del territorio degli Stati Uniti, ovvero soggetti che si trovino al di fuori dei confini nazionali, ma siano «US persons» (cittadini e residenti permanenti); inoltre si prescrive l'adozione di procedure di «minimizzazione», con l'intento di evitare l'intercettazione delle comunicazioni relative a cittadini statunitensi e assicurare in ogni caso il rispetto dell'interesse alla *privacy* e alla libertà d'espressione di cui al Primo Emendamento[50]. Del pari, il secondo schema normativo di maggior rilevanza, quello delineato dal § 215 *Patriot Act*[51], contrappone nettamente il regime dell'acquisizione di *foreign intelligence information* concernente rispettivamente soggetti stranieri e cittadini americani. In quest'ultimo caso si prevede che l'ordine di esibizione (e segnatamente l'ordine di produrre «any tangible things») contemplato dalla norma in oggetto possa essere emesso soltanto nel quadro di investigazioni volte a contrastare il terrorismo internazionale o attività clandestine di spionaggio, sempre che ciò non avvenga esclusivamente sulla base di attività protette dal Primo Emendamento della Costituzione federale[52]. In entrambi i casi, quindi, la tutela accordata dal Primo Emendamento opera come un fattore conformativo della disciplina dell'attività di *intelligence* soltanto a beneficio dei soggetti di nazionalità statunitense, poiché si intende evitare che dietro lo schermo della tutela della sicurezza si celi un'attività repressiva del dissenso democratico[53]. Il rispetto della libertà di parola e di pensiero non vale, però, in questo contesto, a favore degli stranieri[54]. A ciò si aggiunga che – a differenza di quanto avviene nel sistema definito dalla direttiva 95/46/CE – la stessa normativa generale sul trattamento dei dati personali nel settore pubblico, il *Privacy Act* del 1974, si applica unicamente ai cittadini americani e agli stranieri ammessi con lo status di residente permanente[55]. Di riflesso le *non-US persons* sono normativamente collocate all'interno di uno spazio ben poco presidiato

[50] L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* cit., 791..
[51] 50 U.S.C. § 1861. In tema v. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* cit., 326; F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 24.
[52] L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* cit., 802.
[53] A.K. Chhabra, *Fisa Surveillance and Aliens*, cit., 20.
[54] A.K. Chhabra, *Fisa Surveillance and Aliens*, cit., 24.
[55] 5 U.S.C. § 552a (a) 2; sul punto v. F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 12..

sul piano dei meccanismi di garanzia e degli strumenti di tutela (i quali non sono completamente assenti, ma limitati a singoli settori, come quello presidiato dall'*Electronic Communications Privacy Act*[56]). Infine, l'interpretazione fornita dalla *Foreign Intelligence Surveillance Court* dei presupposti e del contenuto dell'ordine di esibizione previsto dal § 215 *Patriot Act* sembra confermare il regime di tutela affievolita per i metadati, implicito nella già illustrata *third-party doctrine*. Nel momento in cui la corte ritiene sufficiente emettere un unico provvedimento per legittimare una raccolta in massa e su base giornaliera di una mole elevatissima di dati, il controllo giudiziario preventivo – evocato varie volte dalle autorità statunitensi a testimonianza della sostanziale legittimità del programma di sorveglianza – viene di fatto ridotto ad un mero simulacro[57].

4. Il conflitto regolatorio USA/EU nella materia dei dati personali

Le onde d'urto del terremoto prodotto dalle rivelazioni di Snowden hanno innescato un processo di revisione dei meccanismi di controllo e sorveglianza elettronica, che potrebbe portare in futuro a mutamenti rilevanti. Tuttavia, come si è già accennato in precedenza, tale ripensamento critico ha interessato prevalentemente la questione della tutela dei cittadini statunitensi. Per quanto concerne la posizione degli stranieri, le uniche dichiarazioni di impegno sono state, almeno fino a pochi mesi fa, quelle riflesse nella *Presidential Policy Directive-PPD28*, le quali sembrerebbero peraltro ridimensionate degli orientamenti interpretativi sin qui adottati dalle autorità competenti[58]. Ciò ha determinato una tensione crescente con lo spazio giuridico e politico europeo, che è sfociata in un'aperta contrapposizione tanto sul piano parlamentare quanto su quello giurisdizionale[59].

Tale dinamica ha definito una nuova fase del conflitto regolatorio transatlantico, deflagrato a seguito dell'introduzione della direttiva 95/46/

[56] Cfr. *Suzlon Energy v. Microsoft Corporation*, 671 F.3d 726 (9th Circuit 2011).
[57] Così con argomenti molto persuasivi, L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* cit., 757 ss., 863-898.
[58] Si veda in proposito l'interessante analisi di D. Severson, *American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Changes,* in 56 *Harvard Int. L. J.* 465, 481-492 (2015).
[59] Sintetizzo qui quanto più approfonditamente esposto in F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* 78 *Law & Cont. Prob's* 101 (2015).

CE[60]. Difatti, ove se ne ripercorrano i momenti caratterizzanti, si potrà notare come in un primo momento il divario normativo USA/UE abbia prodotto attriti rilevanti soprattutto al livello del settore privato[61]. Era questo il contesto nel quale fu raggiunto, con notevoli difficoltà, l'accordo *Safe-Harbour*: difficoltà derivanti essenzialmente dalla diversa impostazione generale del sistema di tutela dei dati personali negli USA e in Europa. Mentre in Europa la disciplina si era sviluppata nel corso degli anni in maniera organica, includendo nel suo raggio d'applicazione tanto il settore pubblico quanto il settore privato e mirando a un bilanciamento (per quanto difficile e contestato) tra l'esigenza di libera circolazione dei dati nel mercato unico e quello della tutela dei diritti fondamentali, negli Stati Uniti il quadro rimaneva molto più asimmetrico e disorganico[62]. Il settore pubblico godeva di una regolamentazione tendenzialmente generale ed organica (il *Privacy Act*), la quale rispecchiava l'assunto condiviso negli anni '70 (l'epoca nella quale si erano diffusi i primi elaboratori elettronici di grandi dimensioni e limitata capacità di calcolo), per cui le minacce fondamentali alla sfera di riservatezza degli individui sarebbero derivate principalmente dal potere pubblico[63]. Per contro, il settore privato era connotato da discipline molto frammentarie (*cable communications act, video privacy act*, etc.), o dai rinvii alla potestà autoregolatoria dei privati (codici di condotta e simili), ove un ruolo fondamentale era giocato dal meccanismo del *notice and consent*[64]. La precomprensione del giurista, in questo caso, assegnava ai valori della libertà contrattuale, di iniziativa economica, nonché alla libertà d'espressione, un ruolo assiologicamente sovraordinato rispetto a quello della tutela (avvertita come paternalistica) del *data privacy*[65]. Si comprende quindi come la distanza più eclatante tra i due modelli regolatori si concentrasse sulla disciplina del trattamento dei dati in ambito privato, riducendosi tale divario nel settore pubblico a profili disciplinari importanti ma non decisivi (come l'assenza di un'autorità

[60] In tema si veda G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU,* cit., 657 ss.
[61] J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* in 38 *Hous. L. Rev.* 717, 728 (2001); F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* cit., 108-110.
[62] P.M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* in 126 *Harvard L. Rev.* 1966, 1974-1979 (2013).
[63] Cfr. in proposito P. Schwartz, *Data Processing and Government Administration: The Failure of the American Response to the Computer,* in 43 *Hastings L. J.* 1321 (1992).
[64] J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* cit., 725-730.
[65] In termini generali v. J.Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 *Yale L. J.* 1151 (2004).

amministrativa indipendente, il limitato rilievo del principio di necessità/*data minimization*, o il meccanismo di *enforcement* incentrato sull'iniziativa dei privati e sui rimedi risarcitori) [66]. Di qui la via dei *Safe Harbor Privacy Principles*, che avrebbero dovuto risolvere tale conflitto in una maniera *market-friendly*[67], e di qui anche la fragilità delle garanzie previste nello stesso Accordo per l'ipotesi di accesso da parte del settore pubblico ai dati detenuti da soggetti privati (vedi *infra,* § 6).

Nella sua prima fase di applicazione, il meccanismo di coordinamento sembrava avere dato buona prova di sé: l'adesione volontaria al sistema *Safe Harbor* da parte di alcune delle più importanti aziende statunitensi, insieme all'innalzamento dello standard di tutela a favore di tutti gli utenti (europei e non) e al ruolo di supervisione assunto dalla Federal Trade Commission, aveva fatto parlare di una competizione al rialzo, elevando la materia della protezione dei dati a controprova empirica del fenomeno descritto dagli scienziati della politica come *Brussels effect*[68]. Le rivelazioni di Snowden hanno gettato una diversa luce sul meccanismo in esame, facendo emergere gli elementi di criticità insiti nel fenomeno dell'accesso sistematico da parte dei poteri pubblici ai dati di terzi detenuti in mano privata: i dati legittimamente acquisiti nell'ambito dei rapporti contrattuali con soggetti privati (e trasferiti all'estero conformemente alle procedure *Safe Harbor*) vengono poi fatti oggetto di acquisizione in blocco e trattamento da parte di autorità pubbliche al di fuori di un adeguato quadro di garanzie e diritti. Questo, fondamentalmente, è il problema operativo da cui ha origine la controversia *Schrems*, la quale però non rappresenta il primo momento di emersione del suddetto conflitto e si inserisce all'interno di una più ampia dialettica tra sistema europeo e sistema statunitense. Difatti, l'Accordo *Safe Harbor* rappresentava il momento terminale di una prima forma di attrito tra i due ordinamenti, relativa soprattutto alla disciplina del settore privato e dei rapporti di mercato. All'indomani dell'11 settembre e dell'introduzione di una capillare normativa antiterrorismo negli USA, la quale ha notevolmente compresso i già non amplissimi spazi di protezione della *privacy* informativa, il suddetto conflitto regolatorio si

[66] La più approfondita analisi comparatistica è quella offerta da F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* cit., 619-635.

[67] P.M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* cit., 1979 ss.; J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* cit., 738 ss.; in tema si veda anche il contributo di V. D'Antonio – S. Sica, *I* Safe Harbor Privacy Principles*: genesi, contenuti, criticità, infra* in questo Volume.

[68] A. Bradford, *The Brussels Effect,* 107 *N.W. U. L. Rev.* 1, 22-26 (2012).

è progressivamente spostato dal settore privato al settore pubblico[69]. La prima disputa rilevante in ordine cronologico ebbe origine dalla pretesa da parte delle autorità USA di ottenere preventivamente da parte delle compagnie aeree la comunicazione dei dati identificativi dei passeggeri di voli per, da o attraverso gli Stati Uniti[70]. Investita della questione da parte delle stesse compagnie, la Commissione ha negoziato un accordo con il governo USA volto ad assicurare un quadro minimo di tutele, incentrato sui principi di trasparenza, accuratezza e sicurezza (originariamente siglato nel 2004, poi rinnovato nel 2007 e nel 2012) [71]. La seconda occasione di conflitto fu rappresentata dall'acquisizione coattiva da parte del Dipartimento del Tesoro USA, in attuazione del *Terrorist Finance Tracking Program* (TFTP), di una vasta messe di dati finanziari concernenti trasferimenti di fondi e altre operazioni bancarie da parte della *Society for Worldwide Interbank Financial Telecommunications* (SWIFT), la cui sede principale è ubicata in Belgio, ma con succursali operative anche in Olanda e negli USA[72]. La controversia che ne è derivata ha condotto infine all'approvazione nel 2010 di un apposito accordo bilaterale (TFTP II), che introduce specifiche salvaguardie per i dati personali relativi a cittadini europei[73].

5. La prospettiva della Corte di Giustizia: da Digital Rights *a* Schrems

Il c.d. Datagate rappresenta quindi soltanto l'ultimo capitolo di una dinamica di confronto più ampia, la quale però aveva visto sin qui pro-

[69] F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* cit., 110-117.

[70] In tema M. Botta – M. Viola de Azevedo Cunha, *La protezione dei dati personali nelle relazioni tra UE e USA, le negoziazioni sul trasferimento dei PNR,* in *Dir. Inf.* 2010, 315.

[71] Decisione della Commissione 2004/535, 2004 O.J. (L 235) 11; Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), 2007 O.J. (L 204) 18; Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 2012 O.J. (L 215) 5.

[72] Si veda F. Clementi – G. Tiberi, *Sicurezza interna, diritti e cooperazione internazionale nella lotta al terrorismo: i casi Pnr e Swift,* in www.astrid-online.it, 2013.

[73] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 2010 OJ (L 195) 5.

tagonista la Commissione europea e in una posizione alquanto defilata la Corte di Giustizia. Il cambiamento del quadro istituzionale determinato dal Trattato di Lisbona, e in particolare l'attribuzione alla Carta dei Diritti di un'immediata efficacia precettiva e del medesimo valore giuridico dei Trattati, ha contribuito ad alterare un siffatto equilibrio[74]. La Corte di Giustizia sembra avere assunto una posizione notevolmente più incisiva e coraggiosa, non diversamente peraltro dal Parlamento Europeo, che ha risposto allo scandalo NSA con molteplici iniziative, tra le quali l'approvazione di uno specifico emendamento alla Proposta di Regolamento Generale sulla tutela dei dati personali volto a imporre la mediazione istituzionale delle autorità di garanzia europee per i casi di trattamento dei dati per finalità di giustizia da parte delle autorità straniere (c.d. *anti-PRISM clause*) [75]. Nelle tre decisioni ricordate in apertura del presente scritto – *Google Spain, Digital Rights* e *Schrems* – la Corte ha ribadito il rango primario del diritto alla protezione dei dati, traendone una serie di

[74] In generale su questi aspetti v. F. Bestagno, *I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia,* in *Dir. umani e dir. int.,* 2015, 259, spec. 262, 266 ss.

[75] Questo il testo dell'art. 43a nella sua proposta originaria: «1.No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State. 2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority. 3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with Article 44(1)(d) and (e) and (5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57. 4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1)». Nel testo definitivo del Regolamento la norma è stata così modificata: «Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter».

implicazioni particolarmente significative sia sul piano della circolazione transfrontaliera dei dati, sia su quello del bilanciamento con i legittimi interessi alla sicurezza nazionale e alla libertà d'impresa[76].

In *Google Spain* la Corte ha proposto una lettura a compasso allargato della clausola di giurisdizione iscritta nell'art. 4 della direttiva 95/46/CE, forzando interpretativamente la formula «contesto delle attività di uno stabilimento»[77], così da sovrapporla al criterio dell' «offerta di beni e servizi indirizzata a soggetti dell'Unione», fatta propria da diversi atti del diritto privato regolatorio[78], nonché dal nuovo Regolamento Generale sulla tutela dei dati personali (art. 3, comma 2, lett. a) [79]. In tal modo il perimetro di operatività della disciplina europea in materia di protezione dei dati personali risulta notevolmente ampliato, tanto da far parlare di una vera e propria applicazione extra-territoriale della normativa comunitaria[80]. L'obiettivo sotteso a un siffatto intervento, come pure al Regolamento, consiste verosimilmente nel contrasto alle strategie di aggiramento della disciplina di protezione, funzionale peraltro anche all'attuazione di condizioni di parità concorrenziale per tutti gli operatori che si rivolgono al mercato europeo[81]. Appare giustificato, a tal riguardo, parlare di un vero e

[76] I In tema si leggano i contributi di G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, e di O. Pollicino – M. Bassini, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, entrambi *infra* in questo Volume..

[77] Sull'art. 4 della direttiva e i criteri di giurisdizione ivi fissati cfr. L. Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU citizens by Websites Worldwide?, Int'l Data Privacy L.,* 2010, 1.

[78] H.W. Micklitz, *The Internal v. The External Dimension of European Private Law – A Conceptual Design and a Research Agenda,* EUI Working Papers, 2015, 7, accessibile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2627718 [ultimo accesso 12.7.2016].

[79] IIn tema v. G. Caggiano, *L'interpretazione del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali,* in *Dir. Inf.* 2014, 616-618; e in G. Resta – V. Zeno-Zencovich, a cura di, *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* Roma, 2015, 55; P. Piroddi, *Profili internazionalprivatistici della responsabilità di un motere di ricerca per il trattamento dei dati personali,* in *Dir. Inf.* 2014, 623 ss.; G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, *infra* in questo Volume. Nell'ambito della giurisprudenza della Corte di Giustizia cfr. anche la sentenza del 1° ottobre 2015, causa C-230/14, *Weltimmo*.

[80] B. van Alsenoy – M. Koekkoek, *Internet and jurisdiction after* Google Spain*: the extraterritorial reach of the 'right to be delisted',* 5 *Int'l Data Privacy L.* 105, 110-111 (2015)..

[81] In questa prospettiva cfr. anche G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU,* cit., 674-678; per una disamina delle implicazioni della decisione *Google Spain* in ordine al flusso transfrontaliero dei dati v. M.L. Rustad – S. Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data*

proprio atto di esercizio della 'sovranità digitale' [82].

Con la decisione *Digital Rights* l'asse dell'intervento giurisdizionale si appunta invece sul settore pubblico e segnatamente sul conflitto tra *privacy* e sicurezza[83]. Investita della questione concernente la validità della direttiva 2006/24/CE, la Corte rileva che l'obbligo di conservazione dei dati di traffico per un periodo compreso tra 6 mesi e 2 anni integra un'ingerenza illecita nella sfera di riservatezza tutelata dagli artt. 7 e 8 della Carta dei Diritti. In particolare, la Corte osserva che, pur non essendo violato il contenuto essenziale dei suddetti diritti *ex* art. 52, par. 1, della Carta (essendo escluso l'accesso al contenuto delle comunicazioni e essendo previste alcune garanzie minime di protezione dei dati personali) [84], la normativa comunitaria comporta un sacrificio sproporzionato dei diritti alla riservatezza e alla tutela dei dati personali sotto tre profili fondamentali: *a*) il carattere generale e indifferenziato del programma di conservazione dei dati, e dunque l'assenza di limiti nella fase della raccolta; *b*) la durata irragionevole del periodo di conservazione; *c)* l'assenza di idonee garanzie in punto di accesso da parte dei terzi e utilizzo dei dati. In sostanza la Corte rigetta le tecniche di *blanket data retention,* in quanto idonee a determinare nei cittadini la sensazione che 'la loro vita privata sia oggetto di costante sorveglianza' [85] e quindi – anche a prescindere dall'esistenza di uno specifico pregiudizio (richiesto invece dalla Corte Suprema USA quale prerequisito dello *standing* nei casi in cui si censuri la legittimità dei programmi di sorveglianza elettronica)[86] – incompatibili con i valori di dignità e autodeterminazione informativa accolti dall'ordinamento europeo[87]. Ciò giustifica la soluzione particolarmente rigorosa adottata dalla Corte, la quale sancisce, per la prima volta, l'invalidità totale di una direttiva

Flow, 28 *Harvard J. L. & Tech.* 349 (2015).

[82] V. Zeno-Zencovich, *Intorno alla decisione nel caso* Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, retro* in questo Volume.

[83] In tema M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di* data retention, in *Dir. Un. Eur.,* 2014, 803, spec. 806 ss.

[84] Corte di giustizia, 8 aprile 2014, cit., §§ 39-40; sul punto v. O. Pollicino – M. Bassini, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit., par. 5.

[85] Corte di giustizia, 8 aprile 2014, cit., § 37.

[86] *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013); sul punto v. le considerazioni critiche di N.M. Richards, *The Dangers of Surveillance,* 126 *Harv. L. Rev.* 1934, 1935 (2013).

[87] Si veda nella medesima prospettiva la decisione Corte eur. Dir. uomo, 4 dicembre 2008, nn. 30562/04 e 30566/04, *S. and Marper v. UK.*

del Parlamento e del Consiglio per contrasto con la Carta dei Diritti[88].

Il monito espresso dalla Corte si indirizzava principalmente nei confronti dei governi europei, fautori negli ultimi anni di una politica che, in nome all'interesse alla sicurezza, aveva legittimato restrizioni sempre maggiori della sfera dei diritti fondamentali dei cittadini, delle quali la direttiva 2006/24/CE costituiva un esempio emblematico[89]. Tuttavia l'apparato argomentativo della decisione lasciava chiaramente intendere che analoghi, se non più incisivi, strumenti di salvaguardia avrebbero dovuto essere apprestati per l'ipotesi in cui la raccolta e la conservazione dei dati fossero disposti, per le medesime ragioni di sicurezza, da parte di autorità straniere. Ciò si desume in maniera inequivocabile dal § 68 della pronunzia, ove si legge che «tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti. Orbene, siffatto controllo, effettuato in base al diritto dell'Unione, costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali» [90]. È difficile non cogliere in filigrana un riferimento sufficientemente preciso al fenomeno – già di dominio pubblico al momento della decisione – dell'accesso sistematico da parte delle autorità USA ai dati personali relativi a cittadini europei.

Vista in quest'ottica, la decisione *Schrems* non fa che trarre le logiche conseguenze dalle premesse fissate nella pronunzia *Digital Rights* e segnatamente dal tipo di bilanciamento ivi accolto tra *privacy* e sicurezza. Oltre a negare l'effetto preclusivo del giudizio di adeguatezza compiuto dalla Commissione ex art. 25 nei confronti delle autorità di protezione dei dati nazionali[91], la Corte si spinge a sindacare nel merito la validità della Decisione 2000/520 della Commissione, travalicando i confini posti dalla domanda di rinvio pregiudiziale. Significativo è innanzitutto il modo in cui tale sindacato è condotto, in quanto la Corte appunta la propria attenzione non tanto sul contenuto intrinseco dei Principi stabiliti nell'Accordo *Safe Harbor* (i quali vincolano in primo luogo i soggetti *privati*

[88] Sul punto v. F. Bestagno, *I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia,* cit., 266.
[89] Per un quadro di sintesi v. l'ampia indagine di M. Nino, *Terrorismo internazionale, privacy e protezione dei dati personali,* Napoli, 2012, 147-350.
[90] Corte di giustizia, 8 aprile 2014, cit., § 68.
[91] Corte di giustizia, 6 ottobre 2015, cit., §§ 38-66.

che aderiscano al programma di autocertificazione) [92], quanto sul quadro istituzionale dell'ordinamento con il quale tali Principi sono destinati a interagire. L'anello critico dell'intero sistema è costituito dalla clausola – di cui all'Allegato I, quarto comma della Decisione – con la quale si stabilisce che l'applicabilità dei Principi in esame può essere limitata «se e inquanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» [93]. Questa clausola rende possibili – come osservato dalla Corte – ingerenze, fondate su esigenze connesse alla sicurezza nazionale, nei diritti fondamentali dei cittadini europei[94]. È per il suo tramite, infatti, che le autorità USA hanno potuto acquisire in maniera formalmente legittima una massa enorme di dati personali relativi a cittadini europei, trasferiti dai providers di telecomunicazioni in osservanza dei principi *Safe Harbor*. Ne deriva un duplice ordine di questioni: *a*) sussistono nell'ordinamento di destinazione regole idonee a limitare le suddette ingerenze allo stretto necessario per conseguire il legittimo obiettivo della protezione della sicurezza nazionale?; *b*) sono previsti specifici rimedi, di natura giurisdizionale o amministrativa, a tutela dei soggetti destinatari dei programmi di sorveglianza? Tali quesiti sono rilevanti ai fini del giudizio di adeguatezza di cui all'art. 25 della Direttiva, interpretato alla luce della Carta dei Diritti Fondamentali dell'Unione Europea[95]. A ciascuno di essi la Corte dà una risposta negativa. Attribuendo uno specifico rilievo alle risultanze empiriche dell'indagine condotta dalla Commissione bilaterale UE/USA, la Corte stigmatizza tanto l'estensione e i caratteri dei programmi di *bulk collection* adottati dalle agenzie statunitensi, quanto l'assenza di alcun rimedio esperibile da parte dei cittadini europei[96]. In particolare, viene giudicata radicalmente incompatibile con i precetti di cui agli artt. 7 e 8 della Carta dei Diritti una normativa, quale quella statunitense, «che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare

[92] Corte di giustizia, 6 ottobre 2015, cit., § 98.
[93] In tema cfr. anche V. D'Antonio – S. Sica, I Safe Harbor Privacy Principles: *genesi, contenuti, criticità*, cit., par. 3.4.
[94] Corte di giustizia, 6 ottobre 2015, cit., § 87.
[95] Su questo modello interpretativo v. in particolare F. Bestagno, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali, in Il dir. dell'Un. Eur.*, 2015, p. 25 ss.
[96] Corte di giustizia, 6 ottobre 2015, cit., § 90 ss.

l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta» [97]. Tali ingerenze vanno ben oltre quanto strettamente necessario ai fini della protezione degli obiettivi di interesse pubblico (ledendo pertanto il principio di proporzionalità) e, nel caso specifico del diritto al rispetto della vita privata (art. 7 Carta), ne intaccano il contenuto essenziale, sottoponendo lo stesso contenuto delle comunicazioni ad un regime di tutela particolarmente affievolito[98]. Inoltre risulta leso il contenuto essenziale del diritto a una tutela giurisdizionale effettiva (art. 47 Carta), per ciò che al singolo individuo è negata sia la facoltà di accedere ai dati che lo riguardano, sia di ottenere la rettifica o la soppressione di tali dati[99]. Di qui la declaratoria di invalidità della Decisione 2000/520, in quanto atto interno idoneo a legittimare, sia pure in via mediata, la compressione dei diritti fondamentali dei cittadini europei da parte delle autorità estere.

Conclusioni

A seguito della controversia *Schrems c. Data Protection Commissioner* l'attitudine 'extraterritoriale' della normativa europea in materia di protezione dei dati risulta ulteriormente rafforzata[100]. Se con la pronunzia *Google Spain* l'ambito oggettivo di applicazione della direttiva definito dall'art. 4 è stato esteso in via interpretativa, con la decisione *Schrems* è lo strumento offerto dall'art. 25 a essere significativamente potenziato. Tali interventi s'iscrivono con coerenza all'interno della dinamica di competizione regolatoria descritta in precedenza, dove ai ripetuti fenomeni di violazione transfrontaliera dei diritti fondamentali – resi possibili dallo sviluppo delle tecnologie dell'informazione e della comunicazione – corrispondono pun-

[97] Corte di giustizia, 6 ottobre 2015, cit., § 93.
[98] Corte di giustizia, 6 ottobre 2015, cit., § 94; sul punto si leggano le considerazioni di O. Pollicino – M. Bassini, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit.
[99] Corte di giustizia, 6 ottobre 2015, cit., § 95.
[100] In generale v. Dan J.B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses,* 50 *Stan. J. Int'l L.* 53, 71 (2014); Id., *Extraterritoriality in the Context of Data Privacy Regulation,* 7 *Masaryk Univ. J. L. & Tech.* 87 (2013); più articolato il quadro argomentativo offerto da Y. Poullet, *Transborder Data Flows and Extraterritoriality: The European Position,* 2 *J. Int'l Commerc. L. & Tech.* 146 (2007).

tualmente meccanismi di reazione a carattere dichiaratamente 'nazionalistico'[101]. Tale termine non è impiegato in un'accezione dispregiativa, bensì per denotare l'impronta tipicamente 'locale' del modello di disciplina (e di bilanciamento degli interessi) che si intende proteggere, a fronte dei rischi di aggiramento derivanti dall'utilizzo delle tecnologie informatiche e dalla de-localizzazione dei dati su server remoti[102]. Tali reazioni possono essere di varia natura: la proposta avanzata in Francia e in Germania di dare vita ad un *cloud* europeo costituisce una tipica risposta a carattere tecnologico, che preluderebbe a nuove forme di autarchia digitale[103]; mentre gli interventi della Corte di Giustizia fanno ricorso, piuttosto che agli arcani ingranaggi del 'codice' tecnologico, alla 'mano visibile' della legge. Ciò non toglie che in entrambi i casi l'obiettivo di fondo consiste nella riaffermazione della sovranità del sistema di riferimento, declinata nel senso più specifico della sovranità digitale[104], a dispetto di tutte le tesi anarco-libertarie affermate nella prima fase dello sviluppo dell'Internet, le quali rivendicavano, in uno con l''aterritorialità' dei rapporti digitali, la loro strutturale immunità dalla potestà regolatoria degli Stati[105]. Poste queste premesse, è ragionevole ipotizzare che la dialettica transatlantica prosegua secondo il consueto itinerario, sostituendo alla fase dell'aperto confronto quella della negoziazione tesa a nuovi accordi bilaterali[106].

In effetti, l'osservazione degli ultimi sviluppi delle relazioni USA/UE sembra muoversi esattamente in questa direzione. Da un lato le negoziazioni tra le autorità europee e quelle statunitensi hanno condotto alla stipula del nuovo Accordo «Privacy Shield» , il quale sostituisce il precedente Safe Harbor[107]. Dall'altro il Congresso degli Stati Uniti ha approvato, nel

[101] A. Chander – U.P. Lê, *Data Nationalism, 64 Emory L.J. 677* (2015).
[102] V. Zeno-Zencovich, *Intorno alla decisione nel caso* Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* cit.
[103] A. Chander – U.P. Lê, *Data Nationalism*, cit., 690-692.
[104] V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo Internazionale delle reti di telecomunicazione*, cit., par. 2.
[105] Per una ricostruzione attenta di tali tesi, ed una discussione della famosa 'Dichiarazione d'indipendenza del Cyberspazio' di J.P. Barlow, si veda R.H. Weber, *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles,* Berlin-Heidelberg, 2014, 15 ss.
[106] PPer alcune considerazioni in proposito v. M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* cit., 743.
[107] Per un'analisi dettagliata dei contenuti dell'accordo v. T. Grau – T. Granetzny, *EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?,* in *NZA,* 2016, 405 ss.; S. Sica – V. D'Antonio, *Verso il Privacy Shield: il tramonto dei Safe Harbor Privacy Principles, infra* in questo Volume.

dicembre 2015, il *Judicial Redress Act.* Tale legge estende alcune delle (già deboli) garanzie di tutela dei dati personali, riconosciute in capo ai cittadini statunitensi dal *Privacy Act* del 1974, e segnatamente la possibilità di agire per il risarcimento dei danni arrecati per il trattamento illecito di tali dati da parte delle agenzie governative, ai cittadini dei «covered countries» (ossia i paesi o le organizzazioni regionali selettivamente riconosciuti dall'Attorney General), venendo incontro quindi ad una parte delle richieste avanzate dalle autorità europee[108].

Il problema della tutela degli stranieri viene dunque affrontato secondo la più classica delle logiche 'bilaterali'. L'indispensabile esercizio di realismo non deve, però, fare perdere di vista la peculiarità degli interessi coinvolti nel campo della tutela dei dati personali, i quali trascendono il paradigma tradizionale della sovranità territoriale per attingere alla dimensione tipicamente universalistica dei diritti umani. Riguardata unicamente nell'ottica della competizione regolatoria (che pure assume, come si è visto, un peso rilevante), la vicenda *Schrems* potrebbe essere liquidata come una peculiare riaffermazione del *soft power* europeo, ove si demanda alla logica dei diritti ciò che non si riesce a conseguire attraverso la forza della politica. In realtà la posta in gioco sembra più alta, poiché pertiene alla ricerca di un difficile punto di equilibrio tra la tutela dei diritti dei singoli e l'invasività delle moderne tecniche di sorveglianza elettronica, le quali non soltanto trascendono il confine tra pubblico e privato[109], ma sono insensibili alle stesse frontiere territoriali, ponendo le premesse per vere e proprie forme di *global cybersurveillance*[110]. Se questa è la natura dei conflitti sottostanti, evidentemente le risposte locali, quali quelle offerte dall'ordinamento europeo, non possono che risultare parziali e insoddi-

[108] Per alcuni rilievi in proposito v. G. Greenleaf, *International Data Privacy Agreements after the GDPR and* Schrems, in 139 *Privacy Laws & Business International Report* 12 (2016).

[109] Cfr. F. H. Cate *et al.*, *Systematic government access to private-sector data,* 2 *Int'l Data Privacy L.* 195 (2012); N. M. Richards, *The Dangers of Surveillance,* cit., 1935.

[110] Cfr. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad* , cit., 319, 345-356 (ove è presentata un'articolata analisi delle tecniche utilizzate dalla NSA per intercettare o manipolare il traffico digitale anche al di fuori del territorio USA); D. Severson, *American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Changes,* cit.; C. Comella, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza «Safe Harbor» della Corte di giustizia dell'Unione Europea, infra* in questo Volume par. 3; più in generale A. Masferrer – C. Walker, a cura di, *Counter-Terrorism, Human Rights and the Rule of Law. Crossing Legal Boundaries in Defence of the State,* Cheltenham, 2013.

sfacenti. Si richiederebbe, invece, il rafforzamento degli strumenti offerti dal diritto internazionale, in modo da dare effettiva attuazione, adeguandoli alla realtà del contesto tecnologico, ai principi iscritti nell'art. 12 della Dichiarazione Universale dei Diritti Umani e nell'art. 17 del Patto Internazionale dei Diritti Civili e Politici[111], ove la riservatezza è elevata al rango di diritto umano, indipendentemente dalle appartenenze nazionali e territoriali. In questo senso sembrano muoversi alcuni recenti interventi dell'Assemblea Generale delle Nazioni Unite[112] e del Consiglio dei diritti umani[113], oltre alle varie dichiarazioni dei diritti che s'inscrivono all'interno del variegato universo del 'costituzionalismo digitale' contemporaneo[114]. Si tratta di segnali incoraggianti, ma la strada da percorrere è evidentemente ancora molto lunga.

[111] In proposito v. E.A. Rossi, *Il diritto alla privacy nel quadro giuridico europeo e internazionale alla luce delle recenti vicende sulla sorveglianza di massa,* in *Dir. com. sc. int.,* 2014, 331.
[112] Cfr. la Risoluzione del 18 dicembre 2013, UN Doc A/RES/68/167, *The Right to Privacy in the Digital Age*.
[113] Cfr. la Risoluzione del 1 aprile 2015, UN Doc A/HRC/RES/28/16, *The Right to Privacy in the Digital Age*, con la quale si delibera la nomina di uno *special rapporteur on privacy*.
[114] L. Gill – D. Redeker – U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights,* Berkman Center for Internet & Society, Research Pub. N. 2015-15 (9 Nov. 2015), accessibile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120 [ultimo accesso 12.7.2016]; F. Musiani, *Une 'Charte' pour les droits des Internautes? Perspectives et alternatives,* in *Droit et société,* 2012, 425; M. Bassini – O. Pollicino, a cura di, *Verso un Internet Bill of Rigths,* Roma, 2015.

Abstract

This article focuses on the background of the ECJ Schrems decision and deals with the regulatory conflict between USA and Europe in the field of data protection. It provides a detailed analysis of the legal architecture of the mass surveillance programs adopted by the US security agencies and discusses the issue of privacy protection for foreign citizens. By comparing the US and the EU approach, it details the transatlatic conflict that arose in the aftermath of the introduction of the Directive 95/46 and looks at the ECJ Digital Rights, Google Spain and Schrems decisions as integral part of such regulatory conflict. It argues that given the particular features of the technological context, which makes extraterritorial violations much easier, decision-makers should take more seriously the universal character of the right to privacy as a fundamental human right.