Giovanni Sartor - Mario Viola De Azevedo Cunha

Il caso Google e i rapporti regolatori USA/EU

SOMMARIO: 1. Introduzione: divergenze e convergenze politico-giuridiche tra Europa e Stati Uniti - 2. La trasmissione dei dati sui passeggeri (PNR) e gli accordi SWIFT - 3. Il caso Snowden - 4. La discussione sul Regolamento sulla protezione dei dati - 5. Google- Spain: un conflitto giuridico o politico? - 6. Conclusione.

1. Introduzione: divergenze e convergenze politico- giuridiche tra Europa e Stati Uniti

La regolazione della protezione dei dati negli Stati Uniti e nell'Unione Europea presenta divergenze non solo in aspetti particolari, ma anche sulle ispirazioni più astratte. Infatti, benché i valori etico-giuridici e gli interessi economico-politici in gioco siano gli stessi negli Stati Uniti e nell'Unione, tali valori e interessi si presentano con diversa intensità nelle due sponde dell'Atlantico, cosicché ne risultano distinti indirizzi politici e giuridici, che si oppongono nel dibattito globale sulla protezione dei dati. L'evoluzione delle norme sociali e dei valori giuridici ha fatto sì che in Europa l'idea della *privacy* si collegasse a quella della dignità[1]. Il valore giuridico della dignità ha molteplici radici, religiose, umanistiche e filosofiche, attinenti alle dimensioni dell'autodeterminazione, del rispetto e dell'eguaglianza, ma la sua tutela giuridica si collega originariamente al tentativo 'democratico' di garantire a tutti i cittadini attributi riservati alle classi privilegiate, cioè l'attributo aristocratico dell'onore e quello romantico di una personalità che si sviluppa liberamente, secondo la propria dinamica interiore. La tutela di questi attributi comporta l'esigenza di proteggere l'individuo rispetto alla circolazione d'informazioni che lo riguardano, suscettibili di incidere sulla sua immagine sociale. Si tratta di un'elaborazione che le culture giuridiche tedesca e francese compivano già

[1] Su questi aspetti, si vedano N.Wong, *Privacy: Charting its Developments and Prospects.* In M.Klang e A.Murray. *Human Rights in the Digital Age* (2005), London: Glasshouse Press. p. 158.

nell'ottocento, cosicché il celeberrimo contributo di Warren e Brandei[2], spesso considerato all'origine dell'idea di *privacy* quale controllo sulla circolazione delle informazioni personali, può forse considerarsi, alla luce di una storia globale del pensiero giuridico, come un trapianto parzialmente fallito[3]. Il valore della dignità ispira in particolare la disciplina europea sulla protezione dei dati, e con riferimento a questo valore l'esigenza di controllare la raccolta e la circolazione dei dati personali è stata affermata non solo nella legislazione e nella giurisprudenza comunitaria e nazionale, ma anche al supremo livello dell'ordinamento dell'Unione, nell'articolo 8 della Carta dei diritti fondamentali, dedicato al diritto alla protezione dei dati personali. Negli Stati Uniti invece, l'idea di *privacy* è rimasta prevalentemente incentrata sulla tutela dello spazio vitale dell'individuo, circoscritto dalla sua persona e proprietà, rispetto alle intrusioni da parte dello Stato, tanto nella raccolta d'informazioni quanto nella limitazione della libertà di scelta. A questa idea si ispira anche la giurisprudenza della Corte suprema, in una serie di celebri sentenze, come Griswold v. Connecticut (1965) e Roe v. Wade (1973).

Le due idee di *privacy*, come controllo 'dignitario' sulla propria rappresentazione sociale e come libertà privata da intrusioni pubbliche, sono peraltro presenti in entrambe le culture giuridiche, e non vi è incompatibilità tra esse, come provano non solo numerosi contributi dottrinali tesi a integrare le due prospettive[4], ma anche il fatto che sia il diritto europeo, sia quello statunitense, contemplano entrambi gli aspetti, nella legislazione come nella giurisprudenza. Tuttavia, i diversi aspetti della *privacy* hanno diverso rilievo nelle due culture, così come hanno diverso rilievo i valori e gli interessi suscettibili di opporsi alla *privacy*. Ne risaltano diverse possibilità che la *privacy* possa essere lecitamente compressa nei conflitti con altri valori e interessi[5].

In particolare, l'assoluta preminenza della libertà di espressione (*freedom of speech*) negli Stati uniti limita l'ambito della protezione della *privacy* rispetto alla pubblicazione d'informazioni personali mediante ogni tipo di mezzi di comunicazione, Internet inclusa. Nell'ordinamento statunitense ogni informazione può essere in linea di principio comunicata al pubbli-

[2] S.Warren e L.Brandeis, *The right to privacy* (1890), *Harvard Law Review*, 4:193-220.
[3] V.J. Whitman, *The two western cultures of privacy: Dignity versus liberty* (2003- 4), *Yale Law Journal*, 113:1152-221.
[4] V. tra tutti, W.L.Prosser. *Privacy* (1960), *California Law Review*, pp. 389-407 e recentemente D.J.Solove, *A taxonomy of privacy* (2006), *University of Pennsylvania Law Review*, pp. 154:477.
[5] N.Wong, *Privacy: Charting ecc.* (2005). *op. cit.* p. 158.

co, con i soli limiti della proprietà intellettuale e di immagini di nudità.

Persino foto di nudità, prese con il consenso dell'interessato, ma pubblicate su Internet senza il suo consenso, possono essere successivamente distribuite in rete contro la volontà dello stesso[6].

Inoltre, ogni informazione o immagine concernente comportamenti in luoghi aperti al pubblico, può essere liberamente distribuita, anche quando si metta l'informazione o immagine a disposizione di un pubblico più ampio e diverso rispetto a quello presente nel contesto originario[7]. Un limite può essere dato dall'esistenza di un'«aspettativa di *privacy*[8]» , ma questa aspettativa opera solo nei casi in cui l'interessato possa prevedere che l'informazione che lo riguarda non sarà raccolta ed elaborata o distribuita, e ciò corrisponda alle prevalenti norme sociali: di conseguenza ogni prassi limitativa della *privacy* che sia socialmente diffusa tende ad essere legittima. In particolare, la preminenza della libertà di espressione preclude, nel diritto statunitense, ogni spazio per il diritto all'oblio su Internet: se un'informazione è stata legittimamente diffusa al pubblico, può continuare a essere distribuita, e può essere ripubblicata senza limiti. Quindi, mentre negli ordinamenti europei il diritto all'oblio rispetto a informazioni pregiudizievoli per l'interessato e non più attuali è variamente riconosciuto[9], negli Stati Uniti non c'è praticamente alcun limite alla

[6] Si veda J.Whitman, *The two western ecc. op. cit.*, p. 1200. Recentemente peraltro alcuni Stati USA hanno emanato leggi che proibiscono la pubblicazione di immagini sessualmente explicite senza il consenso dell'interessato, nel entativo di contrastare il diffuso fenomeno del revenge porn (pornografia di vendetta, avente lo scopo di umiliare o imbarazzare).

[7] Come esempio estremo, ricordiamo il caso di Oliver Sipple, che sventò eroicamente un attentato alla vita del presidente Gerald Ford, ma così facendo si espose alla curiosità della stampa, che ne rivelò l'orientamento omosessuale, tenuto fino ad allora nascosto alla famiglia. Sipple successivamente si suicidò (J.Whitman *The two western ecc.* [2003-4], *op. cit.* p. 1196).

[8] Il Parlamento Europeo, modificando il testo della Proposta di Regolamento Generale sulla Protezione dei dati, ha incluso il requisito che sia soddisfatta la «ragionevole aspettativa» di *privacy* dell'interessato nell'Art. 6 lettera (*f*), quale condizione aggiuntiva per l'elaborazione giustificata da legittimi interessi del titolare, (PARLAMENTO EUROPEO, Risoluzione legislativa del 12 marzo 2014).

[9] Per una trattazione dei diversi aspetti del diritto all'oblio, in Italia e all'estero, si vedano i contributi in F.Pizzetti a cura di, *Il caso del diritto all'oblio* (2013), Giappichelli. Sugli aspetti comparati, v. in particolare O.Pollicino e M.Bassini, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, *ibid.*, pp. 185-228; Sul diritto all'oblio v. anche, tra gli altri: G.Finocchiaro, *La memoria della rete e il diritto all'oblio*, in *Dir. Inf.* 2010, pp. 393-403. G.Sartor, *The right to be forgotten: dynamics of privacy and publicity*, in L.Floridi. *The protection of information and the right to privacy* (2014), Springer, p. 1-15. V. *retro* in questo volume il commento di G. Finocchiaro,

pubblicazione di informazioni vere su eventi passati[10]. È vero che alcuni precedenti e testi legislativi sembrano attribuire un diritto all'oblio su alcuni fatti del passato (per esempio reati giovanili[11]), ma essi sono stati superati dalla costante giurisprudenza della Corte Suprema che ha affermato il primato della libertà di espressione. Ad esempio, nel caso Cox v. Cohn (429 US 469, 493-496 [1975]), concernente la pubblicazione del nome della vittima di uno stupro, la Corte Suprema affermava che, in generale, nessuna responsabilità poteva discendere dalla divulgazione di informazioni contenute in documenti pubblici. Il fatto che notizie vere siano pregiudizievoli alla reputazione dell'interessato non esclude la liceità della loro pubblicazione[12]. Per i giudici statunitensi la pubblicazione della fedina penale di una persona è garantita dal Primo Emendamento. Secondo il diritto statunitense Wikipedia può legittimamente respingere la richiesta, presentata da due cittadini tedeschi, condannati per aver ucciso un attore famoso, che i loro nomi fossero rimossi dalla pagina su questo attore[13].

La preminenza attribuita alla libertà di espressione ha inoltre condotto i giudici statunitensi, nella loro interpretazione della sezione 230 del Communication Decency Act, a riconoscere la più ampia tutela al provider che ospiti informazioni accessibili al pubblico, anche quando la distribuzione di tali informazioni un comportamento illecito da parte di chi le carica in rete. Ogni limitazione dell'immunità del provider comporterebbe infatti il rischio di una «censura collaterale» limitatrice della libertà di espressione, poiché il timore di incorrere in sanzioni indurrebbe il provider a rimuovere anche informazioni lecite, nel timore che possano esporlo a responsabilità[14]. Anche la libertà d'iniziativa economica

par. 2 e *infra* il commento di S.Sica e V.D'Antonio, par. 7.

[10] F.Werro, *The right to inform v. the right to be forgotten: A transatlantic clash*, in A.Colombi Ciacchi, C. Godt, P. Rott, e L.J.Smith (a cura di), *Liability in the Third Millennium*, pp. 285-300, Baden-Baden, 2009.

[11] La dottrina fa riferimento ad un caso del 1931 deciso dalla Corte d'Appello della California (Melvin vs Reid), in cui il diritto all'oblio è stato esplicitamente riconosciuto come una conseguenza immediata del diritto alla *privacy*. R.A.Dotti, Proteção da vida privada e liberdade de informação (1980), São Paulo: Revista dos Tribunais, pp. 90-91.

[12] J.Rosen, *The Right To Be Forgotten* (2012), Symposium Issue, 64 *Stan. L. Rev. Online* 88, February 13, p. 91.

[13] *Ibid.* p. 88.

[14] Sull'idea di censura collaterale, v., J.M.Balkin, The future of free expression in a digital age (2008), Pepperdine Law Review, 36:101-18 e J.Rosen, The right to be forgotten (2012), Stanford Law Review Online, 64:88-92. Per una generale limitazione della responsabilità del provider ai casi in cui si provi l'«actual malice» dello stesso, v. M.A.Lemley, Rationalising Internet safe harbours (2007), Journal on Telecommunication

viene spesso ad acquistare preminenza rispetto alla *privacy* nel contesto statunitense. Così la rilevazione e la cessione di profili di consumatori, la distribuzione di rapporti attinenti al credito, il riuso di dati personali per scopi diversi e ulteriori rispetto a quelli che ne hanno determinato la raccolta, sono ritenuti comportamenti leciti indipendentemente dal consenso dell'interessato. I vantaggi economici che queste pratiche possono comportare, facilitando gli scambi e la libertà d'iniziativa economica degli operatori, superano di regola, nella prospettiva statunitense, le esigenze di tutela della *privacy*, se non in ambiti nei quali i rischi siano particolarmente evidenti, come nel trattamento dei dati genetici[15]. Peraltro, anche nel diritto dell'Unione le esigenze del traffico economico prevalgono in taluni casi sulla *privacy*, consentendo, per ragioni economiche, trattamenti non autorizzati dall'interessato.

Ciò vale in particolare nell'ambito della formazione e dell'adempimento dei contratti, nella distribuzione d'informazioni sul credito, nella raccolta di informazioni per la tutela giudiziale di diritti anche economici, ecc.

Le due culture giuridiche sembrano differire anche nell'attitudine rispetto al rischio derivante dall'innovazione tecnologica. All'idea statunitense che l'innovazione debba essere libera e non debba richiedere autorizzazioni (*permissionless innovation*, secondo lo slogan di Vinton Cerf, uno degli inventori di Internet[16]), si oppone spesso in Europa il principio di precauzione, chiamato «legge della paura» dai suoi detrattori[17], che assume la pericolosità e quindi l'illiceità dell'innovazione in assenza di prova contraria, verificata dall'autorità competente. Un esempio di questo atteggiamento può forse ravvisarsi nell'Art. 24, comma 1, lettera (*g*) del nostro Codice *privacy*. Anziché limitarsi ad affermare la liceità dei trattamenti destinati a soddisfare un legittimo interesse del titolare, in assenza di prevalente interesse contrario, come fa la Direttiva europea sulla protezione dei dati, la nostra legge richiede altresì la previsione della liceità del tratta-

and High Technology Law, 6:101-19. Sul rapporto tra tutela della *privacy* e responsabilità dei provider, vedi G.Sartor, Providers' liabilities in the new EU data protection regulation: A threat to Internet freedoms? (2013), International Data Privacy Law. pp. 3-12. V. anche G.Sartor e M.Viola De Azevedo Cunha, Il caso Google-ViviDown tra protezione dei dati e libertà di espressione online, in Dir. Inf. 2010, 645.

[15] Il conflitto tra la tutela della *privacy* e l'esigenza di facilitare gli scambi mettendo a disposizione delle parti tutte le informazioni rilevanti era già sottolineata da S.Rodotà, Tecnologie e diritti (1995), Bologna.

[16] V.Cerf, *Keep the Internet open*, New York Times, 24 Maggio 2012.

[17] Secondo la celebre caratterizzazione di C.Sunstein, *Laws of fear: Beyond the precautionary principle* (2005), Cambridge University Press.

mento da parte del Garante, rendendo così illegittimo ogni trattamento di dati personali che non sia previsto dal garante o espressamente consentito dal titolare. La possibilità di elaborare dati personali in modi nuovi, per scopi legittimi, ma non originariamente previsti ed espressamente consentiti, è divenuta particolarmente significativa oggi, nel contesto del c.d. *big data.* Si tratta della raccolta automatica di enormi quantità di dati (sull'uso dei servizi di Internet, le abitudini dei consumatori, il traffico, ecc.) che possono essere utilizzati, grazie alle tecniche del c.d. *data mining*, per molteplici finalità di utilità economica, scientifica, o sociale, non prevedibili al momento della raccolta dei dati stessi[18]. Ai diversi valori giuridici, o meglio al diverso peso di essi nel sistema giuridico statunitense e in quello europeo, si aggiunge il diverso peso degli interessi in gioco. I protagonisti dell'economia della rete si trovano negli Stati Uniti, essi godono dei vantaggi economici dell'elaborazione dei dati personali, e hanno un'enorme capacità di lobbying nei confronti del legislatore statunitense. Non stupisce che sia proprio il legislatore statunitense a dedicare maggiore attenzione agli interessi dei protagonisti economici di Internet, o almeno a esitare di fronte a ogni misura che possa compromettere tali interessi. Il legislatore europeo invece, benché oggetto esso stesso di forti pressioni lobbystiche, sente l'esigenza di contribuire a limitare lo strapotere delle imprese statunitensi della new economy, a tutela dei consumatori, ma anche delle imprese europee, cosicché la restrizione delle pratiche commerciali che incidono sulla *privacy* può assumere connotazioni protezionistiche.

Anche nel campo pubblico e in particolare in quello della sicurezza, le culture giuridiche europee e statunitensi sembrano dare diverso peso agli interessi, valori, ed esigenze in gioco. Gli Stati Uniti, quale una superpotenza militare, impegnata in numerosi scenari, e quindi soggetta a particolari rischi e minacce, divenute realistiche dopo l'attentato alle Torri Gemelle, tendono a dare maggiore rilievo alle esigenze della sicurezza nazionale, così come a quelle strategiche e geopolitiche[19]. Inoltre, il fatto che gli Stati uniti posseggano strumenti per il controllo delle comunica-

[18] Quando i dati diventano una materia prima, suscettibile di usi molteplici, emerge l'esigenza di evitare lo 'spreco' che risulterebbe dall'eliminazione delle informazioni disponibili non appena raggiunto lo scopo della loro raccolta, esigenza in conflitto con i principi della minimizzazione dei dati personali e della loro utilizzabilità solo per scopi predeterminati. Questa testi è sostenuta, tra gli altri da F.Cate, P.Cullen e V.Mayer-Schönberger, *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (2014), Microsoft Corporation.

[19] Il ricorso a tecnologie di sorveglianza globale, quale mezzo necessario per anticipare minacce terroristiche è affermato da Ph.Bobbitt, *The Shield of Achilles* (2002), Penguin; Ph.Bobitt, *Terror and Consent* (2008), Allen Lane.

zioni a livello globale, e che nel loro territorio risiedano i principali attori della rete, rende a essi possibile effettuare una raccolta ed analisi globale di informazioni, come evidenziato dal programma Prism, reso noto dalle rilevazioni di Edward Snowden[20]. Quindi, la presenza di maggiori esigenze in tema di sicurezza e controllo globali, e la disponibilità di mezzi di controllo capaci di soddisfare in qualche misura tali esigenze, induce a una prospettiva più favorevole all'impiego di mezzi di sorveglianza. Ciò non significa che la raccolta massiccia di informazioni effettuata a tal fine possa considerarsi moralmente e politicamente giustificata, e legittima alla luce della stessa normativa americana e del diritto internazionale, ma contribuisce a spiegare come alla sorpresa e all'indignazione dei governi europei (siano esse autentiche o ipocrite) corrispondano atteggiamenti più sfumati e differenziati di là dall'Atlantico[21]. Le diversità che abbiamo illustrato contribuiscono a spiegare perché Stati Uniti e Unione europea abbiamo adottato diversi modelli per la protezione dei dati, una disciplina generale in Europa e discipline settoriali, principalmente rivolte verso i soggetti pubblici, negli Stati Uniti. Ciò non esclude importanti convergenze. Ricordiamo come la disciplina Europea sulla protezione dei dati riprenda i *Fair Information Principles*, già enunciati in una relazione del *U.S. Secretary's Advisory Committee on Automated Personal Data Systems* nel 1973[22], nell'ambito dell'iniziativa culminata nell'adozione del Federal *Privacy* Act statunitense nel 1974. Inoltre sempre più pressanti si fanno le richieste di una disciplina più rigorosa della *privacy* negli Stati uniti, estesa anche al settore privato, e che possibilmente preveda anche un'autorità di controllo imparziale. Diverse soluzioni sono state proposte al fine di conciliare tale disciplina con la tradizione giuridica statunitense, dall'accentuazione degli aspetti proprietari della *privacy*, al rilievo delle norme sociali (*fair information rules*), all'affidare il controllo a una commissione parlamentare piuttosto che a un'autorità amministrativa[23].

Una convergenza verso una riduzione della tutela della *privacy* si è

[20] V. H.Farrell e M.Finnemore, *The End of Hypocrisy: American Foreign Policy in the Age of Leaks* (2013), 92 *Foreign Aff.* 22.

[21] Per una difesa della opportunità strategica e della legittimità giuridica di Prism, v. Ph.Bobbit, *NSA is upholding, not subverting, the law* (2013). Il testo è disponibile a *http://www.ft.com/cms/s/0/2da229bc-d1bc-11e2-9336-00144feab7de.html#axzz39N5uZYM1* [consultato il 03/08/2014].

[22] U.S.A., *Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, 1973, Il testo è disponibile all'indirizzo *https://www.hsdl.org/?view&did=479784* [consultato il 03/08/2014]..

[23] Per quest'ultima tesi, si veda J.Rosen, *«About the Author». The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (2004). Random House pp. 213 ss..

invece realizzata dopo gli attacchi terroristici del settembre 2011[24]. Gli Stati Uniti, subito dopo gli attentati alle Torri Gemelle, adottavano due provvedimenti restrittivi dei diritti dei cittadini. Il Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*) autorizza agenzie ed enti governativi ad avere libero accesso a varie banche di dati pubbliche e private[25], permettendo, ad esempio, l'accesso alla cronologia delle chiamate telefoniche, e-mail e a file finanziarii e medici. L'*Aviation and Transportation Security Act* esige che tutte le compagnie aeree che volano verso gli Stati Uniti forniscano i dati dei propri passeggeri (*Passenger Name Record* - PNR) al *Customs and Border Protection Administration* degli Stati Uniti (CBP) prima che l'aereo decolli verso gli USA. Anche nell'Unione Europea l'idea che la *privacy* e la protezione dei dati possano essere limitate ai fini della lotta contro il terrorismo e la criminalità ha ottenuto il sostegno di molti governi, soprattutto dopo gli attentati terroristici di Madrid e Londra. Lo scambio di dati personali tra le autorità di polizia in diversi Stati membri dell'UE è diventato elemento essenziale della cooperazione internazionale contro il terrorismo e la criminalità organizzata[26]. Recentemente, tuttavia, l'esigenza della protezione dei dati, anche nel campo sicurezza, si è imposta nella giurisprudenza della Corte di Giustizia, che ha dichiarato l'illegittimità della Direttiva sulla Data Retention, che imponeva ai provider di servizi di telecomunicazione la conservazione dei dati sul traffico telefonico[27]. Già il Gruppo di Lavoro Articolo 29 nel suo «Parere sulla necessità di un approccio equilibrato alla lotta contro il terrorismo", aveva espresso perplessità su tale provvedimento, affermando che «I provvedimenti contro il terrorismo non devono compromettere gli stand ard per la

[24] S.Rodotà, *La vita e le regole – Tra diritto e non diritto* (2006), Milano: Feltrinelli, p. 82. «La prospettiva di una più forte tutela attraverso strumenti giuridici, tuttavia, è contraddetta dalle tendenze legislative avviate dopo gli attentati dell'11 settembre 2001. Negli Stati Uniti, il Patriot Act consente a una serie di soggetti pubblici un accesso pieno a qualsiasi banca dati pubblica o private, cancellando così la garanzia offerta dai divieti di interconnessione. Diventa problematica la possibilità di sottrarre il corpo elettronico allo sguardo totale di poteri non controllabili».

[25] S. Rodotà *La vita e le regole ecc.* (2005), *op. cit.* p. 82.

[26] Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen (COM(2009)0262 final). *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0262:EN:HTML*[consultato il 03/08/2014]..

[27] DIRETTIVA 2006/24/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

protezione dei diritti fondamentali che caratterizzano le società democratiche, e non è necessario che producano 'effetti siffatti' e rilevando che «un elemento fondamentale della lotta al terrorismo è costituito dall'impegno alla salvaguardia di quei valori fondamentali che costituiscono la base di ogni società democratica, ossia proprio i valori che coloro che praticano l'uso della violenza tentano di distruggere»[28]. Tuttavia, a conferma della diversità delle prospettive culturali e politiche presenti in Europa, il governo del Regno Unito ha recentemente presentato una proposta di legge, con il sostegno di maggioranza e opposizione, che reintroduce l'obbligo di conservare i dati sul traffico telefonico, in vista del loro uso nella prevenzione e repressione del terrorismo e della criminalità[29]. Nel Sudamerica, la protezione dei dati personali è ispirata alla prospettiva europea[30], a causa dei legami storici e culturali tra Europa continentale e Sudamerica, che si estendono alla cultura giuridica e al disegno istituzionale. Anche nel Sudamerica la protezione della *privacy* si collega al principio del rispetto della dignità e la maggior parte dei paesi sudamericani ha riconosciuto l'*Habeas Data* quale diritto costituzionalmente garantito. Molti paesi (circa la metà) hanno già adottato una disciplina generale di protezione dei dati personali ispirata al modello europeo, anche per poter soddisfare il requisito di adeguatezza di cui all'articolo 25 della direttiva europea 95/46/CE, e quindi poter elaborare dati provenienti dall'Europa. Peraltro, il Brasile, la più grande economia del Sudamerica, benché abbia assunto la leadership regionale nella protezione dei dati dopo le rivelazioni del caso Snowden, non dispone ancora di una legge generale sulla protezione dei dati.

Il Sudamerica sembra propendere per la prospettiva europea anche sul diritto all'oblio, benché non manchino decisioni giudiziarie e scelte legislative maggiormente sensibili alle esigenze della libertà di espressione e della protezione degli intermediari. In Argentina, paese che ha adottato una legge generale sulla protezione dei dati ispirata dalla direttiva europea,

[28] ARTICOLO 29 - GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI. Parere 10/2001 sulla necessità di un approccio equilibrato alla lotta contro il terrorismo. *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp53_it.pdf#h2-14* [consultato il 30/06/2014]..

[29] UK Data Retention and Investigatory Powers Act 2014. Il testo è disponibile a *http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf* [consultato il 03/08/2014].

[30] A.M.Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches* (2012), *International Law News*, Vol. 41, nº 4. Il testo è disponibile a *http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html* [consultato il 30/06/2014].

un recente caso ha affrontato il diritto all'oblio. Una pop star argentina, che aveva posato per delle foto osé in gioventù, aveva chiesto a Google e Yahoo di escludere le foto dalle loro ricerche, sostenendo che la loro reperibilità avrebbe violato il suo diritto all'oblio. Il giudice argentino si schierava con la pop star, condannando Google e Yahoo a pagare una multa, e ordinando loro di rimuovere tutte le immagini sessuali che contenevano il nome della pop star. La decisione era però ribaltata in appello, considerando che Google e Yahoo avrebbero potuto essere ritenute responsabili solo se avessero saputo che il contenuto era diffamatorio e avessero avuto la possibilità di rimuoverlo. Ci sono oggi almeno centotrenta casi pendenti nei tribunali argentini nei quali si chiede la rimozione di foto e contenuti generati dagli utenti, la maggior parte promossi da personaggi dello spettacolo[31].

In Brasile, il *Superior Tribunal de Justiça* – La Corte d'appello più alta in Brasile per questioni non-costituzionali del diritto federale – ha recentemente affrontato in due casi (congiuntamente decisi il 28 maggio 2013) il tema diritto all'oblio nei confronti dei provider. Nel primo caso i giudici brasiliani riconoscevano il diritto alla rimozione della notizia concernente l'incriminazione di un soggetto poi assolto. Secondo la corte la continuata pubblicazione della notizia avrebbe violato la dignità umana dell'interessato, che continuava a essere considerato un 'sospetto' nel suo ambiente sociale[32]. Nel secondo caso[33], la Corte respingeva la richiesta che il nome della vittima di un omicidio risalente al 1958 non fosse menzionato in un programma televisivo. La Corte riteneva che il reato avesse avuto notorietà nazionale e che il nome della vittima fosse diventato parte della memoria collettiva, e quindi fosse necessario alla rappresentazione dell'evento.

In Brasile la recente legge sul *Marco Civil* garantisce l'immunità dei fornitori di servizi di Internet, i quali sono responsabili per la diffusione di informazioni illegali solo se non adempiono a ordini di rimozione di un'autorità competente (un giudice)[34]. Pertanto, sembra che in Brasile il provider non sia tenuto a conformarsi a richieste di rimozione da parte di privati, in assenza di previa determinazione autoritativa circa l'esistenza di

[31] J.Rosen (2012), *The Right To Be Forgotten ecc. op. cit.* p. 91.
[32] Superior Tribunal de Justiça. REsp 1.334.097-RJ, Rel. Min. Luis Felipe Salomão.
[33] Superior Tribunal de Justiça. REsp 1.335.153-RJ, Rel. Min. Luis Felipe Salomão.
[34] Articolo 19. Al fine di garantire la libertà di espressione e di evitare la censura, il fornitore di servizi di Internet sono responsabili solo se non rispettano una decisione di una autorità giudiziaria nel senso di escludere tale contenuto entro il limiti tecnici del loro servizio e entro il termine indicato nella decisione, fatte salve le disposizioni di legge in senso contrario.

un obbligo di rimozione. L'unica eccezione è il caso di immagini, video o altri materiali contenenti nudità o atti sessuali di carattere privato, nel quale caso il provider dovrà conformarsi alla richiesta di rimozione da parte dell'interessato. Nelle pagine seguenti considereremo alcuni casi in cui si sono manifestate queste convergenze e divergenze tra Europa, Stati Uniti e Sudamerica, per poi approfondire l'esame dei contrasti emersi rispetto al caso Google-Spain e trarre alcune considerazioni conclusive.

2. La trasmissione dei dati sui passeggeri (PNR) e gli accordi SWIFT [35]

Lo *US Aviation and Transportation Security Act*, adottato nel 2001, esigeva che tutte le compagnie aeree che volano verso gli Stati Uniti fornissero i dati dei propri passeggeri, detti PNR, (*Passenger Name Records*). Tale norma dava luogo a reazioni accese in alcuni Stati membri dell'UE, che conducevano a negoziati tra l'UE e gli Stati Uniti con l'obiettivo di consentire la trasmissione dei PNR, assicurando un livello adeguato di protezione dei dati. Nel febbraio 2003 la Commissione Europea e la *customs and Border Protection Administration (CBP)* emettevano una dichiarazione congiunta[36] in base alla quale la Commissione autorizzava temporaneamente le compagnie aeree europee a trasferire i PNR alle autorità statunitensi, in attesa di trovare una soluzione definitiva al problema.

Nel marzo del 2004 la Commissione sottoponeva al Parlamento il progetto della propria decisione sull'adeguatezza del trattamento dei PRN rispetto agli standard europei, accompagnato dal progetto d'impegno del CBP, cui faceva seguito la proposta di decisione del Consiglio concernente un accordo con gli Stati Uniti.

Nonostante le osservazioni critiche del Parlamento, la Commissione e il Consiglio procedevano adottando rispettivamente la decisione di adeguatezza e l'accordo. Il Parlamento ricorreva alla Corte di Giustizia contro i due provvedimenti, adducendo diversi motivi: eccesso di potere, violazione dei principi essenziali della direttiva, violazione dei diritti fondamentali e violazione del principio di proporzionalità.

Il 30 maggio 2006 la Corte di Giustizia annullava i provvedimenti

[35] V. M.Botta e M.Viola De Azevedo Cunha, *La protezione dei dati personali nelle relazioni tra UE e USA: le negoziazioni sui trasferimento dei PNR*, in *Dir.Inf.*, 2010, pp. 315-341.

[36] *Joint statement* approvato al termine ella riunione tenutasi a Bruxelles il 17/18 febbraio 2003 tra i rappresentanti dalla Commissione Europea e del CBP.

impugnati sulla base del primo motivo, cioè, in ragione fatto che il trattamento verteva su questioni di pubblica sicurezza, e pertanto non rientrava nella disciplina comunitaria sulla protezione dei dati, ragion per cui né la Commissione poteva deliberarne l'adeguatezza né il Consiglio, quale organo delle Comunità Europee, poteva regolarlo mediante l'accordo con gli USA. Gli USA e l'Unione Europea adottavano allora un accordo temporaneo (*«interim agreement»*[37]) , per permettere la continuazione del trasferimento dei PNR agli USA in attesa dell'accordo definitivo. Nel 2007 si stipulava un nuovo accordo, che consentiva un più ampio trattamento dei PNR, in ragione delle pressioni effettuate dal Dipartimento della sicurezza interna statunitense sulla Presidenza del Consiglio e la Commissione Europea. Tale accordo era adottato dal Consiglio quale organo del terzo pilastro dell'unione Europea (Cooperazione giudiziaria e di polizia in materia penale) e quindi non era soggetto al controllo della Corte di Giustizia.

Nel 2011, l'Unione Europea, quale istituzione che riuniva le competenze precedentemente suddivise nei c.d. Pilastri, firmava un nuovo accordo PNR con gli Stati Uniti. Tale accordo è entrato in vigore il 1 Luglio 2012 con il consenso del Parlamento europeo e l'approvazione del Consiglio dell'UE[38]. L'accordo prevede alcune garanzie a protezione dei dati, giudicate peraltro insufficienti dal Gruppo di Lavoro Articolo 29[39]. In Sudamerica, i dati PNR sono generalmente trasferiti alle autorità statunitensi senza che siano ancora stati stipulati, per quanto è noto, accordi internazionali in materia. In particolare, il governo brasiliano nel 2005 annunciava di aver autorizzato le compagnie aeree a fornire alle autorità statunitensi i dati dei passeggeri e di aver iniziato i negoziati

[37] 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. Firmato a Washington il 19.10.2006. Il testo dell'accordo è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy /docs /adequacy /pnr/ 2006 _ 10 _ accord_US_en.pdf* [consultato il 03/08/2014].

[38] COUNCIL OF THE EUROPEAN UNION. Council adopts new EU-US agreement on Passenger Name Records (PNR). Luxembourg, 26 April 2012 - 9186/12. Il testo è disponibile a *http://consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf.* [consultato il 05/07/2014].

[39] ARTICLE 29 WORKING PARTY. Letter from the Article 29 Working Party addressed to LIBE Committee of the European Parliament regarding the new draft agreement on the transfer and use of Passenger Name Records, known as PNR data. Brussels, 6 January 2012. Il testo è disponibile a *http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf* [consultato il 14/08/2014].

con il governo degli Stati Uniti in vista della conclusione di un accordo PNR Brasile – USA[40]. Gli accordi sul trasferimento dei PNR evidenziano come esigenze di sicurezza possano condurre a limitazioni della *privacy* e della protezione dei dati. Queste esigenze, oltre che le pressioni politiche statunitensi, hanno indotto l'Unione a conformarsi alle richieste di trasferimento, anche se il compromesso emerso non ha pienamente soddisfatto i difensori della *privacy*, e in particolare le stesse Autorità europee per la protezione dei dati. Gli accessi al database delle operazioni interbancarie SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), accessi effettuati dal governo statunitense nell'ambito del programma antiterrorismo TFTP (*Terrorist Finance Tracking Program*), hanno originato un analogo conflitto tra Stati Uniti e Unione Europea. Anche in questo caso una prima bozza di trattato per l'accesso ai dati SWIFT, frutto dei negoziati tra Stati Uniti e Commissione, era respinta dal Parlamento Europeo, che approvava poi una versione successiva, che aggiungeva alcune garanzie a tutela della *privacy* dei cittadini europei. Per assicurare una più efficace garanzia dei dati europei si adottava altresì una misura tecnologica: l'architettura del sistema informatico di Swift era modificata, in modo che i dati concernenti le operazioni intraeuropee rimanessero esclusivamente in Europa, non essendo più riportati nel centro dati statunitense di SWIFT.

Le rivelazioni di Edward Snowden, evidenziavano peraltro come gli Stati Uniti avessero violato o eluso i limiti sull'uso dei dati stabiliti dall'accordo. Di conseguenza il Parlamento Europeo chiedeva nel 2013 la revoca del trattato[41].

3. Il caso Snowden

Come già osservato nella prima sezione di questo articolo, i principali ISP e fornitori di servizi di rete sono basati negli Stati Uniti. La preminenza economica delle imprese statunitensi ha implicazioni politiche importanti, poiché tali imprese sono in grado di determinare, in modo confor-

[40] 'O Globo'. O mundo. «Governo brasileiro aceita compartilhar informações de passageiros com destino aos Estados Unidos». Pubblicato nel 26 febbraio 2005.

[41] PARLAMENTO EUROPEO. Risoluzione del Parlamento europeo del 23 ottobre 2013 sulla sospensione dell'accordo TFTP a seguito della sorveglianza dell'Agenzia per la sicurezza nazionale statunitense (*2013/2831(RSP)*). Il testo è disponibile a *http://www.europarl.europa.eu/sides/getDoc.do-?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//IT* [consultato il14/08/2014].

me ai propri interessi e a valori, la regolazione di Internet. Possono farlo predisponendo unilateralmente le modalità di funzionamento dei propri servizi e le regole cui gli utenti si debbono attenere, ma anche influenzando la definizione di standard tecnici o esercitando pressioni nei confronti dei decisori politici. Il ruolo politico di tali imprese è rafforzato dalla posizione tendenzialmente monopolistica di cui godono, grazie all'effetto di rete (l'attrattività delle reti più ampie), posizione che offre loro grandi spazi di azione, anche in contrasto agli interessi degli utenti. Inoltre, il fatto che i protagonisti di Internet siano situati negli Stati Uniti conferisce una posizione privilegiata al governo di questo paese, alla cui giurisdizione sono sottoposte tali imprese. Le imprese di Internet possono essere indotte o costrette a collaborare con il governo statunitense, fornendo a tale governo dati e strumenti per operazioni di sorveglianza sul terrorismo, ma anche per indagini giudiziarie, spionaggio militare e politico, e persino spionaggio industriale. È opportuno ricordare che le istituzioni economiche e politiche statunitensi, e i valori che le ispirano, hanno contribuito in modo decisivo allo sviluppo di Internet quale ambito di progresso e libertà. In particolare, le libertà garantite in questo paese all'iniziativa economica privata, così come alla ricerca scientifica e alla manifestazione di opinioni, accompagnate dal sostegno pubblico alle iniziative tecnologiche, hanno consentito che Internet nascesse quale rete aperta, si arricchisse di sempre nuove funzionalità e diventasse globale, conservando la capacità di favorire l'innovazione delle tecnologie e dei modelli economici, ma anche la creatività degli individui, e il dialogo politico e culturale[42].

Le rivelazioni dall'ex consulente della NSA (*National Security Agency* statunitense), Edward Snowden – l'esistenza di programmi di sorveglianza di massa, che contavano anche sulla complicità di altri paesi occidentali[43]–hanno però messo in luce il lato 'oscuro' del predominio statunitense sulla rete. Nel fatto che «gli Stati Uniti controllano Internet, le aziende americane profittano sproporzionatamente di Internet, i servizi di sicurezza statunitensi hanno accesso privilegiato a tutto che attraversa Internet» si è ravvisata una nuova forma di colonialismo, in cui si fondono profili economici e politici[44]. Tali rivelazioni hanno messo in discussione la

[42] Sulla 'generatività' di Internet, v. J.Zittrain, *The Generative Internet* (2006), 119 *Harvard Law Review* 1974.

[43] M.Shears, *Snowden and the Politics of Internet Governance* (2014). Security& Surveillance. Il testo è disponibile a *https://cdt.org / blog /snowden-and- the-politics-of-Internet-governance/* (03/08/2014).

[44] Dichiarazioni attribuite a P. Verveer da R. Hill, *Internet Governance: The Last Gasp of Colonalism, or Imperialism by Other Means?*, in R.Radu et al. (eds), *The Evolution of*

governance di Internet, oggi svolta attraverso organizzazioni private create in base alle leggi degli Stati Uniti e situate nel territorio degli Stati Uniti (ICANN e IETF), grazie alle quali gli Stati Uniti possono esercitare un'influenza anche sulle norme tecniche di funzionamento di Internet e sulla sua amministrazione.

Sulla scia del caso Snowden, numerosi governi hanno sostenuto, con diverse motivazioni, l'esigenza di passare a un nuovo ordine multilaterale. Come esempio si può citare la dichiarazione presentata dal governo del Pakistan – con il sostegno Ecuador, Venezuela, Cuba, Zimbabwe, Uganda, Russia, Indonesia, Bolivia, Iran e Cina – al Consiglio per i Diritti Umani nel settembre 2013, concernente le rivelazioni di Snowden, il fallimento dell'attuale sistema di governance di Internet e la necessità di un nuovo quadro internazionale[45]. Benché si possa dubitare della misura in cui tali richieste esprimano l'esigenza di una maggiore tutela dei diritti umani, piuttosto che quella di sottoporre Internet a un più intenso controllo politico finalizzato alla repressione del dissenso, il predominio statunitense su Internet sembra insostenibile a lungo termine, e vi è l'esigenza di trovare un diverso quadro istituzionale per il governo di questa infrastruttura globale.

In Europa, Germania, Francia e Spagna, hanno reagito con indignazione alle rivelazioni del monitoraggio di massa effettuato dalla NSA. In Germania l'opinione pubblica e i partiti di opposizione hanno chiesto spiegazioni al governo, il quale ha risposto assumendo un ruolo di leadership nella contestazione le pratiche di sorveglianza e spionaggio statunitensi. Il governo tedesco è giunto a proporre agli Stati Uniti di firmare un trattato bilaterale di non spionaggio, pur ribadendo che gli Stati Uniti rimanevano un partner fondamentale per la Germania e che, in particolare, che i negoziati del TTIP (*Transatlantic Trade and Investment Partnership*) non erano in discussione[46].

Nonostante l'apparente indignata sorpresa di alcuni capi di stato europei, emergeva successivamente, con il rilascio di nuovi documenti da parte dello stesso Snowden, che alcuni paesi europei, tra cui Francia e Regno Unito, avevano agito di concerto con la NSA nelle pratiche di sorveglianza globale e avevano condiviso con gli Stati Uniti enormi quantità di dati[47].

Global Internet Governance: Princiles and Policies in the Making , Springer and Schulthess, 2014. p. 81.

[45] M.Shears, *Snowden and the Politics ecc.* (2014). *op. cit.*

[46] V. *http://rt.com/news/170868-merkel- spy-scandal-serious/* [consultato il 03/08/2014].

[47] J.Follorou, *La France, précieux partenaire de l'espionnage de la NSA* (2014), Le Monde. Disponibile a *http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-parte-*

Il Direttore nazionale dell'intelligence USA, James Clapper, dichiarava, infatti, al Congresso degli Stati Uniti che lo stupore dei governi europei era almeno in parte ipocrita, poiché la sorveglianza era stata compiuta con il sostegno delle agenzie d'intelligence locali[48].

Anche in America Latina le reazioni alle rivelazioni di Snowden erano forti, soprattutto dopo che la stampa aveva reso noto che gli Stati Uniti stavano conducendo operazioni di spionaggio in diversi paesi sudamericani, tra cui Brasile, Colombia, Messico e Venezuela.

In particolare, tali operazioni non si limitavano alla prevenzione del terrorismo e della criminalità, ma si estendevano al controllo di Internet e delle comunicazioni telefoniche con finalità commerciali, per esempio, per cercare informazioni sull'industria petrolifera[49]. Questa situazione portava la Presidente del Brasile–che, come la Cancelliera tedesca, è stata oggetto di sorveglianza da parte dei servizi statunitensi – ad affermare al vertice del Mercosur del 12 luglio 2013 che «qualsiasi atto di spionaggio che violi i diritti umani, soprattutto il fondamentale diritto alla *privacy*, e minacci la sovranità delle nazioni, merita di essere condannato da qualsiasi paese che si definisca come democratico[50]». Le rivelazioni di Snowden portavano la Presidente del Brasile a cancellare un viaggio negli Stati Uniti nel mese di ottobre 2013 e ad accelerare l'emanazione del c.d. «Marco Internet Civil, la legge che «stabilisce principi, garanzie, diritti e obblighi per l'uso dell'Internet in Brasile»(Legge n 12,965, del 23 aprile 2014[51]). A conferma del ruolo di leadership assunto dalla Germania e dal Brasile nelle rispettive aree d'influenza – Unione Europea e America Latina - Brasile e Germania presentavano una proposta di risoluzione comune sulla *privacy* online nell'Assemblea generale delle Nazioni Unite, che era approvata all'unanimità[52]. Di conseguenza, l'Assemblea generale delle Nazioni Unite chiedeva all'Alto commissario per i diritti umani di preparare una relazione sul diritto alla *privacy* nell'era digitale.

naire-de-l-espionnage-de-la-nsa_3522653_651865.html [consultato il 03/08/2014].

[48] J.Borger, *GCHQ and European spy agencies worked together on mass surveillance* (2014). The Guardian. Disponibile a *http://www.theguardian.com /uk-news/2013 /nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden* [consultato il 03/08/2014].

[49] V. Latin America and Edward Snowden: South Americans in glasshouses. The Economist. Disponibile a *http://www.economist.com/ node / 21582154 / print* [consultato il 03/08/2014].

[50] V. Latin America and Edward Snowden: South Americans in glasshouses. Cit.

[51] Il testo della legge è disponibile (in portoghese) a *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l1296 5.htm* [consultato il 03/08/2014].

[52] United Nations General Assembly. Resolution 68/167 onThe right to *privacy* in the digital age. Adopted on 18 December 2013. Il texto è disponibile a http://www.un.org/ga/search/view_doc.asp?symbol = A/RES/68/167. [consultato il 05/06/2014].

4. La discussione sul regolamento sulla protezione dei dati

La Proposta della commissione per un Regolamento Generale sulla Protezione dei Dati Personali ha suscitato ampie discussioni tra l'Unione da un lato e le imprese di Internet e il governo statunitense dall'altro, dibattito che ha risentito delle rivelazioni di Snowden[53]. Alcuni aspetti del regolamento rispondono alle esigenze delle imprese globali di Internet: la sostituzione di un'unica normativa europea alle diverse discipline nazionali oggi esistenti; l'indicazione di un'unica autorità per la protezione dei dati quale soggetto competente per tutte le questioni concernenti un certo titolare, quella dove è stabilito il titolare stesso; la creazione di un organo di appello per assicurare la coerenza tra le decisioni nazionali[54]; l'esplicita estensione delle immunità dei provider anche alle violazioni della protezione dei dati; la possibilità che l'adozione unilaterale di regole vincolanti sulla protezione dei dati da parte di un'impresa stabilita in un paese estero possa costituire una base giuridica sufficiente al trattamento dei dati anche in mancanza di un'adeguata disciplina autoritativa. Adottando il modello tipicamente statunitense dell'autoregolamentazione, il Parlamento europeo ha introdotto nella bozza predisposta dalla Commissione il sigillo europeo per la protezione dei dati, rilasciato dalle autorità di protezione dei dati per garantire che il titolare o il responsabile è in conformità al regolamento (art. 43). Il sigillo limita la responsabilità amministrativa dei titolari, e consente loro di trasferire dati all'estero senza dover ottenere volta per volta l'autorizzazione delle autorità di protezione dei dati[55]. Altri aspetti del regolamento, invece, hanno incontrato l'opposizione delle imprese e del governo statunitensi: la previsione di regole tecniche per la *privacy by design* stabilite dalla commissione, anziché da organizzazioni per la standardizzazione aperte e basate sulla partecipazione di tutte gli interessati (multi-stakeholderism); l'eccessivo rigore degli obblighi di

[53] C.Kuner et al., *The proposed EU data protection regulation two years later (2014). Privacy & Security Law Report*, 13 *PVLR* 8. Bureau of National Affairs, p. 1.

[54] Nel Consiglio dell'Unione europea, peraltro, sono emersi profondi disaccordi circa la competenza unica (one-stop shop) e il meccanismo di appello. Così osservano Kuner et al. (2014), *The proposed ecc. op. cit.*, p. 6: Diversi blocchi di stati membri hanno opinioni contrastanti in merito al regolamento: alcuni vogliono raggiungere presto un accordo su di esso (ad esempio, Francia, Italia e Spagna), altri sono completamente opposti (ad esempio, in Danimarca, Svezia e Regno Unito), e il terzo gruppo sta nel mezzo. La posizione assunta dalla Germania sarà fondamentale per vedere se il Consiglio possa raggiungere un accordo".

[55] C.Kuner et al *The proposed ecc.* (2014), *op. cit.*, p. 3.

notifica di 'data breaches' (poi attenuati nelle modifiche introdotte dal Parlamento); la potenziale applicabilità della normativa europea a ogni trattamento che coinvolga interessati situati in Europa anche quando il sito che esegue il trattamento non abbia specifica destinazione europea[56]. Il tema più controverso è stato però quello del diritto all'oblio, o del 'diritto a essere dimenticati', la cui portata innovativa era stata enfatizzata dalla Commissaria Reding. Nonostante le affermazioni rassicuranti della stessa Reding e della Commissione, secondo cui tale diritto non avrebbe limitato le libertà di espressione, informazione e ricerca storica[57], il possibile conflitto era immediatamente identificato ed enfatizzato dagli osservatori statunitensi. Secondo l'opinione prevalente negli Stati Uniti, l'affermazione di un diritto dell'interessato alla rimozione delle informazioni che lo riguardano metterebbe a rischio le libertà altrui, e in particolare le libertà di esprimere opinioni su terzi, di comunicare informazioni, e di accedere alle stesse. Le potenzialità censorie di tale diritto erano addirittura assimilate agli interventi su Internet attuati da regimi oppressivi, come la Cina e alcuni governi del Medio Oriente[58], e si affermava che la disciplina del 'diritto ad essere dimenticati', imponendo a Google di rispondere alle richieste di rimozione, avrebbe trasformato Google stessa in un riluttante «censore capo per l'Unione europea[59]». Peter Fleisch, Global *Privacy* Council di Google. paventava l'adozione di un'«interpretazione estremistica» del «right to be forgotten», secondo la quale gli interessati non solo avrebbero potuto chiedere alle autorità competenti di ordinare la rimozione ai fornitori dei contenuti, ma si sarebbero potuti rivolgere direttamente agli intermediari di Internet, chiedendo loro di rimuovere informazioni personali, e gli intermediari sarebbero stati responsabili se si fossero rifiutati di ottemperare nei casi in cui l'informazione avrebbe invece dovuto essere rimossa (secondo il successivo giudizio dell'autorità competente[60]).

[56] V. *http://www.insideprivacy.com/international / european-union / draft-report-on-the-proposed-eu-data-protection-regulation-released/* [consultato il 14/08/2014].
[57] V.Reding, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5* (22/01/2012). Disponibile a *http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF* [consultato il 15/08/2014].
[58] J.Rosen, *The Delete Squad Google, Twitter, Facebook and the new global battle over the future of free speech* (2013), The New Republic, (April 29): pp. 1-7.
[59] J.Rosen, *The right to be forgotten (2012). Stanford Law Review Online*, pp. 64:88-92.
[60] V. anche P.Korenhof et al., Timing the Right to Be Forgotten: A study into «time» as a factor in deciding about retention or erasure of data (2004). Paper written by panelists of the «Timing the Right to Be Forgotten» panel at the Computers, *Privacy* and Data Protection Conference 2014 Panel organized by Paulan Korenhof and the Tilburg Institute for Law, Technology, and Society TILT); G.Sartor, The right to be forgotten:

Queste osservazioni critiche erano accolte in qualche misura dal Parlamento Europeo, il quale, modificava il testo predisposto dalla Commissione, eliminando il riferimento a un «right to be forgotten» sostituito dal richiamo del tradizionale diritto alla cancellazione (erasure) di dati elaborati senza una base giuridica[61]. Il Parlamento introduceva altresì tra le condizioni per la cancellazione la presenza di una decisione «final and absolute» di una «court or regulatory authority» suggerendo forse come il giudizio di illegittimità, presupposto per la cancellazione, dovesse essere affidato ad autorità pubbliche competenti, piuttosto che agli intermediari.

Questo apparente avvicinamento tra posizioni europee e statunitensi sulla rimozione di informazioni da Internet era però interrotto dalla decisione della Corte di Giustizia sul caso Google-Spain, che adottava proprio l'interpretazione qualificata come 'estremistica' dal general legal counsel di Google, Peter Fleischer. I giudici, infatti, conferiscono all'interessato il diritto rimozione di link a notizie legittimamente pubblicate e distribuite in rete, un diritto esercitabile direttamente nei confronti dei motori di ricerca. Questi sono ritenuti responsabili per la continuata accessibilità di tali notizie, ogni qualvolta la *privacy*, nel corso del tempo, sia divenuta prevalente rispetto libertà di espressione, essendo diminuito l'interesse pubblico alla conoscenza delle stesse notizie.

5. Google Spain: un conflitto giuridico o politico?

Il processo davanti alla Corte di Giustizia è stato caratterizzato dalla partecipazione di diversi attori, portatori di diversi valori e interessi, che hanno assunto posizioni contrastanti. L'avvocato generale Jääskinen[62] aveva proposto una decisione antitetica rispetto a quella adottata dalla Corte: egli non solo aveva escluso che Google potesse essere responsabile, ma aveva considerato la stessa immune rispetto a ordini di rimozione, quando si fosse limitata a svolgere la propria fisiologica funzione di

dynamics of privacy and publicity, in L.Floridi (editor), The protection of information and the right to privacy (2014), Springer.

[61] Sulle modifiche proposte dal Parlamento, v. C.Kuner et al. (2014), *The proposed ecc.* op. cit.

[62] Conclusioni dell'Avvocato Generale Niilo Jääskinen., presentate il 25 giugno 2013 (1), nella Causa C-131/12 Google Spain SL e Google Inc.contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.

indicizzare tutti i contenuti in rete, non essendo, in tale ruolo, titolare di un'elaborazione di dati personali. Inoltre, la preminenza della libertà di espressione, secondo la tradizione nordeuropea, più vicina in questo riguardo all'esperienza statunitense, conduceva Jääskinen a ritenere che la responsabilizzazione del motore di ricerca avrebbe indotto lo stesso alla rimozione dei link a ogni materiale contestato, e che ciò avrebbe comportato un inammissibile pregiudizio alla libertà di espressione-comunicazione di chi avesse pubblicato un'informazione on-line. Anche i pareri degli Stati membri divergevano su importanti questioni. I governi spagnolo, italiano e polacco, nonché la Commissione, ritenevano che «l'autorità nazionale possa ordinare direttamente al gestore di un motore di ricerca di rimuovere dai propri indici e dalla propria memoria intermedia informazioni contenenti dati personali pubblicati da terzi, senza doversi rivolgere previamente o simultaneamente all'editore della pagina web nella quale compaiono tali informazioni». Invece il governo polacco escludeva la legittimità della rimozione dagli indici di un motore di ricerca di informazioni lecitamente pubblicate su Internet[63].

I governi greco, austriaco e polacco, nonché la Commissione affermavano che si potesse dar luogo alla rimozione di dati dagli indici solo nelle ristrette condizioni previste per l'opposizione al trattamento, di cui all'art. 14 della direttiva, cioè in presenza di motivi preminenti e legittimi attinenti alla situazione particolare degli interessati, e «non per il semplice fatto che tali persone ritengano che tale trattamento possa arrecare loro pregiudizio o che esse desiderino che i dati costituenti l'oggetto di detto trattamento cadano nell'oblio[64]». Inoltre i governi greco e austriaco reputavano «che la persona interessata debba rivolgersi all'editore del sito web in questione», anziché al motore di ricerca[65].

Più ampia possibilità di rimozione, ma sempre condizionata a un pregiudizio dell'interessato, a norma dell'art. 7 (f) della direttiva, era affermata invece dai governi spagnolo e italiano[66]. Secondo la Commissione e i governi spagnolo ed italiano, il fatto che l'informazione sia stata pubblicata regolarmente e continui a essere disponibile nella pagina web del titolare iniziale del trattamento non esclude gli obblighi del motore di ricerca. Il governo della Polonia aveva sostenuto, al contrario, che la liceità della

[63] Corte di Giustizia, Sentenza della Corte (Grande Sezione) del 13 maggio 2014), nella Causa C-131/12, § 65.
[64] Ivi, § 90.
[65] Ivi, § 90.
[66] Ivi, § 91.

pubblicazione on line escluderebbe l'obbligo di rimozione[67]. La Corte è andata al di là delle opinioni di tutti i governi intervenuti nel processo. Essa ha affermato, accogliento la tesi dei governi italiano e spagnolo, che «il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita[68]». Secondo la Corte, inoltre, la richiesta di rimozione da parte dell'interessato può essere rivolta direttamente al motore di ricerca, senza l'intervento di un'autorità giudiziaria o amministrativa e senza richiedere la prova di un pregiudizio effettivo all'interessato. Mentre i governi italiano e spagnolo ritenevano possibile «bloccare l'indicizzazione dei dati nella misura in cui arrecasse un pregiudizio all'interessato[69]», la Corte affermava che il diritto all'oblio non presuppone un pregiudizio. La persona interessata ha il diritto incondizionato di ottenere la rimozione delle informazioni collegate al suo nome, diritto che prevale «non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse [del ...] pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona». La prevalenza presuntiva della *privacy* viene meno solo «qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi». La decisione della Corte si basa quindi sugli assunti della lesività dell'aumento di accessibilità fornito dall'indicizzazione, della prevalenza almeno presuntiva dell'interesse alla *privacy* rispetto alla libertà d'informazione, anche rispetto a informazioni legittimamente pubblicate, e dell'irrilevanza del ruolo neutrale degli intermediari rispetto alla responsabilità per violazioni della protezione dei dati. La decisione del caso Google-Spain ha suscitato forti reazioni da parte degli operatori di Internet. Google pur criticando la decisione della Corte, ha iniziato a dar seguito a essa, offrendo un'interfaccia web nella quale gli interessati possano esprimere le proprie doglianze, e procedendo a rimuovere i link contestati, molti dei quali riguardano informazioni di apparente interesse

[67] Ivi, § 65.
[68] Ivi, § 88.
[69] Si utilizza 'interessato' qui nel senso del Codice *Privacy* Italiano.

pubblico. Questo esito censorio è stato interpretato da alcuni come una conferma dell'assurdità della decisione da Corte, che obbliga i provider a esercitare un ruolo improprio, e da altri invece come cinica scelta tattica di Google, che rifiuta di essere selettiva nelle proprie scelte di rimozione, al fine di screditare la decisione dei giudici e ridurre i propri costi[70]. Non si vede peraltro perché Google dovrebbe procedere a rimozioni più selettive, sottoponendosi al rischio di possibili sanzioni nel caso che le proprie valutazioni non dovessero coincidere con l'eventuale successiva decisione autoritativa[71].

Sul tema è intervenuto recentemente Jimmy Wales, il fondatore di Wikipedia, il quale ha qualificato l'esercizio del diritto a essere dimenticato come «profondamente immorale», poiché «la storia è un diritto umano e una delle peggiori cose che una persona possa fare è cercare di tacitare un altro[72]». Secondo Lila Tretikov, direttore esecutivo della Wikimedia Foundation (l'ente che gestisce Wikipedia) «la Corte europea ha abbandonato la sua responsabilità di difendere uno dei diritti più importanti e universali, il diritto di cercare, ricevere e trasmettere informazione», e di conseguenza «risultati di ricerche accurate stanno sparendo in Europa senza spiegazione pubblica, senza prova reale e senza esame giudiziale, di modo che ne risulta un'Internet crivellata di buchi di memoria alla Orwell[73]». Sembra indubbio che questa decisione contribuirà ad accrescere il divario tra Europa e Stati Uniti in materia di protezione dei dati. Infatti, la costruzione della Corte sembra del tutto incompatibile con alcuni principi fondamentali dell'ordinamento giuridico statunitense. Essa è in evidente conflitto con la libertà di parola garantita dalla costituzione statunitense: non solo la Corte afferma che la *privacy* può limitare la libertà di espressione, ma attribuisce alla prima un ruolo almeno presuntivamente prevalente sulla seconda. Inoltre la tesi della Corte appare incompatibile con l'idea dell'immunità del provider rispetto alle informazioni prodotte da terzi, immunità conferita dal Communication Decency Act (CDA) statunitense e interpretata in modo assai esteso dai giudici americani.

[70] Notizia riportata in J.Owen. *Right to be forgotten: Google accused of deliberately misinterpreting court decision to stoke public anger* (2014). The Independent, 3 giugno.
[71] Come si è osservato, l'anelito all'oblio prevale (quasi) sempre e impone al gestore del motore di ricerca, se allertato, di intervenire per correggere il proprio sistema di indicizzazione, v. A.Palmieri e R.Pardolesi, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google* (2014), *Nuovi Quaderni del Foro italiano*, Quaderno n. 1 (27 maggio 2014), p. 7.
[72] S.Curtis e A.Philipson, *Wikipedia founder: EU's right to be forgotten is 'deeply immoral'* (2014), The Independent, (13 agosto).
[73] S.Curtis e A.Philipson (2014), *Wikipedia founder ecc. op. cit.*

Nella decisione della Corte manca anzi ogni riferimento alle limitazioni della responsabilità del provider stabilite dalla Direttiva sul commercio elettronico, benché tali limitazioni siano state ribadite, anche rispetto alla violazione delle norme sulla *privacy*, nell'Articolo 2, comma 3 della proposta di Regolamento Generale sulla Protezione dei dati[74]. Sembra quindi inevitabile che la scelta della Corte favorirà alla divisione di Internet secondo linee nazionali (o regionali), accrescendo la 'balcanizzazione' della rete già in atto rispetto ai paesi che adottano forme più o meno intense di censura: i link a dati da dimenticare saranno inaccessibili agli utenti europei, rimanendo invece a disposizione degli statunitensi. Il Sudamerica, come osservavamo, sembra poter adottare una posizione intermedia tra Stati Uniti ed Europa almeno nel caso brasiliano: pur non escludendo la soggezione dei provider agli ordini autoritativi di rimozione motivati dal diritto all'oblio, la limitazione della responsabilità degli intermediari sembra escludere che questi possano essere soggetti a sanzione per aver respinto richieste private di rimozione, tranne nell'ipotesi di immagini, video o altri materiali contenenti nudità o atti sessuali di carattere privato.

6. Conclusione

Come si è illustrato nelle pagine precedenti, nella disciplina della protezione dei dati, e in particolare nella regolazione del diritto a essere dimenticati (la rimozione e dell'occultamento, totale o parziale, di informazioni personali da Internet), si contrappongono diversi valori, che hanno diversa importanza in diversi ordinamenti. In particolare, alla preminenza assoluta della libertà di espressione nel sistema giuridico statunitense si contrappone il rilievo della protezione dei dati in Europa, rilievo che è divenuto preminenza presuntiva nella decisione Google-Spain. Alla fiducia nella libertà economica e nel progresso tecnologico tipiche della cultura statunitense si oppongono i più sospettosi atteggiamenti degli europei. Inoltre, negli Stati Uniti l'atteggiamento negativo rispetto alle intromissioni pubbliche nella vita privata dei cittadini è spesso superato di fronte alle pretese esigenze della sicurezza interna e internazionale, mentre gli europei, pur più propensi ad accettare i limiti posti dall'interesse pub-

[74] Secondo il quale il regolamento si applicherà «without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive».

blico alle proprie attività, sono meno sensibili rispetto alle minacce alla sicurezza. Questi diversi atteggiamenti si traducono in diverse valutazioni giuridiche: ciò che agli uni appare garanzia della dignità e personalità dell'interessato appare agli altri un'inaccettabile limitazione della sfera di libertà dell'individuo.

Ai diversi valori giuridici si affiancano diversi interessi di soggetti pubblici e privati. Innanzitutto l'interesse degli utenti dei motori ad avere accesso alla massima quantità di informazione e a ottenere risposte affidabili, nel senso di risposte che riflettano lo stato delle informazioni disponibili in rete. A questo interesse si unisce l'interesse di chi carica informazioni in rete, e in particolare di chi è l'autore di tali informazioni, a raggiungere la sfera più ampia possibile di lettori e l'interesse delle imprese di Internet a offrire la massima quantità di informazioni ai propri utenti, e a evitare i costi e i rischi connessi all'esercizio di una funzione censoria. A tali interessi si oppone l'interesse dell'individuo a rimuovere informazioni personali pregiudizievoli o comunque sgradite. Gli Stati Uniti sono interessati a mantenere la superiorità delle proprie imprese mentre gli europei sono interessati a limitare tale superiorità e a promuovere le attività delle proprie. In particolare, gli europei non desiderano che i vincoli che essi pongono alle proprie imprese si traducano in una limitata competitività delle stesse rispetto alle imprese statunitensi, esonerate da tali vincoli.

Gli Stati Uniti desiderano conservare la propria preminente influenza sulla governance di Internet, per sostenere a livello globale i propri valori (libertà di espressione, libertà economiche, ecc.) ma anche per tutelare i propri interessi economici e politici. L'Unione europea è interessata a esercitare una maggiore influenza su Internet, per i medesimi scopi, ma con riferimento a valori (*privacy*, dignità, diversità culturale) e interessi parzialmente diversi. Lo stesso può dirsi per i governi di altri paesi, in particolare nel Sudamerica.

La sentenza della Corte si presta a essere interpretata come una decisa affermazione della prospettiva europea, in aperto contrasto con quella statunitense. Ciò può contribuire a rendere tale decisione accettabile e anzi gradita ai cittadini e ai soggetti politici europei, anche a causa della diffusa irritazione nei confronti degli Stati Uniti e delle imprese di Internet, accresciutasi dopo le rivelazioni di Snowden. Alcune pratiche dei principali fornitori di servizi di Internet nella gestione dei dati degli utenti europei (la profilazione degli utenti, l'estesa conservazione dei loro dati, la combinazione di dati concernenti diversi servizi, la commercializzazione di tali dati, ecc) hanno infatti contribuito a generare un sentimento nega-

tivo, la cosiddetta «Googlephobia». Tale sentimento è stato rafforzato dal comportamento fiscale degli stessi fornitori, consistente nell'adozione di strategie tese a minimizzare l'imposizione, trasferendo i profitti negli stati che, all'interno o all'esterno dell'Unione europea, offrissero condizioni più favorevoli.

Infine, il caso Snowden ha da ulteriormente rafforzato quest'attitudine, dandole una connotazione politica, oltre che economica.

È impossibile specificare con precisione il ruolo che i sentimenti appena descritti possono aver giocato nella decisione della Corte. Certamente essi non sono direttamente rilevanti per la giustificazione giuridica di tale decisione, restando estranei alle sue motivazioni giuridiche. Tuttavia, quei sentimenti possono aver contribuito a determinarla, dandole legittimità 'politica' quale scelta a favore dei valori e dei cittadini europei contro il superpotere economico degli operatori statunitensi di Internet e il superpotere politico del loro governo. Resta da vedere se questo sentimento rimarrà saldo di fronte alle implicazioni operative della decisione della Corte. L'accresciuta tutela dell'autodeterminazione sulle proprie informazioni giustificherà davvero, per i cittadini dell'Unione, la compressione della loro libertà d'informazione? Saranno molte le informazioni d'interesse pubblico a essere rese inaccessibili in seguito alle richieste di rimozione e come inciderà tale censura sul dibattito pubblico? E gli obblighi nascenti dal diritto a essere dimenticati (in particolare, l'onere di valutare correttamente caso per caso ogni richiesta di rimozione) pregiudicheranno la capacità competitiva delle imprese europee rispetto alle grandi concorrenti statunitensi, che meglio possono adempiere a tali obblighi, grazie alle superiori risorse economiche e organizzative? I cittadini europei preferiranno accedere ai servizi di Internet offerti ai cittadini statunitensi piuttosto che a quelli europei, per aver accesso a informazioni più complete, usando le tecniche oggi adottate nei paesi governati da regimi repressivi, ad esempio, accedendo a Internet mediante una rete virtuale privata (Virtual Private Network-VPN statunitense)? Solo il tempo potrà dare una risposta ai molti interrogativi sollevati dalla sentenza della Corte Europea, anche alla luce delle reazioni dei sistemi giuridici degli Stati membri a questa decisione innovativa, che pur basandosi su aspetti comuni alle tradizioni europee (*privacy* come aspetto della dignità e diritto all'oblio), trae da essi implicazioni non pienamente condivise neppure in Europa, oltre che avversate di là dall'Atlantico.

Abstract

The paper aims at comparing the perspectives of EU law and US law on data protection and providers' liability, in particular with regard to the Google-Spain case. First we examine the foundational differences between the approaches adopted in the EU and US, with some references also to South American legal systems. Then we examine some significant divergences or convergences between EU and US, such as in particular those emerging with regard to the transmission in the US of assengers name records (PNR) and SWIFT data, the Snowden case, the debate on the new European data protection regulation. Finally, we consider how political attitudes might have influenced the Google-Spain decisions, or in any case, the way in which it has been received in Europe.