LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze Politiche

Cattedra: Diritto Internazionale

IL CASO DATAGATE E LA TUTELA DELLA PRIVACY: ASPETTI DI DIRITTO INTERNAZIONALE E DI DIRITTO COMPARATO

RELATORE

Prof. Roberto Virzo

CANDIDATO

Rosario Parise

MATRICOLA

068842

ANNO ACCADEMICO: 2013/2014

INDICE

CAPITOLO 1

CAPITOLO 2

CONCLUSIONI

CAPITOLO 1

1.1. Premessa

In questo capitolo si passeranno in rassegna le principali contingenze che hanno caratterizzato lo scandalo *Datagate*[1], con l'intento di fornire le informazioni fondamentali sul caso integrate da un focus specifico sulla risonanza internazionale di questo episodio. A tal proposito, dopo una prima sezione essenzialmente esplicativa sugli eventi in questione, verranno esposte brevemente le posizioni e gli eventuali coinvolgimenti dei principali attori del caso, oltre ai provvedimenti messi in atto o auspicati dagli stessi in seno alle Nazioni Unite. A queste ultime, infine, sarà dedicata la conclusione del capitolo, con particolare attenzione alla risoluzione del 18 Dicembre 2013 e al relativo rapporto dell'ufficio dell'Alto Commissario delle Nazioni Unite per i Diritti Umani dal titolo "*The Right to Privacy in the Digital Age"*. Prima di iniziare la trattazione degli eventi è inoltre fondamentale effettuare delle precisazioni: la prima riguarda una sostanziale *vacatio legis* nel diritto internazionale in materia di spionaggio telematico e in tempi di pace, nonché in materia di tutela della privacy e della protezione dei dati personali in una normativa internazionale organica, la seconda è più associata agli avvicendamenti storici ancora in corso. Partendo proprio da quest'ultima osservazione, è doveroso puntualizzare che il caso *Datagate* non può dirsi concluso: l'eco dello scandalo risuona sovente nei rapporti diplomatici tra gli Stati, in particolar modo quando in queste relazioni sono coinvolti gli Stati Uniti. Si attendono ancora importanti sviluppi: Edward Snowden, il *whistleblower* che ha dato vita al caso, risiede attualmente in Russia, dove l'iniziale asilo politico annuale concesso nell'Agosto 2013 è stato esteso tramite un permesso di soggiorno della durata di tre anni. È ancora aperta l'inchiesta del procuratore federale tedesco Range sulle intercettazioni operate a danno del cancelliere Merkel. E ancora, varie sono le tematiche in discussione presso l'Assemblea Generale delle Nazioni Unite sul caso, le quali necessitano di una serie di ulteriori risoluzioni. Una proposta per un vero e proprio codice etico contro lo spionaggio spregiudicato e non regolamentato, che riaffermi il diritto alla riservatezza, è stata avanzata da Germania e Brasile e ha fatto diversi proseliti all'interno della GA sino ad arrivare alla

[1] Denominazione data dalla stampa italiana allo scandalo nato dalle rivelazioni dell'ex analista Edward Snowden, che riguardano il programma segreto di sorveglianza di massa messo in atto dalla *National Security Agency* statunitense.

risoluzione analizzata nel terzo paragrafo di questo capitolo. Persino i garanti per la privacy del mondo, durante la 35ma conferenza tenutasi a Varsavia nel Settembre 2013, hanno adottato una risoluzione in materia di educazione digitale in cui i governi si impegnano a promuovere un programma educativo comune per i propri cittadini. Svariati sono gli esempi che possono essere enunciati a tal proposito, a riprova del fatto che esistono innumerevoli spinte a dare una diversa, più ricca e più completa regolamentazione ad una materia che ancora il Diritto Internazionale non affronta compiutamente. Riallacciandosi dunque alla prima, importantissima osservazione sollevata in precedenza, senza dubbio correlata a quella sovresposta, si può affermare che manca una disciplina omogenea, specifica e internazionalmente condivisa che possa legittimamente disciplinare il caso *Datagate*. Se infatti lo spionaggio in tempi di guerra è oggetto di una disciplina *ad hoc* grazie al protocollo addizionale alle convenzioni di Ginevra del 1949[2], non si può dire lo stesso di una situazione corrispettiva in tempi di Pace. In questo caso, infatti, non esiste una regolamentazione precisa a cui poter far riferimento. Nel caso in cui vi fosse una violazione dei locali di una missione diplomatica (attraverso, ad esempio, l'introduzione di strumentazioni o qualsiasi altro agente esterno), si verificherebbe una inosservanza dell'art.22 della Convenzione di Vienna sulle relazioni diplomatiche del 1961. Tecnicamente, tuttavia, i dati raccolti sono stati spesso intercettati senza alcuna introduzione nei luoghi della missione, in quanto le intercettazioni avvenivano attraverso congegni fisicamente esterni ai summenzionati locali. Nondimeno, secondo l'interpretazione di Ronzitti, anche questa evenienza "*potrebbe realizzare una violazione della "pace della missione" ed un'offesa alla sua 'dignità', anche queste vietate dallo stesso articolo della Convenzione di Vienna*"[3]. Ciò che rende questo caso ancora più complesso sotto il profilo del diritto internazionale è dato dal fatto che si tratti principalmente di *cyberspionaggio*; ciò significa che grazie ai nuovi mezzi forniti dalla tecnologia cibernetica più all'avanguardia, le agenzie di pubblica sicurezza possono intraprendere attività di spionaggio senza il bisogno di varcare i confini territoriali di un altro Stato e violare di conseguenza la sovranità territoriale di quest'ultimo. La questione andrebbe dunque principalmente affrontata sul

[2] Ai sensi del paragrafo 1 dell'art.46 del suddetto protocollo, *"Malgrado ogni altra disposizione delle Convenzioni o del presente Protocollo, un membro delle forze armate di una Parte in conflitto caduto in potere di una Parte avversaria mentre svolge attività di spionaggio, non avrà diritto allo statuto di prigioniero di guerra e potrà essere trattato come spia".*

[3] Ronzitti, N., *Il Caso Snowden e le regole dello spionaggio,* Affari Internazionali, http://www.affarinternazionali.it/articolo.asp?ID=2369, (consultato il 17/07/2014).

piano della tutela della privacy, cosa che in effetti sta verificandosi in seno alle Nazioni Unite.

1.2. Datagate: il caso

Il *Big Bang* del caso *Datagate* esplode in data 6 Giugno 2013, quando il quotidiano britannico *The Guardian* pubblica in esclusiva le rivelazioni di un *whistleblower*, che per il momento rimarrà segreto, secondo cui i dati telefonici degli abbonati a Verizon, la più vasta rete di telecomunicazioni statunitensi, sarebbero stati forniti direttamente alla *National Security Agency* grazie ad una decisione top secret. Il giorno successivo viene rivelata all'opinione pubblica mondiale l'esistenza di Prism, un programma segreto varato nel 2007 e rinnovato cinque anni dopo dall'amministrazione Obama. Esso consiste nell'utilizzo, da parte dell'intelligence degli Stati uniti, di Google, Facebook, Microsoft e Yahoo! al fine di monitorare una serie di comunicazioni a danno di utenti statunitensi ed esteri al di fuori del territorio americano. Gli Internet provider negano la partecipazione al programma. Subito dopo è la volta di Tempora, un programma simile al Prism grazie al quale la GCHQ (servizi segreti britannici) raccoglierebbe un'enorme quantità di informazioni di privati cittadini tramite cavi sottomarini transatlantici usati per il trasferimento delle comunicazioni elettroniche.[4] Nel frattempo arriva la risposta del presidente Obama, il quale definisce il programma "*un necessario compromesso tra privacy e sicurezza*"[5]. Gli Stati Uniti d'America aprono un'indagine sul caso, mentre il 9 Giugno la talpa dell'NSA si rivela al mondo: Edward Snowden, ex analista dell'Agenzia di Sicurezza Nazionale statunitense ed ex agente della CIA, da Hong Kong rivela al Guardian la propria identità. Tre giorni dopo l'Unione Europea chiede ufficialmente spiegazioni riguardo al programma Prism. Il generale e direttore dell'NSA Keith Alexander, a tal proposito, difende strenuamente le posizioni dei servizi segreti e la legittimità del programma, controllato severamente, secondo tali dichiarazioni, dal potere legislativo e giudiziario americano. In data 13 Giugno viene aperta negli Stati Uniti un'inchiesta contro Snowden e ne viene richiesta, qualche giorno dopo, l'estradizione. La talpa del Datagate parte dunque alla volta di Mosca,

[4] MACASKILL,E., BORGER,J., HOPKINS,N., DAVIES,N.,BALL,J., "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications", The Guardian, 21 giugno 2013, disponibile su www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, (conslutato il 17/07/2014).
[5] OBAMA, B., *discorso a San Jose, California,* in data 7 Giugno 2013.

incrinando i già algidi rapporti tra il Cremlino e la Casa Bianca. Gli Stati Uniti, di conseguenza, gli annullano il passaporto, costringendo Snowden a rimanere bloccato nell'aeroporto moscovita. L'Equador, nel frattempo, si propone per fornire asilo politico, mentre emergono nuove rivelazioni secondo cui alcuni vertici europei sarebbero stati intercettati e diversi capi di governo monitorati. Il 29 Giugno si rivela un altro *whistleblower*: Wayne Madsen, ex luogotenente della marina con un passato nell'NSA, il quale ha rivelato il coinvolgimento di vari Paesi del vecchio continente nel programma di intercettazioni. Ciò produce un'immediata reazione europea e un congelamento dei rapporti diplomatici tra le due sponde dell'Atlantico. Pochi giorni dopo scoppia un gravoso caso diplomatico tra l'Europa e la Bolivia: il presidente Evo Morales è infatti stato costretto ad atterrare presso l'aeroporto di Vienna dopo un vertice a Mosca, in quanto alcuni Paesi europei, con il sospetto che Snowden fosse nascosto nell'aereo di Stato, non hanno immediatamente concesso il permesso di sorvolo. A questo proposito è da menzionare che la Convenzione di Chicago del 1944 prevede degli obblighi agli Stati per quanto riguarda l'aviazione civile, ma non per quanto riguarda gli aeromobili di Stato. Gli Stati in questione non hanno dunque agito contrariamente a tale norma di Diritto Internazionale. Ciononostante, nei due giorni successivi si sfiora una crisi internazionale, dal momento che il presidente boliviano accusa i Paesi europei di averlo sequestrato, mentre il ministro degli esteri Rubén Saavedra, anch'egli nella delegazione partita da Mosca, ha espresso la propria disapprovazione nei confronti del dipartimento degli Stati Uniti, a suo parere artefice dell'atterraggio forzato[6]. La Paz chiude dunque le porte a Washington, minacciando la chiusura dell'ambasciata americana; nel frattempo anche altri Paesi dell'America Latina (Venezuela e Nicaragua) offrono asilo a Snowden. Quest'ultimo rifiuta le proposte e chiede formalmente, in data 12 Luglio, temporaneo asilo alla Russia. Gli alleati europei, ancora privi di spiegazioni esaustive, si muovono in sede comune per chiedere chiarimenti immediati agli Stati Uniti: con una risoluzione adottata con 483 voti a favore e 93 voti contrari, l'Europarlamento ha "condannato con forza lo spionaggio delle rappresentanze dell'Unione europea"[7]. Il Parlamento Comune ha inoltre incaricato una delle sue

[6] PAREDES, I., *Francia, Italia, España y Portugal le negaron tránsito aéreo a Evo*, in La Razón, disponibile su http://la-razon.com/nacional/Francia-Italia-Espana-Portugal-Evo_0_1862813758.html, conslutato il 18/07/2014.
[7] *Europarlamento chiede chiarimenti immediati a Usa*, in l'Internazionale, disponibile su http://www.internazionale.it/news/datagate/2013/07/04/europarlamento-chiede-chiarimenti-immediati-a-usa/, (consultato il 18/07/2014).

commissioni di indagare approfonditamente sul caso per poi presentare una relazione finale nel Dicembre 2013. Sempre nel vecchio continente, in quei giorni, esplode un altro caso che vede, stavolta, la Francia al centro delle polemiche dell'opinione pubblica internazionale. Secondo il quotidiano transalpino *Le Monde*, la DGSE (i servizi segreti esteri francesi) raccoglierebbe in maniera sistematica tutti i segnali elettromagnetici che provengono da computer o telefoni. Ciò si verificherebbe per la totalità delle telecomunicazioni in maniera sistematica, e questi dati sarebbero archiviati per anni in banche dati clandestine (anche se questo sistema figurerebbe velatamente, secondo *Le Monde*, nei documenti parlamentari).

Nella prima metà di Luglio si scopre che la Microsoft ha collaborato in maniera massiccia al programma di intercettazioni della NSA: secondo una serie di documenti forniti al *Guardian* da Snowden, il colosso informatico ha permesso all'agenzia di sicurezza nazionale di entrare in una serie di servizi di mailing e di avere informazioni su un enorme quantitativo di videochiamate. Dopo l'acquisto di Skype da parte di Microsoft, infatti, le intercettazioni secondo la stessa NSA sono triplicate. Si tratterebbe essenzialmente di una raccolta di metadati (ovvero informazioni che rimandano ad altri dati), rielaborata da una direzione interna dei servizi segreti chiamata SSO (*Special source operation*). Secondo il *Guardian* questo sistema permetterebbe di filtrare i due terzi del traffico di tutta la rete. Altri documenti mostrano l'esistenza di un programma ancora più massivo e colossale: XKeystore, una chiave d'accesso per enormi database su internet, utilizzato dagli agenti NSA tramite la sola compilazione di un modulo e senza essere presa in esame da un qualsiasi organo del potere giudiziario. Secondo il quotidiano britannico si tratta del più grande sistema di intelligence online del mondo. Mentre infuria questo ennesimo scandalo, i rapporti diplomatici tra Russia e Stati Uniti si incrinano pericolosamente: viene confermato l'asilo ad Edward Snowden, malgrado vi siano stati vari incontri tra gli esponenti diplomatici dei due Paesi. Il presidente Obama si dichiara deluso dalla decisione di Mosca, tanto da cancellare il vertice con il presidente Vladimir Putin in programma a Settembre. Con la stessa delusione Yury Ushakov, importante personalità del Cremlino in campo di politica estera, commenta questa presa di posizione statunitense, aggiungendo che gli Stati Uniti "non sono ancora pronti per relazioni su basi egualitarie"[8]. Il mese di Agosto è

[8] *Cremlino "deluso" da cancellazione vertice Obama-Putin,* in l'Internazionale, disponibile su http://www.internazionale.it/news/datagate/2013/08/07/cremlino-deluso-da-cancellazione-vertice-obama-putin/, (consultato il 18/07/2014).

segnato da un'ennesima ondata di scandali: mentre la Gran Bretagna fa pressione sul *Guardian* riuscendo ad ottenere la distruzione di alcuni file, emerge dalla NSA l'ammissione che in alcuni, rarissimi casi, siano state violate, da parte di alcuni analisti, le restrizioni alla raccolta di dati disciplinate, oltre che dall'USA Patriot Act e dal Foreign Intelligence Surveillance Act, anche dalle norme dell'Executive Order 12333, che regolano le operazioni di intelligence. Queste dichiarazioni, provenienti dalla massima autorità dell'agenzia governativa, il generale Keith Alexander, entrano in contraddizione con quanto asserito dall'entourage della Casa Bianca, che aveva escluso totalmente questa eventualità. In aggiunta il *Der Spiegel* rivela che gli Stati Uniti avrebbero spiato anche le attività delle Nazioni Unite al Palazzo di vetro di New York, dove le intercettazioni sarebbero arrivate a oltre 450. Nei giorni successivi rischia di scatenarsi una crisi diplomatica con il Messico e il Brasile. Secondo il New York Times, infatti, la mailing list del presidente messicano, appena prima della sua elezione, sarebbe stata tenuta sotto controllo. Fonti meno specifiche arrivano anche sul presidente brasiliano Dilma Rousseff, le cui chat online sarebbero state comunque intercettate dai servizi segreti americani. Il ministro della giustizia brasiliano Eduardo Cardozo chiede immediate spiegazioni, accusando gli Stati Uniti i quali, nell'eventualità della conferma delle accuse del quotidiano newyorkese, sarebbero stati colpevoli di una gravissima violazione della sovranità brasiliana. Enrique Pena Nieto, presidente messicano, ha dichiarato a *Russia Today* di aver chiesto a Barack Obama di aprire un'indagine sugli atti della NSA. Gli attacchi agli Stati Uniti continuano su più fronti: il presidente Rousseff, dopo la convocazione dell'ambasciatore USA a Brasilia e una richiesta di chiarimenti immediati, rinvia l'incontro con Obama, ritenendo le spiegazioni sul caso insufficienti e asserendo che al momento non vi erano le condizioni per una visita. Anche Mark Zuckerberg, fondatore di Facebook, ha espresso critiche verso il modo in cui l'amministrazione statunitense ha condotto le indagini sul caso *Datagate*, accusando la Casa Bianca di mancata trasparenza. Dalla Francia, inoltre, piovono le accuse di *Le Monde* secondo cui la NSA avrebbe spiato 70 milioni di telefonate francesi. Immediatamente il premier transalpino Jean-Marc Ayrault ha richiesto chiarimenti. In questi stessi giorni si conclude il primo processo ad un ex tecnico dell'FBI sospettato di aver abusato del proprio ruolo; dichiaratosi colpevole, patteggia dunque 140 mesi di carcere. Da Strasburgo l'Europa reagisce alla serie di scandali attraverso misure più stringenti per la protezione dei dati personali: il 21 Ottobre la

Commissione per le libertà pubbliche del Parlamento Europeo ha approvato tali misure proposte dal Commissario per la Giustizia Viviane Reading. Il testo prevede pene severissime in caso di violazione: si arriva infatti ad un'ammenda pari al 2% del fatturato annuo per i gruppi attivi su Internet che utilizzano i dati degli utenti fuori dall'Europa senza ottenere il loro previo consenso. Inoltre la Commissione per le Libertà civili dell'Europarlamento ha approvato, nel giorno seguente, le relazioni Albrecht e Droutsas, che prevedono, oltre all'obbligo di ricevere una previa autorizzazione delle autorità nazionali per la privacy prima di fornire i propri dati personali, anche l'obbligo di cancellazione dei summenzionati dati in caso di richiesta degli utenti. La pena, rispetto alla richiesta della commissione, sale al 5% del fatturato annuo per le società che non osservano tali disposizioni. Un ulteriore monito arriva dall'Europarlamento, anche questa volta solo 24 ore dopo, tramite la risoluzione non vincolante presentata da SD, Alde e Verdi e approvata il 23 Ottobre, che invita la Commissione Europea alla sospensione degli accordi antiterrorismo con gli USA. Pur non avendo potere formale per l'interruzione di tali accordi, infatti, il Parlamento Europeo rivendica l'azione della Commissione allorché venga meno il sostegno dell'organo assembleare comunitario. Sempre nel cuore dell'Europa un'altra rivelazione potrebbe seriamente compromettere i rapporti diplomatici con gli alleati statunitensi: da Berlino, in quegli stessi giorni, arriva la notizia che il telefono cellulare del cancelliere tedesco Angela Merkel sarebbe controllato dall'intelligence americana. A questo proposito, a Washington arriva una telefonata dalla Cancelleria Federale. Obama rassicura Angela Merkel, assicurando che gli Stati Uniti non stavano intercettando le telefonate del cancelliere né lo avrebbero fatto in futuro. Non arriva tuttavia nessuna esclusione del fatto che ciò sia avvenuto in passato. A seguito delle rivelazioni del mese di Ottobre, Parigi e Berlino guidano una discussione concertata con gli altri leader europei, che in occasione di un vertice a Bruxelles si dichiarano fortemente preoccupati per lo scandalo *Datagate.* Pur confermando i rapporti di amicizia con gli alleati americani, si ipotizza, in seno al vertice, la sospensione della collaborazione internazionale nella lotta al terrorismo nel caso in cui venisse meno la fiducia tra gli Stati Uniti e i Paesi europei. Ulteriori ammonimenti arrivano dal presidente del Parlamento Europeo Martin Schulz, oltre che dal presidente della Commissione José Manuel Barroso (il quale ha ricordato, in una sua dichiarazione, le condizioni della Repubblica democratica tedesca, paventando una sorta di gestione "totalitaria" dell'informazione). Il presidente Obama

decide dunque di imprimere una svolta alla struttura dell'NSA, imponendone un'immediata riforma e riducendone la discrezionalità in nome della privacy dei suoi cittadini. Nel frattempo un gruppo di esperti esterni si prepara a presentare un rapporto confidenziale dettagliato al Presidente. Le relazioni diplomatiche con la Germania diventano ancora più gelide alla fine del 2013, tanto che il cancelliere tedesco minaccia una possibile interruzione dei rapporti di libero scambio con l'alleato transatlantico dopo la scoperta di un'importante base britannica di spionaggio proprio a Berlino, e accusando l'NSA di essere simile alla Stasi (servizi segreti della Repubblica Democratica Tedesca), riprendendo le parole di Barroso. A Gennaio Obama invita Angela Merkel a Washington per discutere della crisi diplomatica; si apre così uno spiraglio per mettere in atto una trattativa tra Germania e Stati Uniti al fine di creare un accordo anti-spionaggio. In questo stesso periodo il presidente americano incontra le personalità più rilevanti dell'intelligence statunitense per riformare l'agenzia governativa con a capo il generale Alexander. Le proposte del presidente verranno enucleate in un discorso pronunciato il 17 Gennaio 2014; esse stabiliscono la fine della raccolta indiscriminata di metadati, dunque la fine del programma Prism così come è stato concepito, l'accesso ai dati di alcuni specifici tabulati telefonici solo previa autorizzazione di un tribunale, l'interruzione, ove sia presente, della sorveglianza elettronica ai capi di Stato alleati, una maggiore protezione della privacy dei cittadini non statunitensi e la richiesta di formazione, ad opera del Congresso, di un libero comitato di *public advocates* con il compito di intervenire in casi di violazione della privacy da parte di agenzie governative. Oltre a ciò, dieci giorni dopo, Keith Alexander viene sostituito dall'ammiraglio Michael Rogers nel ruolo di capo dell'NSA. Se da una parte il discorso di Obama riceve il plauso francese, che dichiara restaurati i buoni rapporti diplomatici, d'altra parte il mancato accordo anti-spionaggio con la Germania ha portato il cancelliere tedesco a proporre una rete europea anti-intercettazioni: in questo caso le informazioni, le mail e altri dati che provengono dal vecchio continente non dovrebbero passare automaticamente attraverso i server dei provider statunitensi. Il cancelliere Merkel ha inoltre proposto una maggiore omogeneità, a livello europeo, delle norme dei vari Paesi sulla protezione dei dati. La riforma annunciata a Gennaio dal presidente degli Stati Uniti si concretizza in un vero e proprio provvedimento legislativo due mesi dopo. Nello stesso periodo il settimanale tedesco *Der Spiegel* rivela l'esistenza di 300 rapporti sul cancelliere tedesco: le tensioni con la Germania si acuiscono. In data 4 Giugno il procuratore federale Harald Range ha reso

noto al Bundestag che aprirà un'inchiesta sulle attività di sorveglianza. Gli ultimi importanti avvenimenti sul caso *Datagate,* infine, enfatizzano le crescenti avversioni tra i due alleati, mostrando il palese clima di sfiducia che governa i rapporti diplomatici tra questi Paesi: nel mese di Luglio, infatti, i procuratori federali irrompono in casa di un impiegato dell'intelligence tedesca, accusato di aver passato più di 200 documenti alla CIA. Due giorni dopo è la volta di un altro arresto sempre ai danni di un dipendente dei servizi segreti tedeschi, questa volta accusato di avere trasmesso informazioni alla NSA. Concludendo, in data 10 Luglio, la Germania annuncia l'espulsione di un agente della CIA da Berlino, accusato di essere a contatto con i due agenti fermati qualche giorno prima. Frank-Walter Steinmeier, ministro degli esteri tedesco, ha considerato quest'atto una giusta replica alla rottura dei rapporti di reciproca fiducia tra Germania e Stati Uniti.

Si attendono ancora importanti evoluzioni sul caso, come mostrano evidentemente gli eventi sin ora trattati. La storia e le inchieste, nonché un compiuto iter legislativo internazionale, devono ancora fare il proprio corso per arrivare a soddisfacenti ed esaustive conclusioni.

1.3. Le posizioni internazionali e in particolare la posizione europea

In questa sezione si è pensato di analizzare il *Datagate* facendo riferimento al comportamento dei vari Stati e agli sviluppi legislativi sul caso ancora in corso in seno alle Nazioni Unite. Come si evince dalla trattazione sovresposta, lo scandalo ha colpito su più fronti a livello internazionale, diventando fonte di attrito nei rapporti diplomatici tra gli Stati Uniti e svariati Paesi. Gli ultimi avanzamenti legislativi che stanno verificandosi al Palazzo di Vetro, così come a Ginevra presso l'Alto Commissariato per i Diritti Umani, altro non sono che lo speculare risultato di una serie di pressioni internazionali da parte dei Paesi maggiormente lesi dallo spionaggio di massa, oltre che di una serie di ONG e di gruppi di cittadini organizzati, i quali proprio online hanno trovato i mezzi per far fronte comune contro le interferenze indiscriminate dell'intelligence americana[9].

Le prime, importanti riforme hanno inizio proprio negli Stati Uniti, dove la Casa

[9] Uno degli esempi più interessanti è quello del portale *https://optin.stopwatching.us/*, che ha trasformato la protesta in un'enorme petizione via internet, o ancora il manifesto online che richiede alle Nazioni Unite un *Bill of Digital Rights* ideato e firmato da oltre 500 tra i più importanti scrittori mondiali, tra cui 5 premi Nobel, dal titolo *A stand for Democracy in the Digital Age.*

Bianca ha più volte rivisto la propria posizione in merito al caso, dal momento che una serie di rivelazioni sempre più compromettenti hanno costretto Barack Obama a prendere provvedimenti nel modo più tempestivo e risoluto possibile. Come presentato nella rassegna sul *Datagate* trattata nel primo paragrafo, il presidente americano ha incaricato una commissione di esperti di redigere un rapporto, poi consegnato a Novembre e pubblicato il mese successivo. Esso invoca la protezione dello stato di diritto, della democrazia, dei diritti civili, del diritto alla sicurezza e al contempo delle alleanze strategiche e della privacy degli individui. I "saggi" americani chiedono al governo degli Stati Uniti d'America il rispetto di due fondamentali forme di sicurezza: la *national security* e la *personal privacy*; si richiedono inoltre importanti passi per la tutela dei cittadini non americani, oltre che provvedimenti concreti al fine di promuovere trasparenza e *accountability*, affinché eventuali infrazioni non restino nell'impunità. Si enfatizza, nel testo, l'importanza delle corti al fine di dare autorizzazioni a procedere, avversando apertamente qualsiasi forma di *data mining* per scopi di intelligence[10]. La riforma vera e propria è stata dunque preparata due mesi dopo; essa prevede un cambiamento ai vertici dell'agenzia di sicurezza nazionale, un maggiore coinvolgimento del potere giudiziario quanto a concessione di autorizzazioni e una minore discrezionalità ad agire di analisti e funzionari NSA. Inoltre i dati ottenuti dall'intelligence americana non dovrebbero più essere elaborati o archiviati, eccezion fatta per casi di autentico pericolo per la sicurezza nazionale. Persino dal potere giudiziario arrivano pesanti critiche alla gestione del programma Prism; esso è stato dichiarato "verosimilmente incostituzionale", in quanto contrario al IV emendamento della Costituzione Americana, dal giudice federale di Washington Richard Leon, il quale in aggiunta ha espresso il suo scetticismo verso un modo orwelliano di combattere e sventare attentati terroristici, anche perché non vi è alcuna prova accertata che questo programma abbia veramente aiutato l'intelligence americana ad evitare tali minacce. È tuttavia necessario, in questo caso, operare una precisazione, in quanto sulla presunta incostituzionalità l'ultima parola spetterebbe, alla Corte Suprema degli Stati Uniti d'America.

Diverse sono invece le posizioni che arrivano dalle principali potenze del continente asiatico: secondo Luca Mainoldi, giornalista della rivista italiana di geopolitica *Limes*, la Russia e la Cina potrebbero essere indubbiamente interessate ad una monumentale riforma

[10] Recommendation n4.

dello spazio digitale; il caso NSA, in modo del tutto involontario, ha indebolito fortemente le posizioni statunitensi in materia di governance di Internet, tema maggiormente dibattuto in seno alla conferenza mondiale delle telecomunicazioni internazionali di Dubai, alla fine del 2012. Mentre Washington vuole mantenere l'attuale sistema in cui soggetti americani pubblici e privati detengono una posizione preminente, Mosca e Pechino auspicano ad un controllo multigovernativo tramite istituzioni legate alle Nazioni Unite (come ad esempio l'Itu, International telecommunication union). Il caso Snowden potrebbe dunque rappresentare un oggetto di propaganda per fare proselitismo tra gli Stati maggiormente danneggiati dal cyberspionaggio americano e costringere gli statunitensi a rivedere le proprie posizioni sulla questione[11].

La Germania, che secondo le dichiarazioni del settimanale *Der Spiegel* ha rappresentato la base operativa delle attività di intelligence americana in Europa, ha cercato invece di agire su vari livelli. Sul piano interno, non essendo possibile aprire un'inchiesta sullo spionaggio di massa per insufficienza di prove, il procuratore federale ha comunque avviato le indagini sul caso Merkel. A livello internazionale, grazie all'ausilio del Brasile, altro paese fortemente colpito dal caso NSA, è stata presentata in data 2 Novembre 2013 una bozza di risoluzione non vincolante all'Assemblea Generale delle Nazioni Unite, poi approvata il 18 Dicembre dello stesso anno, dal titolo *The Right to Privacy in the Digital Age*[12]. Sulla risoluzione in questione vi sarà un focus più approfondito nel prossimo paragrafo. È inoltre fondamentale aggiungere che Berlino, con l'ausilio Francese, ha promosso una serie di provvedimenti al fine di istituire un sistema di *cloud computing* indipendente. Ciò al fine di ridefinire lo scambio informativo con gli Stati Uniti, che non gode di una vera reciprocità anche a causa dello stato quasi embrionale dell'intelligence comunitaria. Nonostante queste ultime iniziative europee si trovino ancora in uno stadio iniziale e non vi siano concrete spinte legislative in tale direzione, d'altra parte molto si sta facendo, in ambito comunitario, in materia di protezione dei dati personali.

[11] MAINOLDI, L., *Cina, Russia e Usa: il caso Snowden e la guerra di Internet*, in Limes, la rivista italiana di Geopolitica, http://temi.repubblica.it/limes/cina-russia-e-usa-il-caso-snowden-e-la-guerra-di-internet/49053 (consultato il 18/07/2014).

[12] Trattasi della risoluzione 68/167 approvata dall'Assemblea Generale il 18 Dicembre 2013. Per il documento integrale si rimanda al seguente link: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167 (consultata il 18/7/2014)

1.3.1 La posizione Europea: l'iniziativa della Commissione

È proprio l'Unione Europea a fare, negli ultimi tempi, importantissimi passi in avanti al fine di arginare in maniera concertata il pericolo di un nuovo *Datagate*. La Commissione, già sei mesi prima che esplodesse il caso, ha proposto un'imponente riforma del quadro giuridico europeo in materia di protezione di dati personali. Il capitolo V di detta proposta, ad esempio, disciplina in maniera più ferrea il trasferimento di dati ad un paese terzo. Esso deve, ai sensi dell'art.41 par.1, avere "adeguati livelli di protezione"; adeguatezza decisa dalla Commissione in base a una serie di criteri. Innanzitutto lo stato di diritto (par. 2a), oltre all'esistenza di un'autorità per la protezione dei dati personali (par. 2b). Enorme importanza ha anche l'articolo 17 della proposta in questione, che regolamenta il *diritto all'oblio*[13]: quest'ultimo altro non è che il diritto, da parte di un utente, di far sì che i propri dati non compaiano negli archivi di un internet provider, e dunque la possibilità di domandare la cancellazione, il trasferimento o la cessata elaborazione degli stessi laddove non siano più indispensabili agli scopi per cui questi dati erano stati raccolti.

1.3.2. La posizione Europea: la proposta del Parlamento.

Anche il Parlamento Europeo, in data 2 Luglio 2013, ha proposto una risoluzione comune sul programma Prism della *National Security Agency*[14]. Pur confermando il suo sostegno agli alleati transatlantici in materia di lotta al terrorismo e alla criminalità organizzata (proposizione operativa n1), l'Europarlamento condanna con fermezza le attività di spionaggio ad opera dell'NSA ritenendole, qualora fossero accertate, fortemente contrarie alla Convenzione di Vienna del 1961 sulle relazioni diplomatiche. Da Strasburgo arriva inoltre un invito alla Commissione e agli Stati membri di "*prendere in considerazione tutti gli strumenti a loro disposizione nel quadro delle discussioni e dei negoziati con gli Stati Uniti*"[15]. In particolare, riferendosi alla

[13] Nella versione inglese, *Right to be forgotten and to erasure*.

[14] Si veda, in particolare, Parlamento europeo, Proposta di risoluzione comune sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea. La il testo della risoluzione è disponibile su http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P7-RC-2013-0336+0+DOC+XML+V0//IT (Consultato il 20/07/2014)

[15] Si veda il punto 4 della risoluzione 2013/2682(RSP).

Commissione, suggerisce di rivedere proprio gli accordi anti-terrorismo, che forniscono agli Stati Uniti un enorme novero di informazioni. Un ulteriore suggerimento all'organo esecutivo UE viene specificatamente fornito in un punto a sé stante: la proposizione operativa 6 invita il governo statunitense e la Commissione a riprendere i negoziati concernenti il quadro di accordi sulla protezione dei dati personali in modo da garantire maggiori tutele e garanzie ai cittadini europei. Il Parlamento Europeo suggerisce inoltre l'istituzione, a livello comunitario, di "*commissioni parlamentari-giudiziarie miste di controllo e di inchieste esistenti in alcuni Stati membri per i servizi di intelligence*".[16] La risoluzione del Parlamento, come noto, non ha alcun valore vincolante; si presuppone tuttavia che la Commissione, tenuto conto del funzionamento dell'Unione e del rapporto fiduciario che esiste tra i due organi[17], tenga notevolmente in considerazione il parere dell'Assemblea dell'Unione. In ogni caso la risoluzione non può non avere un certo impatto a livello internazionale, rappresentando una forte e immediata risposta dell'Europa allo spionaggio spregiudicato e incontrollato dei suoi vertici.

1.3.3. La posizione Europea: la sentenza della Corte di Giustizia.

Sempre in materia di diritto all'oblio, la Corte di Giustizia ha recentemente emesso una storica sentenza proprio in tale ambito focalizzandosi, in particolare, sui motori di ricerca online. Essa si riferisce al caso di Mario Costeja González, un cittadino spagnolo che ha sporto denuncia nel 2012 contro un giornale nazionale e Google Spagna per la presenza di alcuni suoi dati relativi ad un avviso di vendita all'asta della propria casa, risalenti a qualche anno prima, che violavano il suo diritto alla privacy in quanto apparivano nei risultati di ricerca Google. Tramite l'ausilio dell'agenzia nazionale di protezione dei dati, la denuncia è stata presentata prima alla Corte Spagnola, che poi ha deferito la questione alla Corte di Giustizia. Il cittadino spagnolo ha chiesto l'eliminazione dei propri dati dal giornale (o perlomeno l'alterazione degli stessi), oltre che dai risultati del motore di ricerca Google. L'organo giudiziario

[16] Si veda il punto 15 della risoluzione 2013/2682 (RSP).
[17] A tal proposito si veda il riferimento alla *mozione di censura* disponibile su http://europa.eu/about-eu/institutions-bodies/european-parliament/index_it.htm (consultato il 19/07/2014)

dell'Unione Europea ha ribadito il *right to be forgotten*, da rivendicare nel caso in cui le informazioni riportate siano "*inaccurate, inadequate, irrelevant or excessive*"[18] ricordando d'altra parte che esso non è un diritto assoluto, ma deve essere bilanciato da altri diritti fondamentali quali libertà dei media e libertà di espressione. Bisogna dunque operare, in tale materia, una valutazione caso per caso. Nel commento alla sentenza, la Corte di Giustizia ha inoltre aggiunto:

> *"Il Tribunale rileva a questo proposito che il trattamento anche inizialmente legittimo dei dati precisi può, nel corso del tempo, diventare incompatibile con la direttiva*[19] *in cui, tenuto conto di tutte le circostanze del caso, i dati sembrano essere insufficienti, non pertinenti o non più rilevanti, o eccessivi rispetto alle finalità per le quali sono stati trattati e alla luce del tempo trascorso."*[20]

In conclusione, si può affermare che la sentenza della Corte di giustizia potrebbe offrire una spinta propulsiva all'iter legislativo comunitario in materia di protezione dei dati personali, dando da una parte maggiore legittimità alla riforma auspicata dalla Commissione, dall'altra una risposta legislativa concreta allo spionaggio indiscriminato e non regolamentato che ha portato agli scandali dell'ultimo anno.

1.4. Provvedimenti in seno alle Nazioni Unite

Dall'esplosione del caso *Datagate*, nel Giugno 2013, si è immediatamente avvertita la portata internazionale del caso. Per tale ragione, le Nazioni Unite appaiono come il centro naturale di discussione e risoluzione in merito alla questione dello spionaggio cibernetico di massa. A tal proposito, risulta di grande rilievo la già citata risoluzione dell'Assemblea Generale approvata nel Dicembre dello stesso anno, di cui si parlerà nel corso di questo paragrafo. Prima di introdurre detta risoluzione, è nondimeno importante notare che già nella primavera 2013, dunque prima dell'esordio delle rivelazioni sul caso, il Consiglio sui Diritti Umani si era espresso sulla questione attraverso un rapporto speciale redatto dal *Rapporteur* per la promozione e la protezione del diritto alla libertà di opinione ed

[18] Si veda, a tal proposito, la nota informativa della Commissione Europea sulla sentenza (C-131/12).
[19] È qui intesa la direttiva 95/46/EC del Parlamento Europeo e del Consiglio del 24 Ottobre 1995 sulla protezione degli individui riguardo all'elaborazione di dati personali e al libero movimento di tali dati.
[20] Il testo originale, in lingua inglese, del comunicato stampa No 70/14 è disponibile sul sito della Corte di Giustizia dell'Unione Europea http://curia.europa.eu/.

espressione, Frank la Rue. Esso già esamina le implicazioni della sorveglianza di Stato sull'esercizio dei diritti umani alla privacy e sulla libertà di opinione ed espressione. Il testo dà una panoramica generale dei diritti sopra menzionati, analizzandone anche i meccanismi di protezione, oltre a passare in rassegna i più moderni metodi di sorveglianza di massa. Già nell'introduzione, al punto secondo, si legge:

> *Le innovazioni tecnologiche hanno aumentato le possibilità di comunicazione e di protezione della libera espressione ed opinione, consentendo l'anonimato, il rapido scambio di informazioni e il dialogo interculturale. I cambiamenti tecnologici hanno contemporaneamente aumentato le opportunità per la sorveglianza dello Stato e gli interventi in comunicazione privata degli individui.*

Nel punto terzo, tuttavia, si precisa:

> *Le preoccupazioni per la sicurezza nazionale e le attività criminali possono giustificare l'eccezionale utilizzo di tecnologie di sorveglianza nelle comunicazioni. Tuttavia, le leggi nazionali che regolano ciò che costituirebbe il necessario, legittimo e proporzionale coinvolgimento dello Stato nella sorveglianza delle comunicazioni sono spesso insufficienti o inesistenti. Quadri giuridici nazionali inadeguati creano un terreno fertile per le violazioni arbitrarie e illegittime del diritto alla riservatezza delle comunicazioni e, di conseguenza, minacciano anche la protezione del diritto alla libertà di opinione e di espressione.*

Il rapporto dunque, oltre a spiegare brevemente gli svantaggi e i punti di forza in merito all'utilizzo delle nuove tecnologie nel settore della pubblica sicurezza, mette chiaramente in luce il problema di *vacatio legis* che sussiste non solo a livello internazionale, ma anche a livello dei singoli Paesi[21]. Esso risuona pertanto come un importante campanello d'allarme già prima del dilagare delle imbarazzanti notizie sul Prism e programmi affini[22].

A distanza di poco meno di un anno l'Assemblea Generale è stata costretta a riprendere in esame la questione tramite la risoluzione 68/167, enfatizzando l'impatto negativo che la

[21] Sulle differenze tra meccanismi differenti di tutela della privacy e della protezione dei dati personali si discuterà nel prossimo capitolo, con particolare attenzione alle differenze tra il sistema europeo e quello statunitense.

[22] In verità il rapporto A/HRC/23/40 analizzato in questo paragrafo non è un caso isolato. In altri rapporti infatti (A/HRC/17/27 e A66/290) lo *Special Rapporteur* aveva analizzato l'impatto di Internet nell'espansione delle libertà, notando d'altra parte la profonda inadeguatezza delle misure prese dagli Stati al fine di prevenire e ridimensionare il flusso di informazioni personali online.

sorveglianza di massa e le intercettazioni, incluse quelle extraterritoriali, possono avere sulla fruizione e l'esercizio dei diritti umani. Nel testo compare un principio importantissimo, più volte invocato dalle autorità per la protezione della privacy di tutto il mondo: gli stessi diritti che gli individui hanno *offline* devono anche essere mantenuti, protetti e rispettati *online.* La risoluzione riconosce dunque che il rispetto del diritto alla libertà di espressione e allo stesso tempo la tutela della privacy *online* sono la chiave di volta per infondere fiducia negli utenti di internet; essa dichiara inoltre che qualsiasi tentativo da parte di un individuo di affrontare problemi di sicurezza su Internet deve di conseguenza essere conforme agli obblighi internazionali sui diritti umani. La risoluzione invero afferma, in maniera piuttosto critica, che tutto ciò deve essere garantito attraverso istituzioni trasparenti, democratiche e basate sullo Stato di diritto. Gli Stati infine sono chiamati, ai sensi della quarta proposizione operativa, a rispettare i diritti umani nel contesto della comunicazione digitale e a prendere al contempo una serie di misure che garantiscano a ciascuna nazione, all'interno del proprio sistema legislativo, protezione e tutela contro le intercettazioni, la collezione e la rielaborazione indiscriminata di dati personali e più in generale contro sorveglianza di massa nelle comunicazioni. Come evidente anche dall'ultimo punto della risoluzione, essa non rappresenterà un caso isolato: in attesa di sviluppi successivi della questione, vi saranno altre discussioni in merito durante la 69ma sessione, prevista nel mese di Settembre 2014. A dare ulteriore rilevanza alla questione si aggiunge anche il rapporto dell'ufficio dell'Alto Commissario delle Nazioni Unite per i Diritti Umani riferito giustappunto alla risoluzione appena presa in esame. In tale rapporto si ribadisce il diritto alla protezione contro "l'interferenza illegale nei confronti della vita privata, della casa, della famiglia o della corrispondenza", specificando che per illegale ed arbitrario si intendono anche le interferenze che, pur consentite dalla legge nazionale, sono in contrasto con le disposizioni dell'art. 17 del Patto Internazionale sui diritti civili e politici[23]. Vi è inoltre un importante richiamo a quest'ultimo nella sezione E della parte III,

[23] Esso infatti recita, testualmente: "*Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua*

in cui si stabilisce che, come in quel caso le vittime di una violazione delle disposizioni stabilite dal Patto avrebbero diritto a una riparazione effettiva, così deve essere anche nel caso in cui vi siano inosservanze *online* in tali ambiti. Nella parte V, infine, ribadendo la presenza di significativi *gap* nell'implementazione del diritto alla privacy, si mettono in risalto due osservazioni: la prima riguarda la continua emersione di informazioni sulle pratiche e le politiche di sorveglianza nazionale oltre che extraterritoriale, la cui legalità e costituzionalità è, a più riprese, oggetto di verifica delle Corti a livello nazionale, la seconda evidenzia la preoccupante assenza di azioni governative trasparenti proprio su queste politiche, in quanto ciò ostacola ogni tentativo di dare una valutazione della loro coerenza con il diritto internazionale dei diritti umani e per attribuire eventuali responsabilità in caso di inadempienze.

Conclusioni

Oggetto di questo capitolo è stata una presentazione generale del caso preso in analisi e le relative e più rilevanti posizioni di alcuni attori internazionali a riguardo, con particolare riguardo alla vicenda UE. Dopo un'iniziale premessa elaborata nel tentativo di fornire una spiegazione programmatica in merito all'approccio utilizzato per affrontare il caso, si è passati ad elencare gli eventi più significativi del *Datagate*, con riferimenti più marcatamente diplomatici che relativi al Diritto vero e proprio. Si sono infatti menzionate le diverse crisi tra gli Stati Uniti e la Russia, oltre ad alcuni Paesi dell'America Latina, sino alle ripetute richieste di immediati chiarimenti da parte degli storici alleati Europei. La seconda parte del capitolo ha invece affrontato brevemente le reazioni di alcuni importanti Paesi, oltre a talune conseguenze (in alcuni casi persino "positive" dal punto di vista geopolitico) che il *Datagate* ha prodotto, per taluni Stati, a livello internazionale. Si è brevemente focalizzata l'attenzione sulle posizioni di Russia e Cina, oltre a quella tedesca, per poi approdare alle implicazioni legislative concrete in seno all'Unione Europea e alle

vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese".

Nazioni Unite. Per l'appunto all'ONU è stata dedicata la sezione finale del capitolo, con particolare attenzione ai provvedimenti intrapresi affinché la Comunità Internazionale desse una risposta più diretta e pertinente a questi eventi. Secondo tali disposizioni, infatti, risulta che la sorveglianza di metadati può minacciare la privacy così come la raccolta di contenuti veri e propri[24], che la stessa privacy è fortemente messa a rischio dalla condivisione incontrollata dei dati da parte delle agenzie di pubblica sicurezza, che questo fondamentale diritto è esteso anche ai non cittadini di un determinato Stato, e di conseguenza che lo spionaggio extraterritoriale e di per sé contrario al Diritto Internazionale. Secondo Thomas Hughes, direttore esecutivo di *Article 19*, organizzazione non governativa per la difesa del diritto d'informazione e di espressione, "Internet si presenta oggi come la *front line* nel contesto dello spazio civico", aggiungendo che la risoluzione approvata delle Nazioni Unite "sarà fondamentale nella battaglia per garantire la libertà di Internet, compresa le libertà di riunione, di associazione, di espressione, proprio là dove esse sono più a rischio"[25]. Pur essendo coscienti che le risoluzioni dell'Assemblea Generale non sono di per sé vincolanti per gli Stati, esse esercitano un potere non indifferente all'interno della Comunità Internazionale. I provvedimenti presi in esame non sono risolutivi: come è stato più volte fatto notare, gli eventi e le misure in risposta agli stessi sono ancora in corso d'opera. Non si può tuttavia negare che i recenti sviluppi rappresentano indubbiamente l'incipit di un percorso di regole condivise che la comunità internazionale attende da tempo.

[24] A confermarlo è il già analizzato rapporto A/HRC/27/37, oltre alle dichiarazioni dell'Alto Commissario per i Diritti Umani.
[25] Si veda, a tal proposito, *UNHRC rejects attempts to dilute Internet freedoms,* disponibile su http://www.article19.org/resources.php/resource/37602/en/unhrc-rejects-attempts-to-dilute-internet-freedoms, conslutato il 20/07/2014.

CAPITOLO 2

2.1. Premessa

Nel precedente capitolo si è realizzata una breve disamina dei provvedimenti che stanno muovendo i primi passi per dare una risposta normativa internazionale al caso *Datagate.* In questo capitolo, al contrario, si analizzerà nello specifico la conformità del programma Prism alla vigente normativa europea e statunitense in materia di protezione dei dati personali. Si opererà pertanto una comparazione tra Europa e Stati Uniti sulla materia d'indagine, attraverso una panoramica sui rispettivi sostrati normativi. Quest'ultima sarà realizzata al fine di individuare le discrepanze strutturali tra i due sistemi, con lo scopo ultimo di riscontrare, eventualmente, una compatibilità tra il piano di sorveglianza americano e i sistemi di regolamentazione europeo e statunitense in tale ambito. Si constaterà tuttavia che, in materia di protezione dei dati personali, esistono delle sostanziali differenze tra le due sponde dell'Atlantico: mentre per l'ordinamento europeo il diritto alla privacy e il diritto alla protezione dei dati personali sono elevati al rango di *diritti fondamentali*, a tutela dei quali vi è una struttura normativa ben precisa, non si può dire lo stesso del caso statunitense. I diritti sopraindicati possono infatti, nel contesto giuridico americano, essere agevolmente derogati in favore di una serie di misure antiterrorismo. In altre parole, mutuando una terminologia vicina alla filosofia del diritto, nel *trade-off* tra libertà e sicurezza in materia di privacy e protezione dei dati, gli europei sono normativamente più vicini alle libertà di quanto lo siano gli statunitensi. Partendo da queste differenze si arriverà, nella seconda parte, all'oggetto di indagine, ovvero alla compatibilità del programma Prism con la normativa europea e statunitense. Si vedrà di conseguenza che, data l'analisi della prima sezione, nel caso statunitense il piano di sorveglianza risulta legittimo, cosa che al contrario non può dirsi in un contesto europeo. Tali considerazioni riportano alla rassegna del precedente capitolo sugli eventi che hanno caratterizzato il caso *Datagate*: essi, infatti, hanno avuto in svariati casi proprio l'Europa come centro di sviluppo operativo. Ciò è dunque emblematico di una grande falla nel sistema normativo del vecchio continente: pur essendo corredato, al contrario del caso statunitense, da una regolamentazione fondata su principi ben precisi e tutelati da una solida struttura giuridica,

il sistema europeo non è riuscito a garantire in modo effettivo e concreto il rispetto di tali situazioni giuridiche, sovente eclissate dall'invasività delle misure antiterrorismo. Prima di affrontare nel merito il percorso analitico sin ora descritto, è importante effettuare una distinzione preliminare tra diritto alla privacy e diritto alla protezione dei dati personali: in dottrina, infatti, è stata superato l'approccio che incamera il diritto alla protezione dei dati personali all'interno del diritto alla privacy. In altre parole, il primo non è semplicemente un elemento che caratterizza il secondo, al contrario i due diritti hanno distinte posizioni giuridiche, differendo per finalità e per contenuto.[26] Per quanto concerne le finalità, il diritto alla privacy, intende scongiurare possibili interferenze illegittime del potere esecutivo nella vita privata degli individui; d'altro canto, il diritto alla protezione dei dati ha lo scopo di presidiare i dati personali di un individuo contro un qualsiasi trattamento irrispettoso dei principi di proporzionalità, necessità e limitazione dei dati. Per quanto riguarda il contenuto, invece, il diritto alla protezione dei dati, consistendo esso nella attribuzione di un novero di diritti concernenti il trattamento dei dati personali, presenta una più ampia portata rispetto al diritto alla privacy, che di contro possiede una più ampia forza espansiva, riguardando la regolamentazione e la protezione di un maggior numero di situazioni giuridiche soggettive.[27] In aggiunta, è importante tener presente che anche in ambito di diritto alla privacy vi sono diverse accezioni e molteplici approcci interpretativi: Rodotà definisce la costruzione di tale diritto come quella di un "*dispositivo 'escludente', come strumento per allontanare lo sguardo indesiderato".*[28] Egli si rifà dunque alla definizione originaria della privacy come *diritto ad essere lasciato solo*[29]. La dottrina ha tuttavia sviluppato una serie di accezioni differenti, che pur non cancellando l'enunciato originale vi si accompagnano e ne modificano il significato. Per Alan Westin, professore emerito di *Public Law & Government* presso la *Columbia University* e vincitore del *Privacy Leadership Award of the International Association of Privacy Professionals,* la privacy si definisce come *"l'uso che altri fanno delle informazioni che mi riguardano*[30]*"*.Questo diritto può inoltre essere inteso

[26] RODOTÀ, S., "Prefazione", in *Libera circolazione e protezione dei dati personali*, t. I, R. PANETTA (a cura di), Milano, 2006, p. VII ss.

[27] Si veda, a tal proposito: BONFANTI, M., "Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti", disponibile sulla Rivista *Diritti Umani e Diritto Internazionale*, 2011, p. 437 ss., pp. 440-442.

[28] Cfr. RODOTÀ, S., *Il diritto di avere diritti,* editori Laterza, Bari, 2012, p.320.

[29] WARREN, S. e BRANDEIS, L.D., *The Right to Privacy,* in "Harvard Law Review", 5, 1890, pp.4 e ss.

[30] WESTIN, A., Privacy and Freedom, Atheneum, New York 1970.

come "*tutela delle scelte di vita contro ogni forma di controllo pubblico e di stigmatizzazione sociale*"[31] o addirittura come "*diritto di scegliere liberamente il proprio modo di vivere*"[32]. Tenendo presenti queste distinzioni e le diverse accezioni del diritto alla privacy, si procederà nel percorso analitico considerando il diritto alla privacy secondo la sua accezione originaria, mentre si parlerà allo stesso modo di tale diritto e del diritto alla protezione dei dati personali, che verranno trattati come oggetto di esposizione unitario, viste le evidenti similitudini tra i due e le soventi situazioni in cui essi si sovrappongono, dovute proprio a tali forti analogie.

2.2. La normativa statunitense

Le tutele previste dalla regolamentazione statunitense sulla materia in questione sono ben più circoscritte rispetto al corrispettivo europeo. Secondo il Quarto Emendamento della Costituzione americana:

> *"Non potrà essere violato il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, di fronte a perquisizioni e sequestri ingiustificati; e non si rilasceranno mandati di perquisizione se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare".*

Esso ha dunque lo scopo di evitare un'eccessiva o arbitraria ingerenza del potere esecutivo nella vita privata dei cittadini statunitensi, e l'interpretazione dello stesso ha subìto una notevole evoluzione, essendo stata adattata nel tempo alle contingenze storiche e agli sviluppi tecnologici che tali contingenze hanno comportato: se infatti negli anni '20 del secolo scorso il Quarto Emendamento intendeva tutelare i cittadini dalle sole intrusioni fisiche[33], si è passati, quarant'anni dopo, ad estendere tale tutela anche alle intercettazioni

[31] FRIEDMAN, L., *The Republic of Choice. Law, Authority and Culture,* Harvard University Press, Cambridge (Mass.)-London 1990, p.184

[32] RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité,* Bruylant, Bruxelles-Paris 1990, p.167.

[33] Corte Suprema degli Stati Uniti d'America, Olmstead v. United States, 277 U.S. 438 (1928), sentenza del 4 giugno 1928, p. 466.

telefoniche e alla sorveglianza elettronica in genere[34]. La seconda parte dell'emendamento afferma un principio importante: non si può interferire nella vita privata dei cittadini senza che vi sia un mandato fornito da un'autorità giurisdizionale, la quale è tenuta a concedere tale mandato esclusivamente allorché vi sia un motivo plausibile, una *probable cause*, per pensare che tale ingerenza sia utile a raccogliere informazioni relative alla commissione di un illecito. Nell'ordinamento statunitense bisogna attualmente annoverare tre importanti provvedimenti legislativi particolarmente incisivi sul diritto alla privacy e alla protezione dei dati personali, tutti aventi come scopo fondamentale il mantenimento della sicurezza nazionale e internazionale: l'*Omnibus Crime Control and Safe Streets Act del 1968 (cd. Wiretap Statute)*[35], il *Foreign Intelligence Surveillance Act (FISA) del 1978*[36], e lo *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (acr. USA Patriot Act) del 2001*[37]. Il Wiretap statute si applica nei casi in cui vi sono intercettazioni o indagini che possono riguardare limitazioni del diritto alla privacy e alla protezione dei dati negli Stati Uniti. Per porre in essere tali limitazioni, in questi casi, le agenzie governative abbisognano di un mandato emesso da un giudice ordinario nel rispetto della *probable cause* del Quarto Emendamento. Il FISA, d'altra parte, riguarda le operazioni di *intelligence* all'estero; in questo caso, l'ingerenza nella privacy dei cittadini non statunitensi segue diversi e meno stringenti parametri, dal momento che, al contrario del *wiretap statute*, le autorizzazioni a procedere non vengono concesse da un giudice ordinario bensì da un tribunale speciale creato appositamente per tali operazioni. Tale tribunale ad hoc (chiamato appunto Corte FISA) è composta da 11 *federal district court judges* i quali sono nominati dal capo del Dipartimento di Giustizia americano, e le sue decisioni sono sottoposte a revisione da un'altra Corte appositamente istituita, composta da tre giudici e denominata *FISA Court of Review*.[38] Dal momento che la corte FISA non è

[34] Corte Suprema degli Stati Uniti d'America, Katz v. United States, 389 U.S. 347 (1967), sentenza del 17 ottobre 1967, pp. 351-352; vedi anche: Corte Suprema degli Stati Uniti d'America, Berger v. New York, 388 U.S. 41 (1967), sentenza del 13 aprile 1967.
[35] Omnibus Crime Control and Safe Streets Act of 1968, Public Law No. 90-351, 82 Stat. 197.
[36] Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. 1801-1811, 1821-1829, 1841-1846, 1861-62)
[37] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Public Law No. 107- 56, 115 Stat. 272
[38] Fonte: *About the Foreign Intelligence Surveillance Court*, disponibile sul sito della Corte FISA http://www.fisc.uscourts.gov/. Per maggiori informazioni sull'operato di tale corte, si rimanda al seguente link: http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Leahy-1.pdf.

tenuta a rispettare i principi del Quarto Emendamento e della *probable cause*,[39] non è difficile immaginare che i limiti giudiziari nelle operazioni di *foreign intelligence* siano meno stringenti.

A seguito dell'attentato terroristico alle Torri Gemelle nel 2001, inoltre, gli Stati Uniti hanno varato un'altra importante legge federale, denominata USA Patriot Act. La norma concede una più ampia discrezionalità operativa alle agenzie di pubblica sicurezza (FBI, NSA, CIA) al fine di prevedere e neutralizzare futuri attacchi terroristici. Ciò ha modificato profondamente il FISA, rendendo ancora più blandi i presidi giudiziari istituiti dalla legge del 1978. Basti pensare che nel 2002 ci sono stati oltre 1000 mandati della Corte *ad hoc* per le operazioni di foreign intelligence, che hanno determinato una significativa proliferazione delle indagini rispetto agli anni precedenti. Nondimeno, svariate attività considerate precedentemente al di fuori dell'ambito di applicazione della legge statunitense sono state incluse nel Patriot Act[40], tanto che molti tra i più illustri legislatori non hanno compreso fino in fondo il novero di leggi che governa la sorveglianza elettronica[41]. A tal proposito, l'attuale presidente pro tempore del Senato Americano, Patrick Leahy, ha così commentato lo USA Patriot Act:

> "*[Esso] entra in un nuovo e inesplorato territorio, abbattendo le barriere tradizionali tra le forze dell'ordine e di foreign intelligence.*" [42]

È infine importante sottolineare che la legislazione federale in materia di tutela della privacy e protezione dei dati personali non è omogenea e propriamente armonizzata: essa si presenta come una regolamentazione frammentaria e composta da una serie di norme particolarmente specifiche.

---

[39] Il tribunale deve tener conto, in questo caso, del parametro di *sospetto fondato*, ovvero quando sulla base della documentazione fornita, venga appurato che si tratti di un *agente* o di un *potere straniero,* e l'operazione di intelligence abbia un *fine legittimo.* Sul punto, si veda: NINO, M., *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 Diritti Umani e Diritto Internazionale, 3, 2013, pp.727,746.

[40] Si veda, a tal proposito: YOUNG, M.G. (2001). What big eyes and ears you have! A new regime for covert governmental surveillance. Fordham Law Review, 70(6), 1017-1109.

[41] Sul punto, di veda: JAEGER, P.T., BERTOT,J.C.,MCCLURE, C.R., *The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act*, in Government Information Quarterly, 20, 3, 2013, pp.295-314.

[42] Citato in MCGEE, J. (2001, Nov. 4). *An intelligence giant in the making; antiterrorism law likely to bring domestic apparatus of unprecedented scope*. Washington Post, November 4, 2001, at A4.

2.2.1. Il caso Datagate e la normativa statunitense.

Alla luce di quanto appena descritto, la legittimità del programma di intercettazioni Prism si può riscontrare proprio nell'appena menzionato USA Patriot Act, e in particolare, nella Section 215 di tale legge federale, che ha modificato il titolo V del FISA. In questo modo le agenzie di intelligence, al fine di combattere più efficacemente il terrorismo internazionale, sono state dotate di poteri più ampi e la Corte FISA ha ottenuto la possibilità di emettere mandati secondo parametri meno stringenti.[43] Nondimeno, gli individui vittime di intercettazioni o altre ingerenze governative non hanno diritto di adire tale Corte, e non hanno modo di sapere se le registrazioni o i dati personali sul loro conto siano oggetto di specifico controllo da parte del Governo. Teoricamente i cittadini potrebbero presentare richieste alle autorità governative, ai sensi del *Freedom of information Act* o del *Privacy Act*, al fine di conoscere un'eventuale operazione di spionaggio ai loro danni; ciononostante, le autorità governative hanno facoltà di non dare responso a tali richieste.[44] In aggiunta, vi è l'obbligo di riservatezza per chiunque sia a conoscenza di una richiesta di un'autorizzazione a procedere della Corte FISA, così come della pronuncia della stessa in merito, al fine di salvaguardare la sicurezza nazionale. [45] Infine, ai sensi della Section 701 FISA Aemendments Act del 2008, le agenzie di pubblica sicurezza possono svolgere attività di intelligence nei confronti di cittadini non americani, previa autorizzazione scritta della Corte FISA. Tale autorizzazione, come nel caso della Section 215, è di natura strettamente riservata.[46]

Sulla base della normativa sinora esplicata, il programma Prism è stato più volte autorizzato dalla corte FISA, che dal 2006 ad oggi ha consentito la raccolta di miliardi di metadati attraverso una massiva e indiscriminata operazione di *data mining.*

[43] Sul punto, si veda: O'DONNELL, M.J., "Reading for Terrorism: Section 215 of the USA Patriot Act and the Constitutional Right to Information Privacy", in Journal of Legislation 2002, p. 45 ss.
[44] Sul punto, si veda: BRENNAN CENTER FOR JUSTICE, *Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs*
[45] Sul punto, di veda: WHITEHEAD,J.W., ADEN, H., "Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives", in American University Law Review 2002, p. 1081 ss., p. 1107.
[46] BRENNAN CENTER FOR JUSTICE, op. cit., pp. 2-3.

2.3. La normativa Europea

In Europa la tutela del diritto alla privacy e alla protezione dei dati personali è affidata al Consiglio d'Europa e all'Unione Europea, che utilizzano strumenti normativi basati su una serie di principi comuni. L'articolo 8 della CEDU, ad esempio, disciplina un'ampia serie di interessi riconducibili alla materia in questione. Esso stabilisce deroghe al diritto alla privacy, ammesso che queste siano previste dalla legge, solo quando si è costretti ad operare ingerenze in nome di un fine legittimo (es. *pubblica sicurezza),* e tale misura sia necessaria e proporzionata.[47] La legittimità del fine, inoltre, è data dal rispetto dei principi di accessibilità e prevedibilità legislativa[48]; in altre parole un'ingerenza è legittima laddove sia accessibile ai diretti interessati (accessibilità), oltre ad essere formulata in maniera tale da permettere ad essi di conformare la propria condotta alla misura restrittiva del diritto di privacy (prevedibilità). Sicuramente più specifiche, soprattutto in materia di trattamento di dati personali, sono la convenzione n. 108 e la direttiva n. 95/46/CE[49], le quali stabiliscono una serie di ulteriori parametri proprio sulla disciplina della tutela delle informazioni di carattere personale. Tra questi, nella direttiva 95/46, i più significativi sono senza dubbio il rispetto del principio della qualità dei dati (il quale comprende una serie di sottoprincipi tra cui *liceità*, *proporzionalità*, *finalità limitata e sicurezza dei dati*) e la tutela rafforzata dei dati sensibili[50]. Per ciò che concerne il trasferimento dei dati a Paesi terzi, disciplinato dall'articolo 25 della direttiva in esame, esso deve essere effettuato solo qualora tali Paesi garantiscano un adeguato livello di protezione. L'adeguatezza, in questo caso è valutata in base a:

> *"la natura dei dati, la finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate" (art.25 par.2)*

[47] Sul punto si veda SOTTIAUX, S., Terrorism and Limitation of Rights: The ECHR and US Constitution, Oxford, 2008, pp. 270-271.

[48] Si veda, a tal proposito: DE SENA, P., "Esigenze di sicurezza nazionale e tutela dei diritti dell'uomo nella recente prassi europea", in Ordine internazionale e valori etici - VIII Convegno della Società italiana di Diritto internazionale, Verona, 26-27 giugno 2003, N. BOSCHIERO (a cura di), Napoli, 2004, p. 195 ss., pp. 203-211.

[49] Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, 28 gennaio 1981; Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GU L 281 del 23 novembre 1995.

[50] Cfr. NINO, M.*, op.cit.*

Gli individui direttamente interessati dal trattamento dei dati godono infine di una serie di diritti, tra cui il diritto di accesso ai dati (art.12, sez. V) e il diritto di opposizione (art.14, sez. VII). Altri importanti diritti di cui essi godono, secondo la normativa europea, sono il diritto all'informazione, il diritto di cancellazione, il diritto di rettifica dei dati e il diritto di ricorso contro trattamenti illegittimi. Il riconoscimento di situazioni giuridiche soggettive agli individui direttamente interessati dalle ingerenze sinora elencate è di fondamentale importanza in ambito europeo, in quanto dovrebbe essere emblematico di un'effettiva garanzia del rispetto e dell'osservanza delle norme in materia di protezione delle informazioni personali. A riprova di ciò, la Corte europea dei diritti dell'uomo ha riconosciuto, in svariati casi[51], importanti posizioni giuridiche di natura attiva proprio ai soggetti interessati dal trattamento dei dati, attribuendo un valore significativo ai princìpi sopra menzionati. Proprio questi ultimi rappresentano un fondamentale presidio normativo europeo che, più di altri, possono essere presi in esame nella disamina giuridica del caso *Datagate.* Di indiscusso rilievo, nell'analisi dello scandalo NSA, risulta un'altra garanzia normativa su cui è necessario focalizzarsi, ovvero il principio della finalità limitata. Secondo tale principio, infatti, i dati possono essere rilevati solo se vi è una finalità precisa che porta a questa operazione; essi devono, di conseguenza, essere trattati in maniera esclusivamente compatibile con tale finalità. Il principio in questione tenta così di arginare un eventuale utilizzo arbitrario e sconsiderato delle informazioni personali, collegandosi inscindibilmente al principio di proporzionalità, secondo cui il trattamento dei dati deve essere *adeguato, pertinente e non eccedente* rispetto alle fini per i quali tali dati vengono rilevati o utilizzati[52]. L'importanza di quanto appena esposto è massima se si vuole operare un raffronto con il sistema giuridico statunitense, dal momento che questo principio rappresenta un notevole scarto tra le diverse normative delle due sponde dell'Atlantico. Un'ulteriore conferma della rilevanza di tale principio emerge da una serie di sentenze[53] della Corte europea dei diritti umani, che riprendono la convenzione n.108 e la direttiva 95/46, sottolineando l'importanza della proporzionalità e della finalità limitata nel

[51] Corte europea dei diritti umani: Leander c. Svezia, cit., par. 66 (che attribuisce ai soggetti interessati dal trattamento dei dati il diritto di accesso e comunicazione dei dati); Rotaru c. Romania, cit., par. 83 (che riconosce agli individui il diritto di risarcimento per irregolari conservazioni di informazioni di carattere personale); Segerstedt-Wiberg e altri c. Svezia, cit., par. 120-122 (che attri- buisce ai soggetti sottoposti al trattamento dei dati il diritto di rettifica e cancellazione dei dati stessi).

[52] Cfr. NINO, M., *op.cit.*

[53] Corte europea dei diritti umani: Amann c. Svizzera, par. 75-76; Rotaru c. Romania, par. 47; Segerstedt-Wiberg e altri c. Svezia, ricorso n. 62332/00, sentenza del 6 giugno 2006, par. 79, 88; S. and Marper c. Regno Unito, par. 50, 103.

trattamento dei dati. Il Trattato di Lisbona ha infine fornito alla materia ulteriore linfa normativa, in quanto nell'art. 16 TFUE[54], al paragrafo 2, si pongono le basi per una regolamentazione comune, attraverso l'attribuzione di una serie di competenze agli organi europei in tale ambito. Il Trattato ha inoltre il merito di "cementare" le norme già in vigore, poiché attribuisce natura giuridica vincolante alla Carta dei diritti fondamentali. Gli articoli 7 e 8 di tale carta, infatti, tutelano proprio il diritto rispettivamente alla privacy e alla protezione dei dati personali, elevati di conseguenza al rango di diritti fondamentali[55].

Si può dedurre, dalla disamina presentata in questo paragrafo, che in Europa la materia è stata trattata con particolare dovizia normativa, attraverso una progressiva regolamentazione che ha posto i due diritti in questione in posizione sempre più elevata nella gerarchia delle fonti. A questo punto è importante analizzare la questione alla luce degli avvicendamenti del caso *Datagate*. Ricordando gli eventi più singolari dell'*affaire* NSA, l'Europa è stata più volte al centro delle polemiche, presentandosi spesso come "parte lesa", sebbene, stando alle rivelazioni di Edward Snowden, vi sia una partecipazione attiva del vecchio continente nelle vicende di cyberspionaggio internazionale. Ci si trova dunque in una situazione piuttosto singolare, in quanto si può ben dedurre che i diritti fondamentali alla privacy e alla protezione dei dati personali non hanno resistito all'invasività delle leggi antiterrorismo. L'Europa delle leggi non è riuscita a stare al passo con la smisurata richiesta di informazioni data dai recenti sviluppi tecnologici, dalla globalizzazione finanziaria e dalla necessità di contrastare la minaccia terroristica anche a costo delle libertà personali. La normativa europea in tale materia si è in conclusione dimostrata inefficace, inadeguata e priva di effettività.

2.3.1. Il caso Datagate e la normativa europea.

In base a quanto analizzato sinora, il programma Prism si dimostra senza dubbio incompatibile con la normativa europea disaminata in questo paragrafo per vari motivi: in primo luogo, una qualsiasi operazione di spionaggio che implichi un sistema di intelligence basato su una legislazione *ad hoc*, sulla massima segretezza e

[54] Trattato sul Funzionamento dell'Unione Europea
[55] Si veda HIJMANS, H., "Recent Developments in Data Protection at European Union Level", in ERA-Forum 2010, pp. 219 ss., p. 220.

sull'impossibilità, da parte dei soggetti direttamente colpiti dalle ingerenze governative, di avere informazioni in merito al trattamento dei propri dati, non rispetta i parametri di accessibilità e di prevedibilità legislativa. In secondo luogo, un indiscriminato sistema di *mass surveillance* non si può ritenere, per definizione, conforme ai principi di proporzionalità e finalità limitata. A ciò si aggiunga che la già analizzata Section 701 del US Patriot Act, che autorizza il programma Prism a procedere nei confronti di cittadini non statunitensi senza alcun significativo ostacolo, non può dirsi compatibile con le regole europee e il sistema di diritti posto a presidio di queste ultime. Tale sezione della summenzionata legge federale, infatti, ha molteplici punti di frizione con la convenzione n.108 e la direttiva 95/46, che riconoscono ai cittadini europei fondamentali situazioni giuridiche soggettive tra cui il già citato diritto all'informazione e i diritti di cancellazione, rettifica dei dati, di opposizione e di ricorso contro trattamenti illegittimi. In sintesi, nelle operazioni del programma Prism, secondo le descrizioni più volte fornite in seno al caso *Datagate*, non esiste quella legittimità richiesta dall'articolo 8 CEDU nel caso in cui si operino deroghe al diritto alla privacy.

A questo punto è lecito domandarsi a quale titolo i provider americani dovrebbero conformarsi agli standard europei, pur operando negli Stati Uniti d'America, e perché gli Stati Uniti sono riusciti ad avere accesso ad un così vasto numero di informazioni personali di cittadini europei, vista la vigente normativa. Per rispondere a questo quesito è necessario introdurre un meccanismo istituito dalle autorità europee e statunitensi al fine di agevolare i rapporti commerciali tra le due sponde dell'Atlantico, ovvero il sistema *Safe Harbor.*

2.3.2. *Il Safe Harbor, "ponte normativo" tra Europa e Stati Uniti*

La direttiva 95/46/CE, all'articolo 25, impone dei vincoli rigorosi per quanto concerne il trasferimento di dati personali europei al di fuori del territorio del vecchio continente. Per questa ragione, nel tentativo di far sì che le aziende americane si conformassero agli standard imposti dagli organi comunitari, il Dipartimento del Commercio degli Stati Uniti, in consultazione con la Commissione Europea, ha varato il *Safe Harbor*. Questo sistema si basa su un'adesione volontaria, da parte delle organizzazioni statunitensi che operano in Europa, a una serie di principi,

ovvero: *notifica* (gli individui devono essere informati del fatto che i propri dati sono rilevati), *scelta* (gli individui possono scegliere se il trasferimento di dati a un paese terzo può aver luogo), *sicurezza* (i dati devono essere protetti in modo ragionevole), *onward transfer* (il trasferimento a terzi può avvenire solo verso organizzazioni che rispettano adeguati standard di protezione), *integrità dei dati* (i dati devono essere trattati in modo pertinente agli scopi per cui sono stati raccolti), *accesso* (gli individui interessati devono poter accedere alle proprie informazioni), *garanzie di applicazione* (i principi sopra menzionati devono essere applicati in maniera efficace).[56] Le organizzazioni operanti in Europa devono notificare l'adesione al *Safe Harbor* al Dipartimento del Commercio statunitense, che redige una lista annuale delle compagnie aderenti. Una volta inviata la notifica, tali organizzazioni hanno l'obbligo giuridico di rispettare i principi sopra menzionati, i quali altro non sono che i principali standard europei di protezione dei dati e tutela della privacy. Considerato che vi sia effettivamente stata un'adesione al meccanismo *Safe Harbor* da parte di tutte le compagnie di telecomunicazioni coinvolte nello scandalo *Datagate*, si può individuare una concreta incompatibilità tra gli standard europei e il programma Prism. Gli Stati Uniti, a tal proposito, motivano l'ammissibilità di tale programma tramite due principali argomenti: il primo è che il programma è stato autorizzato da un tribunale indipendente (la corte FISA); il secondo, che le informazioni raccolte dall'intelligence statunitense non sono dati, bensì metadati (ovverosia dati che rimandano ad altri dati). A tali argomentazioni, tuttavia, si potrebbero muovere altrettante obiezioni, in quanto la Corte FISA è un tribunale speciale, il quale opera attraverso una procedura essenzialmente segreta,[57] che ha degli standard decisamente flessibili per quanto concerne le autorizzazioni a procedere in tale materia; inoltre la sua indipendenza è stata sovente contestata dalla dottrina americana. Per quanto concerne i metadati, infine, pur essendo vero che essi non si sostanzino di dati veri e propri, è risaputo che la rilevazione massiccia e costante di informazioni di traffico

[56] Si veda, a tal proposito: 2000/520/CE: Decisione della Commissione, del 26 luglio 2000 ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio. Il testo integrale è disponibile al seguente link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

[57] Si veda, a tal proposito : MAYER, J.D., "9-11 and the Secret FISA Court: From Watchdog to Lapdog?", in Case Western Reserve Journal of International Law 2002, p. 249 ss.; J.T. SOMA, M.M. NICHOLS, S.D. RYNERSON, L.A. MAISH, J.D. ROGERS, "Balance of Privacy vs. Security: A Historical Perspective of the USA Patriot Act", in Rutgers Computer and Technology Law Journal 2005, p. 285 ss.

riconduce senza eccessive complicazioni al contenuto delle conversazioni, soprattutto nell'ambito di internet.[58]

Concludendo, l'analisi sino ad ora effettuata ha mostrato le svariate contraddizioni tra i vari sistemi di regolamentazione, le quali hanno acquisito particolare risalto proprio a causa delle vicende del *Datagate.* Se si potesse, in definitiva, addurre un merito al sistema di intercettazioni venuto alla luce in questi ultimi mesi, sarebbe sicuramente quello di aver permesso alle molteplici forme di attrito tra la normativa europea e statunitense in tale ambito di acquistare rilevanza mediatica agli occhi di giuristi, capi di governo e dell'opinione pubblica internazionale.

2.4. Conclusioni

Il seguente capitolo ha avuto come oggetto di studio la normativa europea e quella statunitense sulla protezione dei dati e la tutela della privacy. Si è cercato di dare una panoramica generale dei due sistemi, operando, per quanto possibile, un raffronto tra questi ultimi e individuando due diversi approcci alla materia trattata. Dalla analisi presentata sono emerse differenze sostanziali tra la regolamentazione europea e quella statunitense, messe particolarmente in luce proprio dal caso *Datagate*. Come risultato dallo studio sinora condotto, infatti, non si può dire che il programma Prism sia legittimo in entrambi i sistemi giuridici, dal momento che il diritto comunitario prevede una serie di standard rigorosi, che non ammettono piani di intelligence di una tale portata e invasività. Ciononostante è risaputo che nel caso *Datagate* l'Europa sia stata più volte protagonista delle rivelazioni di Edward Snowden, in quanto una parte consistente del programma di spionaggio aveva proprio sede nel vecchio continente. Ci si è chiesti come ciò fosse possibile, trovando la risposta nel *Safe Harbor*, che ha permesso a diverse organizzazioni statunitensi di penetrare nel continente europeo. Le suddette organizzazioni, a loro volta, hanno fornito un enorme quantitativo di informazioni al governo americano, infrangendo i principi comunitari e il sistema di regole europee in tale ambito, oltre che lo stesso *Safe Harbor*. Il sistema di trasferimento delle informazioni concordato tra Europa e Stati Uniti si è perciò mostrato profondamente insufficiente, non riuscendo a frenare l'invasività del Prism. A tal proposito, il Parlamento Europeo sta valutando una possibile sospensione dei flussi di informazioni

[58] Si veda, a tal proposito: KOSTA, E., VALCKE, P., "The EU Data Retention Directive. Retaining the Data Retention Directive", in Computer Law & Security Report 2006, p. 370 ss., p. 375

verso gli Stati Uniti, ai sensi della Decisione del 26 Luglio 2000 sull'istituzione di *Safe Harbor*.[59] Come evidenziato anche nel primo capitolo in merito alle crisi diplomatiche tra Germania e Stati Uniti, sono stati messi in discussione, dopo una serie di sconcertanti rivelazioni sullo spionaggio ai danni di leader europei, persino gli accordi commerciali di libero scambio (TTIP),[60] che rischierebbero di non essere stipulati. In realtà esistono anche altre ragioni per cui le trattative per la stipula del trattato siano in una fase di stallo[61], tuttavia una delle principali è senza dubbio l'intenzione di regolare la questione del trasferimento dei dati personali proprio nell'ambito di questo accordo. La regolamentazione di una questione affrontata con particolare cura dal sistema giuridico europeo, che, si ricordi, annovera le norme in materia tra i diritti fondamentali, risulterebbe decisamente sminuita, se fatta rientrare nell'ambito di un accordo commerciale.

L'analisi sinora condotta, alla luce del caso *Datagate*, ha dimostrato che è essenziale rivedere i punti di contatto tra Europa e Stati Uniti nell'ambito della protezione dei dati personali, al fine di evitare che si verifichi nuovamente uno scandalo di tale portata. Bisognerebbe partire, innanzitutto, dal mutuo riconoscimento di una serie di differenze sostanziali tra i due sistemi. Tra i vari punti di frizione vi è, ad esempio, la differente portata della nozione di *law enforcement purpose*, che se nel caso europeo è riferito alla "*prevenzione, accertamento, indagine e perseguimento di qualsiasi reato*", nel caso statunitense si riferisce alla "*prevenzione, individuazione, soppressione, indagine o perseguimento di qualsiasi reato o violazione di legge relative a controlli alle frontiere, di pubblica sicurezza, e la sicurezza nazionale, così come per i procedimenti giudiziari o amministrativi non penali in relazione direttamente a tali reati o violazioni*"[62]. In secondo luogo, gli Stati Uniti attribuiscono una minore importanza ai principi europei esposti nel secondo paragrafo di questo capitolo. A ciò si aggiunga che mentre nel caso europeo detti principi sono estesi a tutti gli individui, al contrario solo negli ultimi tempi il sistema giuridico americano sta muovendo i primi passi verso una maggiore tutela dei cittadini non

[59] Si veda, in particolare, l'art 3, par. 1, Decisione 2000/520/CE, disponibile online su http://www.interlex.it/testi/00_520ce.htm.

[60] Sul contenuto e gli obiettivi dell'accordo si veda, in particolare: http://ec.europa.eu/trade/policy/in-focus/ttip/. (consultato il 24/07/2014).

[61] Un esempio è la pressione dell'opinione pubblica sul governo al fine di eliminare la clausola ISDS del partenariato. Per maggiori informazioni, si veda il seguente link: http://www.out-law.com/en/articles/2014/march/germany-plans-to-block-isds-clause-in-transatlantic-trade-deal/ (consultato il 24/07/2014).

[62] Final Report by EU-US High Level Contact Group on information sharing and privacy and per- sonal data protection, Doc. n. 15851/09 del 23 novembre 2009, disponibile su register.consilium.eu ropa.eu/pdf/en/09/st15/st15851.en09.pdf, pp. 3-4.

statunitensi, sino ad ora pressoché privi di diritti in materia di tutela della privacy. Per ciò che concerne quest'ultimo punto, è necessario che i cittadini europei, laddove i propri dati venissero raccolti ed elaborati da autorità transatlantiche, acquistino a pieno titolo le medesime garanzie dei cittadini statunitensi, e dunque il diritto di informazione e di ricorso presso i tribunali americani.[63]

Considerando tuttavia l'inefficacia delle pur rigide e strutturate norme europee in materia, anche il vecchio continente avrebbe bisogno di riformare la propria normativa, cercando di rafforzare le disposizioni del trattato di Lisbona sulla vincolatività dei principi di diritto alla privacy e tutela dei dati personali, al fine di avere un riscontro effettivo sul rispetto di tali disposizioni.[64] In particolare, si potrebbe procedere ad un rafforzamento delle autorità garanti per la protezione dei dati, [65]e promuovere controlli più severi per ciò che concerne il trasferimento di informazioni verso Stati terzi.[66]

In definitiva, l'Europa dovrebbe utilizzare una serie di espedienti normativi affinché i fondamentali diritti alla privacy e alla protezione dei dati personali siano concretamente presidiati. D'altra parte, in un sistema globalizzato che ha il suo principale archivio di informazioni su Internet, una rete a cui difficilmente può applicarsi il medesimo sistema di "barriere" che esiste tra gli Stati, sarebbe auspicabile che le riforme si sviluppassero anche nel sistema statunitense. Gli Stati Uniti dovrebbero rendere più omogenea la normativa che regolamenta i diritti sopra indicati, e sviluppare un diverso approccio in merito ai princìpi che fanno da sostrato normativo comune ai diritti alla privacy e alla protezione dei dati personali. Solo attraverso una partnership in tal senso si potrebbe promuovere una concreta e tangibile tutela degli interessi degli individui, dentro e fuori dalla rete, sviluppando di conseguenza una serie di garanzie normative che abbiano la capacità effettiva di evitare la minaccia di un nuovo *Datagate*.

---

[63] Parlamento europeo, *Proposta di risoluzione comune sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea*, del 2 luglio 2013, par. 6, lett a), b), c).

[64] Si veda, a tal proposito: P. HUSTINX, "Towards More Comprehensive Data Protection in Europe Including Bi-ometrics − A European Perspective".

[65] HUSTINX, P., "A Clear Signal for Stronger EU Data Protection", disponibile su secure. edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches /2013/13-06-17_Editorial_ZfD_EN.pdf, p. 2

[66] Si veda: DE BUSSER, E., "The Adequacy of an EU-US Partnership", in European Data Protec- tion: In Good Health?, cit., p. 185 ss., p. 195.

CONCLUSIONI

Secondo un importante gruppo di ricerca europeo, i cambiamenti tecnologici del nostro tempo hanno dato vita ad un "*digital Tsunami"*, il quale rischia di abbattersi sugli strumenti giuridici che determinano non solo l'identità, ma la stessa libertà degli esseri umani.[67] Al fine di proteggersi da questa grave calamità, il Sistema Internazionale ha bisogno di importanti barriere dal punto di vista normativo: l'"impero dei diritti" necessita di allargare i propri confini[68], ma quest'azione non basta se adottata dai singoli Stati in maniera disorganica. Viviamo oggi in una "*networked public sphere*"[69], una vera e propria "area pubblica" dominata dalle relazioni sociali e dal massiccio scambio di informazioni sul web. Questa espansione, di conseguenza, risulterebbe indubbiamente inefficace se non venisse accompagnata da una concertazione internazionale per ciò che concerne la regolamentazione di specifiche materie, troppo spesso affrontate in maniera frammentaria o, ancor peggio, affidate all'ambiguità della *governance*. Il caso *Datagate*, così come le sue conseguenze nel campo del diritto internazionale, ha messo in luce questa problematica nel delicatissimo ambito della protezione della privacy e della tutela dei dati personali. Nel corso del primo capitolo si è potuto notare come l'esigenza di portare all'attenzione delle Nazioni Unite la materia sopracitata sia diventata massima dopo l'esplosione delle rivelazioni di Snowden. La volontà di far fronte alla questione era stata innegabilmente già espressa, più volte, soprattutto in ambito comunitario[70]; ciononostante, pare siano bastate le confessioni di un *whistleblower* a far vacillare, nel vecchio continente, un sistema ricco di presidi normativi adeguati nella forma ma inefficaci nella sostanza. L'inconsistenza della regolamentazione europea è stata enfatizzata dall'invasività delle norme antiterrorismo provenienti, in particolar modo, dall'altra sponda dell'Atlantico, dove il trade-off libertà/sicurezza è spesso sbilanciato verso la seconda sfera ai danni della prima. A riprova di ciò, nel corso del secondo capitolo, si sono prese in esame le similarità e le differenze tra

[67] The Future Group, *Freedom, Security, Privacy: European Home Affairs in an Open World,* disponibile su http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf (conslutato il 6/10/2014).
[68] Rodotà, S., *Il Diritto di avere Diritti,* editori Laterza, Bari, 2012, p66.
[69] Friedland, L.A., Hove, T., Rojas, H., *The Networked Public Sphere*, in *Javnost-The Public*, *Journal of the European Institute for Communication and Culture*, vol.13, n.4, pp.5-26, disponibile su http://javnost-thepublic.org/media/datoteke/13-4-friedland.pdf (conslutato il 6/10/2014).
[70] Basti pensare alle direttive comunitarie e alle modifiche al trattato di Lisbona, più volte presi in esame nei precedenti capitoli.

la normativa Europea e quella Statunitense, rilevando una più meticolosa attenzione del vecchio continente in ambito di diritto alla privacy e alla protezione dei dati personali, e al contrario una minor considerazione degli americani verso queste materie, sovente eclissate dalla spropositata forza normativa dello USAPA. L'estensione delle ingerenze statunitensi in Europa, spesso accompagnate dalla tacita o espressa collaborazione (o emulazione) di alcune autorità europee e non europee in esasperate operazioni di *data-mining*[71] evidenziano la assoluta necessità di far fronte alla problematica in ambito internazionale. Prima di ipotizzare un possibile sostrato normativo comune, tuttavia, gli Stati hanno bisogno di creare una serie di presupposti affinché un concreto numero di regole internazionalmente condivise possa agire con i giusti presidi. In particolare in ambito europeo e statunitense, oltre ai più generali provvedimenti menzionati in conclusione al precedente capitolo, vi sono alcuni rimedi che sarebbe auspicabile adottare. In riferimento al caso europeo, ad esempio, è stato suggerito, oltre ad una più rigorosa ed effettiva applicazione delle norme già in vigore, una modificazione della direttiva sulla *data retention*, che risulta eccessiva nelle sue scadenze (da 6 mesi a 2 anni). Ciò al fine di ricondurre il processo di data mining ad un *rispetto effettivo e concreto dei principi di proporzionalità e finalità limitata*[72]. L'Unione Europea deve inoltre muoversi in parallelo con le altre organizzazioni internazionali, al fine di garantire una indispensabile coerenza all'interno dell'ordinamento giuridico del vecchio continente. Questa esigenza è percepita anche dal Garante Europeo per la protezione dei dati, il quale così si esprime in un suo parere del 7 Marzo 2012:

> *La riforma delle norme UE va in parallelo con la modernizzazione delle norme sulla protezione dei dati adottate in altre organizzazioni internazionali. Attualmente, in parallelo alla UE, il Consiglio d'Europa sta valutando come la Convenzione per la protezione delle persone fisiche con riguardo al trattamento automatizzato di dati di carattere personale ('convenzione 108') potrebbe essere modificata per affrontare le sfide di oggi. Lo stesso esercizio si svolge per quanto riguarda le OCSE Privacy Guidelines.*

Nell'ambito della normativa statunitense, invece, è importante che il diritto alla privacy sia interpretato come un principio fondamentale al pari del diritto alla sicurezza, e annoverato

[71] Si pensi al caso francese e alle rivelazioni del quotidiano *Le Monde* sulla collaborazione della DGSE, oppure al programma *Tempora* britannico, o ancora al *Central Monitoring System* indiano.
[72] Nino, M., *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* op. cit., p.746.

tra i diritti umani fondamentali. Bisogna inoltre far sì che il *Safe Harbor*, già definito come "ponte normativo" tra Europa e Stati Uniti, non si riduca ad un semplice canale di trasmissione di dati, tradendo la propria natura di meccanismo di tutela.

Da ciò si deduce che l'evidente utilità del caso preso in esame. Esso è indubbiamente una lezione dalla quale bisogna prendere spunto per una radicale riforma internazionale delle norme sulla protezione dei dati e la tutela della privacy. Non bisogna di conseguenza pensare al *Datagate* come semplice fenomeno foriero di disaccordi e agitazioni nel sistema internazionale. Esso ha al contrario messo in luce le crepe già presenti, a livello globale, in ambito di protezione dei dati personali e tutela della privacy collegate al cyberspazio. Il caso *Datagate* deve dunque essere interpretato non come fattore distruttivo, bensì come occasione per mettere in piedi un sistema di norme internazionalmente condivise che siano dotate di *opinio iuris* sufficiente affinché diventino effettive, vincolanti e inderogabili, e che proteggano l'integrità degli individui dall'arbitraria e indebita appropriazione di dati sensibili relativi alle persone fisiche.

Habeas Data

Il celebre giurista Stefano Rodotà, in un suo libro dal titolo *Il diritto di avere diritti*, mette in particolare risalto l'importanza del cyberspazio come luogo in parte inesplorato dal diritto, che rappresenta un'enorme opportunità per lo sviluppo delle facoltà individuali e sociali ma che allo stesso tempo può tramutarsi in una minaccia, se non dotato di efficaci protezioni normative internazionalmente condivise. La rete e in particolare lo sviluppo del 2.0, che ha determinato la nascita dell'"io sociale dell'era digitale", si presenta oggi come uno spazio in cui gli individui condividono, in maniera più o meno consapevole, un'enorme mole di informazioni personali. Internet si rivela un mezzo profondamente diverso rispetto ai mass media tradizionali: se, infatti, la possibilità di accesso a questi mezzi di comunicazione di massa *trova un limite nella loro stessa natura*[73], non può dirsi la stessa cosa per la rete, con i vantaggi e gli svantaggi che ne conseguono. Il diritto di accesso ad internet dovrebbe dunque essere regolamentato con apposite norme che però tengano conto di una serie di accordi internazionali in materia di protezione dei dati. Al concetto di regolamentazione

[73] Rodotà, S., *Il Diritto di avere Diritti,* op.cit., pag386.

comune si collega inoltre un'altra peculiare caratteristica del web. Quest'ultimo, infatti, non ha confini ben delimitati, e se anche si è cercato, talvolta, di imporre barriere (anche piuttosto stringenti), quest'azione è risultata quanto mai difficoltosa. Per questo motivo, nei rari casi in cui gli stati siano riusciti a limitare l'accesso ad Internet, ciò è avvenuto con enormi difficoltà e al prezzo di una smisurata restrizione delle libertà di stampa e di associazione[74]. Non è dunque auspicabile precludere gli accessi -andando contro l'art.19 della DUDU sul diritto di cercare e ricevere informazioni-, bensì disciplinare accessi consapevoli. La prima, più importante consapevolezza nella dimensione del 2.0, è che "*lo schermo sul quale la persona proietta la sua vita non è più quello del suo personal computer, […]* ma *tende a coincidere con l'intero spazio della rete"*[75]. L'enunciazione originaria della privacy come "diritto ad essere lasciato solo", in questo contesto, risulta quanto mai inappropriata. La personalità degli individui viene condizionata dall'enorme mole di informazioni che essi forniscono alla rete e che ricevono dalla stessa. Nondimeno, i dati relativi agli individui sono conosciuti con sempre maggior facilità da soggetti pubblici e privati attraverso un insieme di meccanismi di *data mining* che possono incidere su una serie di diritti individuali e collettivi. Non a caso l'attuale Presidente dell'Autorità Garante per la protezione dei dati personali, Antonello Soro, nel corso di una conferenza tenuta presso l'Università LUISS Guido Carli, ha individuato nell'attacco alle banche dati la più violenta e distruttiva forma di aggressione ad uno Stato e ai suoi cittadini. L'essere umano, che nel nostro tempo ha compiutamente dato vita ad un essere digitale inscindibilmente legato all'identità della persona fisica, necessita oggi di un'effettiva difesa del proprio *corpo elettronico*. Da qui si sviluppa il concetto di *Habeas Data*, mutuato dal ben più celebre *Habeas Corpus*, grazie al quale si sono mossi i primi passi nella storia dello sviluppo delle libertà personali. L'attualità di questa questione è quanto mai evidente, in quanto essa affronta la questione della sorveglianza di massa e l'appropriazione arbitraria di quella che, ad oggi, si presenta come una parte considerevole dell'identità di un individuo. Il concetto sovresposto è inoltre foriero di una serie di altri princìpi, più volte citati soprattutto nell'ambito della normativa europea. Primo fra tutti il diritto all'oblio, oltre ai princìpi di proporzionalità e finalità limitata. Da ciò si può dedurre come l'importanza della questione

[74] Si pensi alla rete intranet nordcoreana *Kwangmyong*, in cui sono presenti pochissimi siti internet approvati dal Governo e il cui accesso è tra l'altro interdetto alla quasi totalità della popolazione della Corea del Nord.
[75] Rodotà, S., *Il Diritto di avere Diritti*, op.cit., p.395.

sia oggi assolutamente primaria, ed essa debba essere affrontata dal Diritto Internazionale. Se si vuole affrontare la difficile questione della tutela delle persone fisiche nel mondo di internet, non vi può essere una così grande discrepanza tra la tutela delle comunicazioni interne e la scarsa tutela in materia di traffico internazionale di dati, né si può ragionevolmente disciplinare tali materie solo attraverso il principio di territorialità. Le azioni in seno all'Assemblea Generale delle Nazioni Unite, in particolare la risoluzione 68/167, così come il recente rapporto dell'ufficio dell'Alto Commissario delle Nazioni Unite per i Diritti Umani sulla materia in questione, sono indicativi di una precisa volontà di modificare questi aspetti, ma ciò non pare ancora sufficiente. La protezione delle informazioni personali della generazione del web 2.0. dovrebbe infatti far parte di quel diritto cogente che esercita una *"vertical domestication"*[76] sugli Stati, in modo da far sì che gli stessi rispettino universalmente tale principio e che quest'ultimo possa effettivamente tutelare gli individui, dentro e fuori dallo spazio cibernetico, permettendo di conseguenza un effettivo e concreto esercizio delle libertà di espressione e di opinione nell'era digitale.

[76] Koh, H.H., *Why do Nations Obey International Law?,* in "Yale Law Journal",1, 1997,pp.2599 e sgg.

BIBLIOGRAFIA

- BONFANTI, M., *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti Umani e Diritto Internazionale*, 2011
- BRENNAN CENTER FOR JUSTICE, *Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs*.
- FRIEDLAND, L.A., Hove, T., Rojas, H., *The Networked Public Sphere*, in Javnost-The Public, *Journal of the European Institute for Communication and Culture,* vol.13, n.4
- FRIEDMAN, L., *The Republic of Choice. Law, Authority and Culture*, Harvard University Press, Cambridge (Mass.)-London 1990.
- HIJMANS, H., *Recent Developments in Data Protection at European Union Level*, in *ERA-Forum*, 2010.
- JAEGER, P.T., BERTOT,J.C.,MCCLURE, C.R., *The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act*, in *Government Information Quarterly*, 20/3/2013.
- KOH, H.H., *Why do Nations Obey International Law?*, in "Yale Law Journal",1, 1997
- KOSTA, E., VALCKE, P., *The EU Data Retention Directive. Retaining the Data Retention Directive*, in *Computer Law & Security Report* 2006
- MACASKILL,E., BORGER,J., HOPKINS,N., DAVIES,N.,BALL,J., "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications", in *The Guardian*, 21 giugno 2013,
- MAYER, J.D., *9-11 and the Secret FISA Court: From Watchdog to Lapdog?*, in *Case Western Reserve Journal of International Law*, 2002.
- MCGEE, J. (2001, Nov. 4). *An intelligence giant in the making; antiterrorism law likely to bring domestic apparatus of unprecedented scope*. Washington Post, November 4, 2001.
- NINO, M., *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 *Diritti Umani e Diritto Internazionale*, 3/2013.

- O'DONNELL, M.J., *"Reading for Terrorism: Section 215 of the USA Patriot Act and the Constitutional Right to Information Privacy",* in *Journal of Legislation* 2002
- PAREDES, I., *Francia, Italia, España y Portugal le negaron tránsito aéreo a Evo*, in *La Razón*
- RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, Bruxelles-Paris 1990
- RODOTÀ, S., *Il Diritto di avere Diritti*, editori Laterza, Bari, 2012.
- SOTTIAUX, S., *Terrorism and Limitation of Rights: The ECHR and US Constitution*, Oxford, 2008.
- WARREN, S. e BRANDEIS, L.D., *The Right to Privacy*, in *Harvard Law Review*, 5, 1890
- WESTIN, A., *Privacy and Freedom*, Atheneum, New York 1970.
- WHITEHEAD,J.W., ADEN, H., *"Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives"*, in *American University Law Review*, 2002.
- YOUNG, M.G. (2001). *What big eyes and ears you have! A new regime for covert governmental surveillance*, in *Fordham Law Review*, 70(6), 1017-1109.

SITOGRAFIA

http://www.fisc.uscourts.gov

http://www.internazionale.it

http://javnost-thepublic.org

http://la-razon.com

https://optin.stopwatching.us

http://www.out-law.com

http://www.statewatch.org

www.interlex.com

www.europa.eu

www.theguardian.com