Mariavittoria Catanzariti

L'invisibilità del potere nel prisma della sorveglianza elettronica

Il ricorso capillare alla *mass surveillance* – esemplificato dal recente fenomeno del *Datagate* – è stato spesso giustificato come il miglior modo di proteggere i cittadini dal terrorismo globale. Quest'affermazione, apparentemente generica, è in realtà un campo minato di semplificazioni e paradossi, l'uso dei quali manipola fortemente il significato della democrazia. Una delle principali variabili di tale uso è rappresentata dall'alternativa visibilità/invisibilità. I programmi della *National Security Agency*, come *Prism*, *Upstream*, *X-Keyscore*, resi pubblici in seguito alle rivelazioni di Edward Snowden, sono caratterizzati dalla combinazione dell'uso di tecnologie avanzate con le politiche di controllo, per lo più segrete. L'impatto delle trasformazioni tecnologiche nelle società democratiche assume dimensioni tali da far mutare profondamente la percezione dei diritti nel contesto globale: ciò altera inevitabilmente i meccanismi di legittimazione democratica, il peso degli attori pubblici e privati, il prezzo del consenso e i limiti della giurisdizione extraterritoriale. Fenomeni come "*Big Data*" e "*Data Mining*" rappresentano la grande metafora della decostruzione dell'individuo e del suo spazio politico contestualmente alla creazione di altre forme di potere.

La questione urgente riguarda la trasversalità delle politiche dell'invisibilità. Si assiste sempre più al dispiegarsi di complesse dinamiche che attengono a fenomeni globali di *governance*. Occasioni di contraddittorio, confronto e pluralismo politico diventano sempre più rarefatte e non direttamente riferibili a poteri istituzionalizzati, bensì a nuclei emergenti di potere. Ciò accade non soltanto in ordinamenti diversi, ma anche a livelli diversi – nazionale, sovranazionale, transnazionale – nel pubblico così come nel privato. Il risultato consiste in una costante mimesi nell'uso dell'invisibilità da parte di poteri diffusi. Attraverso l'invisibilità dell'esercizio del potere, si misura, infatti, la forza degli attori in gioco. Ecco dunque che l'invisibilità, avendo nei sistemi legali democratici la funzione di sottrarre quote indisponibili di vita alla dimensione politica, si presta molto bene all'uso emergenziale, che costituisce, tuttavia, soltanto una delle sue più evidenti declinazioni.

Quest'articolo, muovendo da una prospettiva teorica, avrà ad oggetto l'analisi del fenomeno del *Datagate*, alla luce del raffronto tra la legislazione e la giurisprudenza americana ed europea.

1. Il segreto della trasparenza

Il fenomeno della *mass surveillance* può essere compreso se lo si colloca all'interno del mutamento di alcune variabili rilevanti del rapporto tra potere e diritti. Come osservato da David Lyon, la sorveglianza di massa può essere definita come "the focused, systematic and routine attention to personal detail for purpose of influence, management, protection and direction"[1]. Essa rappresenta una modalità attraverso la quale è possibile "strutturare il campo d'azione possibile degli altri"[2].

Innanzitutto, sembra necessario porsi un interrogativo preliminare, e cioè se gli effetti che le tecniche di sorveglianza di massa determinano sulle libertà civili e sui diritti fondamentali possano ancora iscriversi nella parabola del costituzionalismo moderno. La costituzionalizzazione dello spazio comunicativo può indubbiamente rappresentare una variabile teorica al modello del costituzionalismo politico[3]. Nelle pagine seguenti si analizzeranno alcuni profili particolari di questo processo.

Vi è da osservare, in primo luogo, che la sorveglianza di massa costituisce un esempio evidente di tecnica segreta di controllo, la quale si avvale della trasparenza virtuale e della possibilità di condividere dati su basi macroscopiche. In secondo luogo, nelle società contemporanee le tecniche di sorveglianza di massa trascendono la dicotomia pubblico/privato, nel senso che possono essere utilizzate indifferentemente sia da attori pubblici sia da attori privati. In sostanza, l'indifferenza di tali tecniche all'uso che ne è fatto tanto da attori pubblici, quanto da attori privati, rappresenta la caratteristica fondamentale. La sorveglianza di massa recide, infatti, quella complementarità oppositiva tra pubblico e privato che sta alla base del sistema dei diritti costituzionalmente garantiti.

Attorno a questa nuova costellazione di fenomeni, che richiedono in ogni caso tutele e rimedi, vi è anche un'incertezza teorica al riguardo. Come osservato da Neil Richards e Jonathan King, la sorveglianza di massa dà luogo a tre fondamentali paradossi: il primo, quello della trasparenza, consiste nel fatto che la sorveglianza, e dunque la conoscibilità dei dati degli individui, si realizza attraverso programmi segreti; il secondo, quello dell'identità, consiste nella cristallizzazione dell'identità di un individuo sulla base dei suoi comportamenti oggetto di videosorveglianza, il che altera sensibilmente il libero determinarsi del paradigma identitario; il terzo, quello del potere, probabilmente il più insidioso, consiste nel fatto che l'apparente riconoscimento di alcuni diritti, come ad esempio la trasparenza in rete, avviene

1 D. Lyon, *Surveillance Studies*, Cambridge, Polity Press, 2007, p. 18.

2 M. Foucault, *Perché studiare il potere. La questione del soggetto*, in H. L. Dreyfus-P. Rabinow, *La ricerca di Michel Foucault. Analitica della verità e storia del presente*, Firenze, Ponte alle grazie, 1989, p. 249

3 G. Teubner, *Fragmented Foundations. Societal Constitutionalism beyond the Nation State*, in P. Dobner – M. Loughlin, *The Twilight of Constitutionalism?*, Oxford University Press, Oxford, 2010, p. 327.

parallelamente alla crescita del potere di attori privati che controllano la selezione e l'aggregazione dei dati[4].

Questi tre paradossi affondano le radici nella storia del rapporto tra visibilità e potere.

Il complesso sviluppo del concetto moderno di pubblicità, nella tradizione giuridica europea, ci mostra un dato costante, e cioè che sin da quando la società non crede più agli *arcana rei naturae*, si appropria costantemente del segreto come strumento di esercizio del potere. L'oggettivazione dell'arcano consiste, dunque, in un processo di differenziazione costante tra il segreto e ciò che esso regola. Tale complesso processo può essere interpretato attraverso diverse letture. Nella modernità, ad esempio, il problema del diritto consiste nelle tecniche di disciplinamento dell'invisibilità. Il diritto moderno scommette, infatti, sulla possibilità che la politica cessi di "apparire" in pubblico attraverso le sue forme. Tuttavia, i meccanismi di incorporazione che il diritto pone in essere non sono integrali. La legittimazione di alcune pratiche sociali opera, infatti, attraverso il meccanismo pubblico della segretezza, che consiste nella previsione di forme pubbliche atte a riconoscere e localizzare l'uso di alcune pratiche segrete. La previsione pubblica del segreto è, infatti, volta a legittimare il carattere arbitrario della decisione segreta. Le forme democratiche sono, infatti, quelle che più delle altre fanno uso del segreto, proprio perché devono riconoscere pubblicamente il limite al potere. Esse necessitano, dunque, di un *surplus* di legittimazione. Esiste, tradizionalmente, un limite di compatibilità tra l'uso del segreto e la democrazia, che consiste nella previsione pubblica, circoscritta a determinati casi e tassativa, dell'uso del segreto. Il ricorso all'invisibilità risulta, pertanto, una pratica giustificabile nella misura in cui essa si collochi all'interno di un processo che di per sé non è segreto[5]. Il fatto che l'invisibilità sia diventata soltanto in tempi recenti sintomatica di una logica emergenziale, ha in realtà ragioni profonde. Esse si rinvengono in una lunga elaborazione teorica, nella quale il segreto ha rappresentato, sin dalla nascita del moderno, la forma comunicativa del nucleo vitale del potere[6].

La localizzazione del segreto, quale schermo di un esercizio illegittimo del potere, è stata, nella storia dei sistemi giuridici europei, legata allo slittamento della linea di confine tra pubblico e privato. In altre parole, molto spesso l'alterazione dell'equilibrio tra pubblico e privato ha determinato la creazione di spazi di invisibilità, rendendone tuttavia visibili i luoghi. Il dare un "volto" all'uso del segreto ha permesso, seppur in maniera limitata, di sviluppare nella democrazia una forma di controllo da parte dell'opinione pubblica. Tale fenomeno si è reso possibile grazie alla resistenza di alcuni limiti all'esercizio indiscriminato del po-

4 N. M. Richards and J. H. King, *Three Big Paradoxes on Big Data*, "Stan. L. Rev. Online", 41, 2013, p. 66.

5 Cfr. D. F. Thompson, *Democratic Secrecy*, "Political Science Quarterly", Vol.114, n.2, 1999, p. 181, p. 182: "Publicity is the pre-condition of deciding democratically to what extent (if at all) publicity itself should be sacrificed".

6 Cfr. più diffusamente M. Catanzariti, *Segreto e potere. I limiti della democrazia*, Torino, Giappichelli, 2014, p. 113.

tere, che hanno costituito i presupposti dello sviluppo delle forme democratiche contemporanee e del neo-costituzionalismo.

Nella tradizione giuridica moderna il riconoscimento dei diritti individuali è avvenuto contestualmente alla creazione dello stato assoluto, poiché tali diritti si sono sviluppati quale forma di emancipazione nei confronti dell'espansione del potere pubblico[7]. Tale complesso fenomeno si è sviluppato attraverso precise tecniche di disciplinamento dei saperi, che hanno determinato la diffusione di forme di controllo sulla produzione della conoscenza.

Questo passaggio è indice, tra i tanti, delle trasformazioni che investono la dicotomia pubblico/privato. Mentre, infatti, il rapporto tra potere e invisibilità è transitato, nella costruzione dello stato di diritto, attraverso la parabola del pubblico, facendo da contraltare al privato, fenomeni come il *datagate* dimostrano che l'appropriazione da parte di pubblico e privato del potere invisibile è stata non soltanto convergente, ma persino concorrente nelle modalità e nei fini[8].

Il problema che si pone nell'era della sorveglianza di massa è, in primo luogo, quello di comprendere se tale inquadramento teorico richieda alcuni correttivi. In secondo luogo, la questione non è tanto quale sia la portata di clausole generali, come la *national security*, in nome delle quali i diritti possono essere sacrificati, bensì in quale misura i meccanismi di disciplinamento delle informazioni regolate dalle nuove tecnologie siano indipendenti dall'esercizio del potere. In altre parole, la pratica di acquisizione, collezione e utilizzo dei dati dei privati, attuata al solo scopo del controllo fine a se stesso come giustificazione della lotta al terrorismo, e cioè ad esempio non in vista di un'indagine penale, seppur non individui necessariamente un *target* determinato di destinatari, ha la funzione di accrescere la forza del potere. La delocalizzazione, tuttavia, non ne diminuisce la forza, poiché la produzione di potere è destinata in ogni caso a espandersi in assenza di limiti al suo esercizio. La *mass surveillance* ha completamente eroso il concetto di limite, operando al di fuori della logica disciplinante delle pratiche di controllo. Una delle ragioni è in parte la totale indipendenza della *mass surveillance* dal rapporto tra pubblico e privato. Al contrario, le tecniche di sorveglianza di massa si avvalgono della cooperazione tra attori pubblici e attori privati. Tra questi ultimi non vi sono soltanto alcune imprese, come le compagnie telefoniche, che traggono naturalmente profitto dalla collezione dei dati, ma anche gli stessi individui che volontariamente decidono di condividere i propri dati su piattaforme virtuali, alleggerendo notevolmente il lavoro della NSA. Il consenso preventivo al trattamento dei dati personali fornito dagli utenti dei *social network* è soltanto un esempio dell'uso strumentale del consenso individuale da parte dei grandi giganti del web. Tale trasversalismo produce l'effetto di neutralizzare l'operatività della dicotomia pubblico/privato come fonte di equilibrio tra poteri e come forma vitale dialettica

7 *Ivi*, p. 87; C. Graeber, *Internet creativity, communicative freedom and a costitutional rights theory response to "code is law"*, in S. A. Pager – A. Candeub, *Transnational Culture in the Internet Age*, Northampton, Edward Elgar, 2012, pp. 135-164, p. 156.

8 Cfr. N. M. Richards, *The Dangers of Surveillance*, "Harvard Law Review", vol. 126, 2013, p. 1935.

della democrazia. L'inedito al quale si assiste, tuttavia, consiste nella gestione di un'enorme mole di dati da parte di attori indifferenziati, tanto pubblici quanto privati. Il fenomeno del "data mining" non può ad esempio essere interpretato in base al modello costituzionale della divisione tra poteri, del bilanciamento degli interessi e del tentativo di evitare il primato del pubblico sul privato o del privato sul pubblico. Il *target* delle tecniche di sorveglianza di massa non è il singolo individuo, bensì masse indifferenziate di dati. L'elemento quantitativo del controllo costituisce una variabile significativa per la comprensione del fenomeno, che nella sua dimensione di scala, assorbe già di per sé *a priori* le diverse conseguenze che comporta: "it is not possible to go against the flow".

Il concetto di rete, che sempre di più disarticola la struttura gerarchica del potere, muta notevolmente la fisiologia del controllo: essa non è più apparentemente verticistica, bensì circolare. Il tradizionale schema del *panopticon* di Bentham viene, infatti, sempre più sostituito dalla struttura reticolare del *network*, nel quale gli individui sono sorvegliati mentre hanno la possibilità di sorvegliare. Ciò comporta l'apparente creazione di uno spazio di libertà, cioè della capacità di controllo individuale attraverso l'acquisizione di informazioni. Tuttavia, esso delocalizza notevolmente la responsabilità degli attori in gioco, determinando un meccanismo inversamente proporzionale, nel quale al crescente potere diffuso corrisponde una riduzione delle forme effettive di controllo individuale.

2. Dalla 'tecnica' al target

La dinamica dell'invisibilità del controllo dei dati funziona in maniera mimetica, nel senso che poteri concorrenti tra loro ne replicano i meccanismi in maniera reciproca. Ciò non consente di considerare isolatamente le dinamiche inerenti alla sorveglianza né dal lato degli stati né da quello del mercato. La cooperazione tra questi poteri disinnesca, infatti, la logica antagonista del limite al controllo segreto dei dati. L'osservazione di questi fenomeni è interessante poiché ha generalmente ad oggetto ipotesi di indisponibilità dei diritti. Le pratiche sottratte al controllo pubblico vengono giustificate spesso, in maniera visibile, attraverso il filtro del segreto di stato. A tal proposito, con riferimento agli Stati Uniti, è degno di nota il caso *ACLU* v. *NSA* [9], nel quale un gruppo di giornalisti, accademici, avvocati e organizzazioni no profit fece ricorso alla corte federale dell'Eastern District of Michigan, lamentando la violazione da parte dell'Esecutivo della dottrina della violazione dei poteri, del Primo e del Quarto Emendamento, nonché di alcune leggi federali e del FISA relativamente alla condotta di intercettazioni illegali[10]. Il Governo replicò opponendo lo *state secret privilege*, ma la corte dispose l'inapplicabilità della

9 *American Civil Liberties Union* v. *NSA*, 493 F.3d 644 (6th Circ. 2007).

10 Cfr. sul punto F. Bignami, *European Liberty Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, "Boston College Law Review", vol. 48, n.3, 2007, pp. 614-619.

Totten Rule (cioè la *non justiciability* del segreto di stato) al caso di specie, perché non riguardava rapporti di spionaggio. Nel sistema statunitense si è molto diffuso nell'ultimo decennio l'utilizzo delle *National Security Letters* (NSL), autorizzazioni attraverso le quali il *Fedeal Bureau of Investigation* (FBI) può ottenere informazioni sulle persone da parte di compagnie telefoniche, Internet providers, banche, agenzie di credito e altre istituzioni, alle quali è posto il divieto di svelarne l'esistenza ai diretti interessati. Il problema fondamentale riguarda l'onere della prova da parte di chi agisce in giudizio, poiché coloro ai quali vengono dirette tali tecniche di sorveglianza, non possono provare l'esistenza di programmi segreti, il cui contenuto non è evidentemente accessibile. Nel caso *Al-Haramain Islamic Foundation, Inc. v. Bush*[11], la District Court dell'Oregon, e nel caso *Clapper v. Amnesty International USA*[12] anche la Corte Suprema hanno ritenuto che sulla parte attrice ricadesse l'onere della prova in merito alla segretezza dei programmi di sorveglianza.

Da ultimo, la Court of Appeals for the Second Circuit di New York, in una recentissima sentenza del 7 maggio 2015, *ACLU v. Clapper*[13], ha dichiarato il sistema di intercettazioni telefoniche americane illegittimo, ribaltando la decisione di primo grado della District Court for the Southern District of New York[14], che invece aveva rigettato le richieste dei ricorrenti sostenendo la mancata violazione del Primo e del Quarto Emendamento della Costituzione Federale. In particolare, secondo la Corte il § 215 del US Patrioct Act, consentendo il trasferimento dei metadati telefonici dalle compagnie telefoniche alla NSA, non aveva violato il Primo e il Quarto Emendamento e precludeva implicitamente il controllo giurisdizionale.

Da parte dello stato, dunque, vi è ancora una forte resistenza del baluardo della sicurezza nazionale come giustificazione di pratiche che sarebbero altrimenti illegittime.

Anche in Europa, il Trattato di Lisbona ha dato impulso alla disciplina della segretazione degli atti a livello comunitario [15]. Come noto, l'art. 346 TFUE fa salva la facoltà di ciascuno stato membro di non "fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza con l'obbligo di leale cooperazione tra gli stati e le stesse istituzioni" [16]. Questa norma si riferisce essenzialmente a tre categorie di documenti: quelli atti a garantire la protezione della pubblica sicurezza, della difesa e delle materie mili-

11 *Al Haramain Islamic Foundation v Obama*, No. 07-0109 (N.D. Cal. 31 March 2010).

12 *Clapper v. Amnesty International USA*, 133 S. Ct. 1138(2013).

13 *American Civil Liberties Union v. James Clapper*, no. 13-3994 (S.D. New York December 28, 2013).

14 *ACLU v. Clapper*, District Court, South. Distr. N.Y. (27 December 2013).

15 Sulle attuali trasformazioni della ragion di stato cfr. M. Koenig-Archibugi, *International Governance as New* Raison d'État*? The Case of the EU Common Foreign and Security Policy*, "European Journal of International Relations", vol.10, n.2, p. 174: "The *new raison d'état* approach asserts that intergovernmental cooperation can be the result of collusive delegation, i.e. the attempt by government to loosen domestic constraints by shifting decision-making to international settings and organizations".

16 Cfr. sul punto H. Kranenborg, *Access to documents and data protection in the European Union: on the public nature of personal data*, "Common Market Law Review", vol. 45, 2008, p. 1079 ss.

tari, delle relazioni internazionali, della politica finanziaria ed economica; quelli ai quali è consentito l'accesso soltanto se vi è il rischio del pregiudizio di un interesse pubblico; infine i documenti, il cui disvelamento comprometterebbe il processo decisionale in seno alle istituzioni [17]. Il problema è emerso nel momento in cui il trattato di Amsterdam ha riconosciuto l'accesso ai documenti del Parlamento, del Consiglio e della Commissione (art. 255 TCE), fino allora coperti da segreto [18]. Il regolamento applicativo di tale disposizione (Regolamento CE 1049/2001) prevede, infatti, la regola dello stato autore come principio generale, sottoponendo, cioè, la divulgazione degli atti al consenso dell'autorità che li ha redatti [19]. In tal modo entra in gioco, ponendosi in apparente conflitto, la disposizione di cui all'art. 4 TUE, che salvaguarda il principio di leale cooperazione. Esisterebbero, in base alla lettura congiunta delle norme, due diversi regimi di segretezza: il primo volto a individuare nel principio di trasparenza la regola generale, derogabile in base alle condizioni previste dall'art. 4 TUE, cioè in base al principio di leale collaborazione, prescindendo dalla volontà dello stato autore responsabile della classifica di segretezza; l'altro volto a tutelare, attraverso l'eccezione dell'art. 9 di detto Regolamento (che rinvia all'art. 4), i cosiddetti documenti sensibili, cioè "quei documenti provenienti dalle istituzioni o dalle agenzie da loro istituite, da Stati membri, paesi terzi o organismi internazionali, classificati come "confidential", "secret" e "top secret", riguardanti interessi essenziali dell'Unione europea o

17 *Ivi*, p. 1084.

18 L'entrata in vigore del Trattato di Lisbona ha inoltre fornito un rimedio alla mancanza di controllo da parte del Parlamento europeo in materia di missioni civili e militari dell'UE, attraverso la predisposizione del Servizio europeo per l'azione esterna (SEAE) nel dicembre 2010. Al Segretario Generale del SEAE fanno capo il centro di coordinamento dell'intelligence (Sitcen) e la direzione generale responsabile delle delegazioni esterne e del bilancio. Delle altre direzioni generali, una ha compiti di ordine generale e di *crisis management*, mentre le altre si occupano di aree o paesi specifici. In risposta all'interrogazione parlamentare n. 4-03732 (Fascicolo n. 110), sono state definite le funzioni del centro di coordinamento: "Il SITCEN non si configura come un vero e proprio organo di *intelligence*, in quanto non effettua direttamente attraverso il proprio personale la raccolta delle informazioni che successivamente elabora. Il Centro attinge però a numerose fonti liberamente disponibili (le cosiddette fonti aperte, *open source intelligence*) e, grazie all'attivo sostegno degli Stati membri, anche ad informazioni rese da queste disponibili in via riservata. In virtù di tali contributi il Centro analizza, elabora e rende disponibili informazioni su temi di sicurezza (interna ed esterna alla UE), sia per usi civili che militari". Il centro opera ventiquattro ore su ventiquattro monitorando gli eventi su scala mondiale e producendo dei rapporti giornalieri. Sul punto cfr. M. Comelli – R. Matarazzo, *La coerenza della politica estera europea alla prova: il nuovo Servizio europeo per l'azione esterna*, in "Documenti Istituto Affari Internazionali" (IAI 1010), 27 maggio 2010. Disponibile in: http://www.iai.it/pdf/DocIAI/iai1010.pdf. Accesso effettuato in: 28/02/14.

19 A. Vedaschi, *Il segreto di stato tra tradizione e innovazione: novità legislative e recenti evoluzioni giurisprudenziali*, "Dir. pubbl. comp. eur.", 2012, p. 982; cfr. sul punto D. M. Curtin, *States of Secrecy: the European Union Executive Unbound*, disponibile in: http://www.transparencyconference.nl/papers, p. 23 ss. Accesso effettuato in: 28/02/2014; Id, *States of Secrecy Top Secret Europe*, disponibile in: http://oratierceks.nl/upload/pdf/PDF-5066weboratie_Curtin.pdf, p. 8-10. Accesso effettuato in: 28/02/14.

di uno o più Stati membri"[20]. Tale limitazione ha ad oggetto la tutela dell'interesse pubblico in ordine alla sicurezza pubblica, alla difesa ed alle questioni militari, alle relazioni internazionali, alla politica finanziaria, monetaria o economica della Comunità o di uno stato membro, ma anche la vita privata e l'integrità dell'individuo. L'eccezione si applica soltanto al settore delle relazioni estere e di difesa, al cosiddetto secondo pilastro. Il problema interpretativo, tuttavia, si presenta ogni qual volta ci si trova a dover gestire informazioni sulle quali viene apposta la classifica di segretezza, in maniera differente, a seconda cioè che i negoziati internazionali seguano il riparto di competenze in politica estera e difesa ai sensi dell'art. 9 del Regolamento, o ai sensi dell'art. 218 TFUE. In questo caso, infatti, il trattato prevede che il Parlamento debba essere informato in modo "completo e tempestivo" durante le fasi dei negoziati, senza che la Commissione o il Consiglio possano essere legittimati a negare l'accesso a informazioni coperte dal segreto, o possa applicarsi la regola del "rifiuto dello stato terzo autore"[21]. L'eccezione prevista dal suddetto regolamento imporrebbe dunque un divieto di disparità di trattamento. Invero, le ragioni che hanno portato all'adozione della disposizione in esame erano legate all'imminente scadenza del termine fissato dal Trattato per l'adozione del regolamento e l'adozione formale a livello europeo degli standard Nato nei settori della politica estera e della difesa. Il rinvio ai regolamenti pose, infatti, fine al problema, poiché l'adeguamento agli standard Nato sarebbe anche potuto avvenire a livello interno, eludendo le difficoltà che si erano manifestate in sede di accordi tra Parlamento e Consiglio[22]. In particolare, tra gli standard Nato fu riprodotta la disposizione che richiedeva il consenso dello stato autore per la declassificazione del documento sensibile[23]. Inoltre i cosiddetti "treaties on mutual legal assistance" (MLATs) tra Europa e Stati Uniti, che coprono le indagini penali, ma non i programmi di sicurezza nazionale, contengono numerose eccezioni al dovere di cooperazione[24]. Il problema del doppio regime, dunque, investe non soltanto le informazioni sulla sicurezza nazionale ma anche la protezione dei dati privati. In tal senso, è molto significativo l'impulso politico derivante dagli *intergovernmental intelligence networks*, che a livello transnazionale giocano un ruolo decisamente più incisivo dei trattati[25]. Un *intergovernmental network* può essere definito come

20 Cfr. D. M. Curtin, *Official Secrets and the Negotiation of International Agreements: Is the Eu Executive Unbound?*, "Common Market Law Review", vol. 50, n.2, 2013, pp. 426-427.

21 Cfr. sul punto D. M. Curtin, *Judging EU Secrecy*, "Amsterdam Centre for European Law and Governance", Research Paper N. 2012-07, p. 8.

22 La riflessione sullo spionaggio ha tradizionalmente riguardato il segreto di stato nazionale, il quale aveva come limite principale il territorio statale, cfr. W. Laqueur, *Un mondo di segreti: impieghi e limiti dello spionaggio*, Rizzoli, Milano, 1986, p. 400 ss.

23 E. De Capitani, *Unione Europea e segreto di stato: un quadro normativo ancora in piena evoluzione*, disponibile in: *http://www.astrid-online.it/Riforma-de/Studi-e-ri/Archivio-26/De-Capitani_Unione-europea_segreto-Stato.pdf*, p. 5. Accesso effettuato in: 28/02/14.

24 F. Bignami, *American Liberty Versus European Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, cit., p. 667.

25 Cfr. sul punto F. Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, "Michigan Journal of International Law", Vol.26, 2005,

"a pattern of regular and purposive relations among like government units working across the boarders that divide countries from one another and demarcate the 'domestic' form the 'international' sphere". Attraverso questa pratica adottata indifferentemente al di qua e al di là dell'Atlantico, come osservato da Bignami, gli stati rinunciano al controllo unilaterale sulla politica estera. Un esempio è stato in Europa l'approvazione del Safe Harbor Agreement nel 2000 e di Europol nel 2003. In entrambi i casi vi era stata una forte opposizione da parte del Parlamento, e tali iniziative erano state implementante grazie alla comitologia che assicurava una più diretta cooperazione tra stati nazionali e Commissione Europea. Queste pratiche sono state considerate un esempio di "indirect administration" attraverso la quale le autorità nazionali compiono per prime la decisione che poi viene spesso soltanto confermata a livello europeo dai comitati rappresentanti degli stati nazionali[26]. In particolare, per quel che riguarda la protezione dei dati personali, l'art. 25 della Direttiva 95/46 prevede che il trasferimento dei dati agli stati terzi possa avvenire soltanto quando vi siano determinate condizioni. Innanzitutto, l'adeguatezza dello standard di protezione da parte del paese terzo deve essere determinato alla luce del contesto in cui avviene il trasferimento; deve essere prestata particolare attenzione alla natura, alle finalità e alla durata del trasferimento; il paese d'origine e il paese d'arrivo del trasferimento. Inoltre le autorità nazionali e la Commissione hanno il compito di segnalare rispettivamente i casi di non adeguatezza degli standard adottati dai paesi terzi rispetto alla direttiva. La sottoscrizione del Safe Harbor Agreement mirava a superare i limiti posti dalla Direttiva attraverso un sistema di autocertificazione di adeguatezza degli standard di trattamento dei dati rispetto a quanto imposto dalla Direttiva 95/46/CE da parte delle società americane operanti nel territorio europeo. I principi sui quali si fonda il Safe Harbor Agreement ricalcano grossomodo il contenuto della direttiva Europea: *notice*, *choice*, *onward transfer*, *security*, *data integrity*, *access*, *enforcement*. Tuttavia il sistema dell'autocertificazione del raggiungimento degli standard richiesti è spesso elusivo di tali principi. In base ad essi, i soggetti interessati dovrebbero fornire il proprio consenso al trattamento e al trasferimento dei propri dati, dovrebbero ricevere una notifica da parte delle società che effettuano il trattamento, potrebbero accedere ai propri dati in qualsiasi momento; le società, di contro, dovrebbero assicurare standard adeguati di sicurezza e integralità dei dati, mentre i governi dovrebbero assicurare delle procedure di effettiva protezione e adeguatezza agli standard richiesti. In particolare, tra le policy di sicurezza più diffuse compare sempre l'obbligo di confidenzialità, integrità e accessibilità dei dati.

Il consenso individuale al trattamento dei dati è apparso negli ultimi decenni, in Europa, soprattutto per quel che riguarda il trasferimento dei dati a livello internazionale, uno strumento limitativo della responsabilità dei service provider e delle società che hanno trattato questi dati. Tale questione è ritornata in maniera

p. 807, 845; Id., *Mixed Administration in the European Data Protection Directive: The Regulation of International Data Transfers*, "Rivista Trimestrale di Diritto Pubblico", 2004, p. 31.

26 Id., *Transgovernmental Networks vs. Democracy*, cit., p. 822.

dirompente nel nuovo regolamento sulla protezione dei dati. Recentemente, peraltro, il Parlamento Europeo ha adottato una risoluzione con la quale ha richiesto la sospensione del Safe Harbor Agreement, alla luce delle connessioni con i programmi di sorveglianza di massa[27].

3. Protezione dei dati: "one unique flow"

L'altro effetto evidente del cambiamento di paradigma relativo ai diritti riguarda, per l'appunto, la protezione dei dati personali. A livello esemplificativo, il sistema europeo e il sistema americano rappresentano due differenti modelli culturali che meritano di essere posti a confronto sotto il profilo del significato che il diritto alla privacy ha assunto tradizionalmente in questi contesti.

Mentre in Europa, infatti, il diritto alla privacy è considerato un diritto fondamentale collegato al concetto di dignità della persona, negli Stati Uniti la privacy appartiene alla sfera di autodeterminazione individuale contro le interferenze di attori pubblici e privati, che può anche essere rinunciata pattiziamente a livello contrattuale[28]. In Europa, inoltre, la tutela può essere definita di tipo preventivo, tant'è che la tutela viene anticipata al livello dell'acquisizione dei dati, grazie all'intermediazione delle autorità amministrative indipendenti, in America la tutela avviene *ex post*: acquisizione iniziale dei dati non significa trattamento dei dati, di conseguenza la tutela è spostata a un livello successivo rispetto al modello europeo. Ciò si spiega anche grazie alla diversa propensione all'*adversarial legalism* da parte degli americani rispetto agli europei, i quali preferiscono optare generalmente per negoziazioni di tipo amministrativo [29].

I programmi svelati da Snowden non costituiscono una rottura rispetto al passato nella storia americana. La politica della sicurezza negli Stati Uniti è stata sin dalla creazione della NSA nel 1952 durante la guerra Fredda orientata alle tecniche di sorveglianza dei propri cittadini. Basti pensare a programmi come Ukusa e Watergate.

Nel 2000 fu rivelato il programma ECHELON, al quale seguirono, dopo l'11 settembre, lo USA Patrioct Act e gli emendamenti del FISA, volti alla realizzazione di specifiche misure di sorveglianza nei confronti dei cittadini non europei. La novità dei programmi rivelati da Edward Snowden come *Upstream*, *XKeyscore* o *Bullrun* consiste nel fatto che per la loro attuazione la NSA si avvale della colla-

27 *Motion for a European Parliament on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on translatlantic cooperation in Justice and Home Affairs* (2013/2188 INI), disponibile in: Resolutionhttp://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN. Accesso effettuato in: 20/12/2014.

28 Cfr. sul punto F. Bignami, *American Versus European Liberties*, cit., p. 609; D. Bigo – S. Carrera e altri, *National Programmes for Mass Surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament, European Union, 2013, p. 12,20, 28.

29 Cfr. sul punto R. A. Kagan, *Adversarial Legalism. The American Way of Law*, Cambridge, Harward University Press, 2003, p. 181.

borazione di network pubblici e privati[30]. Il controllo è capillare e va dall'invio di copie dei dati attraverso cavi internazionali a fibre ottiche a indicizzazioni di indirizzi email, indirizzi IP, liste di nomi, numeri telefonici dai quali gli analisti possono ricavare parametri di selezione (cosiddetti "selectors") rilevanti in base al target di individui oppure comportamenti anomali e sospetti rispetto alla media. I dati, inoltre, possono anche essere integrati attraverso algoritmi in grado di decifrare chiavi crittografiche. Questo fattore costituisce, ad esempio, una criticità nel sistema normativo europeo, tant'è che si è molto discusso se il concetto di metadato potesse rientrare nella categoria dei dati personali[31]. Difatti, le tecniche di sorveglianza hanno subito anche in Europa una profonda accelerazione dopo l'11 settembre, che ha portato nel 2006 all'adozione della Direttiva sul Data Retention, dichiarata invalida dalla Corte di Giustizia soltanto nel 2014[32].

La Direttiva 2006/24/CE sul *Data Retention* prevedeva l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare i dati dei propri utenti per un periodo non inferiore a sei mesi e non superiore a due anni, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno stato membro nella propria legislazione nazionale. Ciò, in base alla Direttiva, aveva lo scopo di "identificare l'abbonato o l'utente registrato", tuttavia in base al solo trattamento dei metadati, e non dei contenuti.

Altri programmi, come quello relativo al *passenger number record*, utilizzato al fine di prevenire e combattere il terrorismo. Il programma prevedeva che i dati potessero essere conservati per tre anni e mezzo; i reclami da parte dei passeggeri potevano essere proposti soltanto per iscritto; i dati trasferiti al Custom Boarder Protection (CBP) potevano essere condivisi con il Transportation and Security Administration (TSA)[33].

Tuttavia, la recente pronuncia della Corte di giustizia ha dichiarato invalida la direttiva sul *Data Retention*, la quale avrebbe, infatti, ecceduto i limiti di proporzionalità, considerando che la conservazione dei dati fino al massimo di due anni da parte delle compagnie telefoniche e l'accesso di tali dati consentito alle autorità nazionali competenti, costituisce un'ingerenza particolarmente grave nel diritto fondamentale al rispetto della vita privata e alla protezione dei dati di carattere personale. In particolare, i programmi di sorveglianza di massa su larga scala non sarebbero stati sufficientemente circoscritti e tali da assicurare che l'interferenza fosse limitata a finalità necessarie. "Inoltre – ha osservato la Corte di Giustizia – il fatto che la conservazione ed il successivo utilizzo dei dati avvengano senza che l'abbonato o l'utente registrato ne siano informati può ingenerare negli interessati la sensazione che la loro vita privata sia oggetto di costante sorveglianza".

30 C. Bowden, *The US surveillance programmes and their impact on EU's citizens fundamental rights*, cit., p. 13-14.

31 Cfr. I. S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, "Public and Legal Theory Research Paper Series", Working Paper n. 12-56, p. 1.

32 Sentenza n° C-293/12, 8-4-2014.

33 A. Busch, *From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic*, Vol. 3, 2006, p. 312.

La direttiva, secondo le argomentazioni della Corte, ha, infatti, permesso di identificare comunicazioni di alcuni individui con utenti registrati e abbonati; la durata delle comunicazioni e il luogo dal quale tali comunicazioni sono state effettuate; la frequenza delle comunicazioni tra gli utenti registrati o abbonati con determinate persone i cui dati sono stati collezionati. I fondamentali motivi in base ai quali la direttiva è stata dichiarata invalida riguardano, in primo luogo, il fatto che essa non distingue tra individui e dati. La Corte afferma, infatti, che la Direttiva ha reso possibile la collezione di tutti i dati di tutti gli individui sottoposti da parte di service providers e compagnie telefoniche, soggetti ai quali l'obbligo di collezione dei dati è rivolto. In secondo luogo, la direttiva non ha previsto alcun criterio oggettivo mediante il quale le competenti autorità nazionali potessero giustificare l'accesso ai dati per finalità di prevenzione, detenzione e indagini penali. Inoltre la direttiva non ha fornito un criterio oggettivo per poter determinare la necessità dei diversi periodi di detenzione compresi tra sei mesi e due anni, e non assicurava al termine del periodo di raccolta la distruzione irreversibile dei dati. Infine, la Corte ritiene che la Direttiva, non richiedendo che i dati rimanessero all'interno dello spazio europeo, avrebbe violato indirettamente la normativa europea, e in particolare la Carta Europea dei Diritti Fondamentali, la Direttiva 45/96/CE sulla protezione dei dati personali e la Direttiva 2002/58/CE sulla protezione dei dati personali e della privacy nel settore delle telecomunicazioni.

Questa sentenza può essere letta come un passo importante nell'insieme delle iniziative che recentemente il legislatore e le corti europee hanno adottato per la salvaguardia dei diritti fondamentali. Negli ultimi tempi in Europa si è assistito al tentativo di arginare la politica americana in materia di *foreign intelligence*. Ciò non è chiaramente avvenuto al livello dei trattati internazionali, bensì al livello giudiziario. Sia la Corte di Giustizia sia la Corte Europea dei Diritti dell'Uomo hanno infatti giocato un ruolo propulsivo nel porre un limite alle forme di controllo operate in violazione del diritto alla *privacy*. In particolare, è recente il rinvio pregiudiziale dell'Alta Corte irlandese nei confronti della Corte di Giustizia in merito alla compatibilità del Safe Harbor Agreement con gli articoli 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea [34]. La questione riguarda la legittimità del trasferimento dei dati da *Facebook* alla NSA alla luce del diritto europeo, in quanto coperto dal *Safe Harbor Agreement*[35]. Persino la recente decisione *Google Spain*, sebbene riguardi la diversa questione dell'applicabilità della direttiva comunitaria in materia di protezione dei dati personali (45/96) al trattamento operato da Google, e in particolare del diritto all'oblio, evidenzia una scelta di politica del diritto orientata

34 High Court of Ireland, *Maximillian Schrems v. Data Protection Commissioner*, n.765JR/2013; per una riflessione attenta sugli art. 7 e 8 della Carta di Nizza nella giurisprudenza della Corte di Giustizia, cfr. O. Pollicino, *Un* digital right *to Privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli art. 7 e 8 della carta di Nizza nel* reasoning *della Corte di Giustizia*, in V. Zeno Zencovich – G. Resta, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma Tre-Press, Roma, 2015, p. 7-28.

35 I principi ispiratori del *Safe Harbor Agreement* sono i seguenti: *Notice*, *Choice*, *Onward Transfer*, *Security*, *Data Intergity*, *Access*, *Enforcement*.

alla tutela dei diritti fondamentali dei cittadini europei anche rispetto a violazioni grazie ad un'interpretazione ampia del criterio di territorialità dei server provider[36].

La Corte Europea, da ultimo, è stata destinataria di un ricorso da parte di una società inglese promotrice delle libertà civili (*Big Brother Watch and Others* v. *UK*[37]), la quale lamenta che il programma inglese di *mass surveillance* cd. TEMPORA violerebbe l'art.8 CEDU. Al momento la Corte non ha ancora emesso una sentenza.

4. Le nuove frontiere del Regolamento Europeo

La recente proposta di Regolamento Europeo che modifica sensibilmente la Direttiva sulla protezione dei dati personali è stata una chiara risposta da parte dell'Europa nel senso di una rivendicazione del principio di territorialità della giurisdizione.

Il 25 gennaio 2012 la Commissione Europea ha presentato una proposta di riforma della disciplina riguardante la protezione dei dati personali, che comprende sia una bozza di Direttiva sulla protezione dei dati personali in materia di giustizia penale, sia il nuovo regolamento sulla protezione dei dati personali[38]. Il regolamento sostituirà la Direttiva 95/46/CE, sarà direttamente applicabile negli ordinamenti nazionali al trattamento dei dati personali in attività di stabilimento del responsabile del trattamento dei dati personali (ad esclusione dei metadati), modificando in parte anche la Direttiva 2002/58/CE, che continua a disciplinare gli specifici obblighi dei service provider. La proposta prevede la non obbligatorietà di notificare i trattamenti all'Autorità di protezione dati, poiché i responsabili e gli incaricati del trattamento sono tenuti soltanto a conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità

Tra le novità del nuovo regolamento ne possono essere ricordate alcune tra le più salienti, come il diritto all'oblio, il principio del "one stop shop", l'obbligo della nomina del "data protection officer". Perché il nuovo regolamento entri in vigore, è necessaria l'approvazione sia da parte del Parlamento sia da parte del Consiglio dell'Unione Europea. Entrambi hanno finora presentato, durante la Presidenza Greca e Italiana 2014, diversi emendamenti al testo della Commissione. Il testo proposto dal Parlamento è stato anche approvato dalla Commissione parlamentare Libertà civili, giustizia e affari interni (LIBE). Il Consiglio dell'Unione Europea ha invece reso note il 29 ottobre 2014 le revisioni al Capitolo IV del Regolamento,

36 Per una riflessione puntuale sul punto cfr. G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i regolatori USA/EU*, in *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, cit., p. 99-124.

37 Application n. 58170 del 4 settembre 2013.

38 *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, disponibile in: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accesso effettuato in: 20/12/2014.

intitolato "Responsabile del trattamento e Incaricato del trattamento", basate su valutazioni che riguardano il rischio del trattamento[39].

Il nuovo regolamento si propone, dunque, l'obiettivo di assicurare un maggiore controllo dei dati personali da parte dei soggetti interessati mediante meccanismi più efficaci di controllo del flusso informativo. Mira, in secondo luogo, a creare un unico mercato dei dati e una disciplina unitaria direttamente applicabile negli ordinamenti nazionali, semplificando le procedure e aggiornando i principi già contenuti nella Direttiva 95/46/CE, per adeguarli all'economia digitale.

Esso si pone, dunque, in continuità con la recente giurisprudenza della Corte di Giustizia, la quale ha assunto il ruolo propulsivo di difesa delle libertà civili mediante un'interpretazione ampia del criterio di territorialità dei server provider.

Tra i problemi aperti del nuovo regolamento vi è quello della giurisdizione extraterritoriale dell'Unione Europea. Il regolamento si applica ai cittadini residenti nell'Unione i cui dati siano oggetto di trattamento da parte di un responsabile del trattamento che non ha il proprio stabilimento nell'Unione, quando ciò riguarda l'offerta di beni e la prestazione di servizi ai cittadini residenti nell'Unione.

In particolare, come anticipato, è stato previsto l'obbligo di nominare la figura di un "responsabile della protezione dei dati" per tutte le pubbliche amministrazioni e le aziende che trattano i dati di oltre cinquemila interessati nell'arco di dodici mesi consecutivi, che hanno più di duecentocinquanta dipendenti, e che per loro natura richiedono il controllo regolare degli interessati.

Tra i principi fondamentali del nuovo Regolamento, si ricordano:

- la portabilità dei dati, previsto dall' art. 18, in base al quale l'interessato ha il diritto di ottenere dal responsabile del trattamento copia dei dati trattati in formato elettronico di uso comune, al fine di poterne fare ulteriori usi;
- il principio di accountability, in base al quale l'onere della prova dell'adozione delle misure preventive è posto in capo al responsabile del trattamento;
- il diritto all'oblio, previsto dall'art.17, che attribuisce all'interessato il diritto alla cancellazione dei dati a prescindere dal luogo in cui sia collocato il server. L'interessato può infatti ottenere la cancellazione dei dati dall'autorità garante in tre casi: quando la raccolta dei dati non sia più necessaria, il procedimento sia avvenuto in maniera non legittima, vi sia un mandato da parte di un'autorità amministrativa o di una corte.

Gli emendamenti presentati dal Parlamento includono tra i destinatari di tale richiesta anche i terzi, per quanto riguarda la cancellazione dei link e delle copie. Le società non europee che offrono servizi ai consumatori europei, sono soggette al regolamento. Anche in questo caso, vi è un'inversione dell'onere della prova: è la società a dover

39 Ad esempio, se il responsabile del trattamento non ha lo stabilimento in Europa e vi opera soltanto occasionalmente, in base alle indicazioni del Consiglio, non sarebbe obbligato a nominare un rappresentante. Inoltre, l'obbligo di consultazione con le autorità garanti sarebbe necessario soltanto nella misura in cui vi sia un comprovato rischio per i diritti e le libertà individuali. Per un commento puntuale cfr. G. Caggiano, *L'interpretazione del criterio di collegamento del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali*, in *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, cit., p. 43-61.

provare che i dati non possono essere cancellati per qualche ragione. Se il responsabile del trattamento ha autorizzato terzi alla pubblicazione dei dati, questi deve essere considerato responsabile della pubblicazione;

– il principio del "One Stop Shop", in base al quale le società si rivolgeranno all'autorità garante del paese nel quale esse hanno il loro stabilimento principale. Ciò eviterà che i titolari dei dati che vivono in uno stato membro debbano presentare il ricorso nello stato nel quale si trovi la società che ha commesso la presunta violazione. Secondo le indicazioni del Parlamento, lo sportello unico dovrebbe permettere alle imprese multinazionali di dialogare con un unico interlocutore nell'Unione Europea (l'Autorità privacy del Paese dove hanno il loro "stabilimento principale"), ma il ruolo dell'Autorità (definita, appunto, "Autorità capofila") deve consistere nel coordinamento di un processo di co-decisione in cui tutte le Authority degli Stati membri interessati da un trattamento devono partecipare ed avere voce (principio di coerenza).
– il principio della privacy *by design* e della privacy *by default*, che consiste nella predisposizione da parte del responsabile del trattamento di misure e procedure tecniche e organizzative volte ad assicurare la conformità del trattamento con le finalità del regolamento e di meccanismi volti a garantire che siano trattati soltanto quei dati necessari per ciascuna finalità specifica del trattamento (art. 23).
– l'introduzione della definizione dei dati pseudonimi, cioè di quei dati che non consentono di identificare una persona fisica, riguardo ai quali il responsabile del trattamento non è obbligato ad acquisire ulteriori dati (art.10).

Per quanto riguarda il trasferimento dei dati agli stati terzi, in base al testo presentato dalla Commissione, occorre alternativamente: a) una decisione della Commissione sull'adeguatezza della protezione offerta dal paese terzo; b) la predisposizione di garanzie adeguate contenute in uno strumento giuridicamente vincolante da parte del paese terzo; c) l'approvazione da parte dell'autorità di controllo di norme vincolanti d'impresa che possano garantire la conformità del trasferimento all'estero ai principi del regolamento. Il Parlamento ha introdotto – oltre alle ipotesi del trasferimento previa decisione di adeguatezza da parte della Commissione, in presenza di garanzie adeguate o in presenza di norme vincolanti d'impresa, contemplate nel testo della Commissione all'art. 42 – l'ulteriore ipotesi del trasferimento non autorizzato dall'Unione Europea (art.43-a). Questo articolo, definito "AntiFisa Clause", inibirebbe il riconoscimento di sentenze o decisioni di autorità amministrative straniere che richiedano ai responsabili o agli incaricati del trattamento la rivelazione e l'invio di dati personali.

Il fenomeno sottostante alla disciplina del *Data Retention*, sfociata da ultimo nel *Datagate*, ha avuto profonde ricadute sulle relazioni tra Europa e Stati Uniti. Dai rapporti del Parlamento Europeo pubblicati nei mesi di settembre e ottobre 2013[40], si evince che vi è stata una massiccia attività di sorveglianza operata dalla

40 Cfr. D. Bigo e altri, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, cit., p. 13; C. Bowden, *The US surveillance*

NSA attraverso vari programmi di intercettazione e di accesso ai dati dei server provider nei confronti dei cittadini europei. Nei confronti di tali cittadini sembrerebbe, infatti, non trovare applicazione il Quarto Emendamento della Costituzione federale[41]. A rendere la situazione ancor più pregiudizievole per gli europei è il *cloud computing*, dopo l'emendamento del FISA Act nel 2008, che ne estende sostanzialmente l'operatività al di là del territorio degli Stati Uniti [42]. Parallelamente è emersa la complicità di alcuni paesi europei nei programmi di sorveglianza di massa, tra i quali Germania, Svezia e Regno Unito, al di fuori dei propri confini nazionali anche in Europa[43]. Tuttavia, mentre il Governo degli Stati Uniti ha pubblicamente ammesso la responsabilità nell'*affaire NSA*, ciò non è avvenuto da parte degli Stati Europei, i quali non hanno mai pubblicamente ammesso il loro coinvolgimento nei programmi di sorveglianza di massa.

Negli Stati Uniti esistono fondamentalmente tre fonti normative sulle quali si basano i programmi di mass surveillance. La prima è il FISA (Foreign Intelligence Surveillance Act, emendato nel 2008) che disciplina la sorveglianza elettronica all'interno del territorio americano allo scopo di ottenere informazioni di *foreign intelligence* da parte di poteri stranieri; il termine "foreign power" include non soltanto gli stati, ma anche le agenzie degli stati stranieri, nonché qualsiasi gruppo coinvolto nel terrorismo internazionale[44]. In particolare, il § 702 del FISA obbliga i server provider a fornire immediatamente tutte le informazioni, gli strumenti e l'assistenza necessari ad acquisire materiali di *foreign intelligence*, attraverso la rivelazione di chiavi crittografiche, dati in transito sui *social network*. Inoltre lo scopo di *foreign intelligence* non deve essere esclusivo, ma soltanto significativo. Tale disposizione non menziona alcun riferimento a limiti territoriali e si rivolge a persone fisiche le quali si trovino presumibilmente al di fuori del territorio americano[45]. Esso inoltre non richiede un ordine giudiziario, essendo sottoposto soltanto a un sistema di certificazione annuale con il quale la FISA Court identifica le categorie di informazioni utili ai fini di *foreign intelligence* che devono essere acquisite in base alla decisione dell'Attorney General e del Direttore della NSA.

programmes and their impact on EU's citizens fundamental rights, cit., p. 12, 28.

41 Cfr. D. Bigo e altri, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, cit., p. 6.

42 C. Bowden, *The US surveillance programmes and their impact on EU's citizens fundamental rights*, cit., p. 22.

43 D. Bigo e altri, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, cit., p. 27, 36.

44 *Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*. 12 dicembre 2013, p. 64. Disponibile in: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. Accesso effettuato in: 20/12/2014.

45 *Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*, 27 November 2013. Disponibile in: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf. Accesso effettuato in: 20/12/2014.

La seconda fonte normativa rilevante è il § 215 dello Usa Patrioct Act, che permette all'FBI di richiedere all'autorità giudiziaria un mandato per ottenere da parte di società "tangible secret records" rilevanti per un'indagine che abbia ad oggetto attività di *foreign intelligence* e sia rivolta a cittadini non americani o di lotta al terrorismo internazionale e alle attività di *intelligence* clandestine. I cittadini americani godono, infatti, della tutela offerta dal Primo Emendamento per la libertà di religione, di espressione, di stampa, di associazione e di petizione nei confronti del Governo per la riparazione dalle ingiustizie. Il problema consiste, in realtà, nel dover interpretare i limiti del concetto di *foreign intelligence information*, che comprende "*information with respect to a foreign-based political organization* or *foreign territory that relates to, and if concerning a United States person is necessary to the conduct of the foreign affairs of the United States*"[46]. Tale definizione generica si riferisce, infatti, a *foreign intelligence information* riguardanti cittadini non americani, purché siano tali da essere rilevanti ai fini della *foreign policy* degli Stati Uniti.

Infine esiste l'*Executive Order 12333* del 1978, emendato nel 2008, che prevede specifici poteri delle agenzie di *intelligence*, tra le quali la collezione di dati di *foreign intelligence*, senza la previsione di alcun limite temporale. Sebbene gli *Executive Order* non possano contrastare con la Costituzione federale, e nel caso di specie con il Quarto Emendamento, tuttavia per essi non esiste un controllo giurisdizionale, rientrando nella piena discrezionalità del Presidente. Inoltre il rapporto *dell'EU-US Working Group on Data Protection* dimostra che l'*Executive Order* menzionato garantirebbe la comunicazione dei programmi di sorveglianza condotti dagli Stati Uniti nei confronti di paesi stranieri, il che non è mai avvenuto, stante la segretezza dell'*Executive Order*.

Vi è da osservare che, paradossalmente, il FISA trova maggiore applicazione nei riguardi dei cittadini europei, mentre può rivolgersi a cittadini americani soltanto quando si tratti di attività rilevanti ai fini della *foreign policy*.

Per quanto riguarda il controllo giurisdizionale sulle attività di *foreign policy*, la FISA Court ha giurisdizione sia per quanto riguarda il FISA sia per quanto riguarda lo USA Patrioct Act, ma non invece nel caso dell'Executive Order 12333. In particolare, in base al paragrafo 215, la Corte deve approvare l'ordine di collezione dei dati imposto alle società. Nel caso della disposizione di cui al paragrafo 702 del FISA, invece, ad autorizzare la collezione dei dati sono l'Attorney General e il Direttore della NSA, mentre il ruolo della Corte è limitato alla conferma di tali ordini in base al mero controllo formale della completezza dei requisiti richiesti. Tuttavia, gli atti emanati dalla FISA Court sono classificati e non vi è diritto per i soggetti titolari dei dati di essere rappresentati dinanzi a essa. La corte opera *ex parte* e *in camera*.

È interessante notare l'argomento utilizzato dal Governo statunitense, secondo il quale occorre distinguere, ai fini della tutela della privacy, l'attività di acquisizione dei dati da quella di collezione dei dati. Secondo tale distinzione, la mera acquisizione dei dati non ne implicherebbe necessariamente il trattamento. L'approccio europeo, invece, anticipa la tutela della privacy già nella fase dell'acquisizione dei dati.

46 50 USC §1801(e)2(B) - http://www.law.cornell.edu/uscode/text/50/1801

5. Conclusioni

Sembra evidente che il fenomeno del *Big Data*, insieme allo scandalo del *Datagate*, investa in maniera profonda il ruolo della concorrenza tra modelli culturali. Dinanzi a un fenomeno di dimensioni globali, le risposte non lo sono. Il conflitto fra ordinamenti è, in realtà, soltanto la punta di un iceberg, sotto il quale si fronteggiano scelte radicali sulle regole che una data comunità intende darsi, e gli stati, si sa, sono dei leviatani. La dissipazione del potere globale tende a disgregare i suoi nuclei di produzione e a delocalizzarne le manifestazioni, rendendo talvolta complementari talvolta indistinguibili cause ed effetti. Anche questa fase si colloca nella grande parabola dei diritti, nella quale la funzione disciplinante del potere rispetto al sapere ha esaurito la sua funzione. Il diritto si rivela inidoneo a regolare il flusso globale dei dati di tutto il pianeta. Per farlo ricorre a soluzioni parziali, scontrandosi con i limiti della territorialità della giurisdizione. Dinanzi a tale scenario, diventa molto difficile ipotizzare una scala di priorità nella gestione del rischio. Come osservato da Gunther Teubner "i *momenta* costituzionali non si limitano alla sfera politica. Nel corso della differenziazione funzionale, tutti i sottosistemi sviluppano energie di crescita che nella loro produttività e distruttività sono fortemente ambivalenti"[47].

Dall'analisi dei programmi di *mass surveillance* europei e statunitensi emerge una forte trasversalità nei contenuti, tale da far riflettere sulle effettive differenze culturali tra i due modelli. Seppure resistano alcuni principi ispiratori della regolamentazione del diritto alla privacy, in generale basata sulla dignità in Europa e intesa come paradigma libertario negli Stati Uniti[48], gli studi recenti mostrano una convergenza nelle pratiche di sorveglianza di massa. Ciò è indice del fatto che la risposta normativa può essere commisurata ad alcuni parametri oggettivi che investono dinamiche globali, ma a livello sovranazionale tali parametri divengono sempre più rarefatti. Nel caso del *Datagate* emerge dalla prospettiva comparata che la giurisprudenza europea ha svolto un importante ruolo regolativo dell'equilibrio tra poteri e diritti, difendendo spesso questi ultimi dall'uso indifferenziato dei primi.

47 G. Teubner, *Logiche costituzionali del toccare il fondo*, "Sociologia e politiche sociali", vol. 14, n. 2, 2011, p. 11.

48 J. Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, "Yale L.J.", 113, 2004, p. 1151.